МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кафедра іноземної філології

ENGLISH FOR CYBERSECURITY

Методичні вказівки
з англійської мови професійного спрямування для самостійної роботи
здобувачів вищої освіти спеціальності *125 Кібербезпека*
першого (бакалаврського) рівня вищої освіти
(Частина I)

Обговорено і рекомендовано
на засіданні кафедри іноземної філології
протокол № 2 від 19.02. 2024 р.

Чернігів 2024

English for Cybersecurity. Методичні вказівки з англійської мови професійного спрямування для самостійної роботи здобувачів вищої освіти спеціальностей *125 Кібербезпека.* першого (бакалаврського) рівня вищої освіти (Частина І) / Укл.: В.А. Пермінова, О. Б. Шендерук, Г.А. Дивнич.Чернігів : НУ «Чернігівська політехніка», 2024. 72 с.

Укладачі:

В. А. Пермінова, кандидат педагогічних наук, доцент, доцент кафедри іноземної філології,
О. Б. Шендерук, кандидат педагогічних наук, доцент, доцент кафедри іноземної філології,
Г.А. Дивнич, кандидат державного управління, доцент кафедри іноземної філології

Відповідальна за випуск:

Литвин С. В., кандидат педагогічних наук, доцент, завідувачка кафедри іноземної філології
Національного університету
«Чернігівська політехніка»

Рецензент:

Сікалюк А.І., кандидат педагогічних наук, доцент кафедри іноземної філології
Національного університету
«Чернігівська політехніка»

ВСТУП

"English for Cybersecurity" – комплексний курс, покликаний забезпечити здобувачів освіти мовними навичками та спеціалізованими знаннями, необхідними для ефективної комунікації у сфері кібербезпеки.

Курс складається з восьми модулів, які охоплюють основні поняття, технічну термінологію, комунікаційні стратегії та тематичні дослідження, пов'язані з кібербезпекою. Ці модулі ретельно структуровані для поступового розвитку мовних навичок та одночасного поглиблення розуміння концепцій кібербезпеки.

У кожному модулі ви знайдете добірку матеріалів для читання. Тексти підібрані таким чином, щоб ознайомити студентів з автентичною мовою, яка використовується в контексті кібербезпеки, надаючи цінну інформацію про специфічні мовні нюанси галузі.

Перед початком роботи з матеріалами для читання студентам будуть запропоновані завдання для підготовки до читання, які активізують відповідну лексику та концепції. Завдання для післячитання заохочують до роздумів, осмислення та застосування набутих знань на практиці.

Інтерактивні вправи та запитання, що спонукають до роздумів, інтегровані в усі модулі для покращення мовних навичок та критичного мислення. Ці елементи покликані сприяти залученню, спільному навчанню та практичному застосуванню мовних концепцій кібербезпеки.

У кожному модулі є спеціальний розділ, присвячений тематичним дослідженням, що дозволяє студентам застосувати мовні навички в реальних сценаріях кібербезпеки. Тематичні дослідження ретельно розроблені, щоб імітувати автентичні ситуації, розвиваючи вміння вирішувати проблеми та посилюючи засвоєння мови.

Для викладачів та фасилітаторів надаються вичерпні методичні рекомендації щодо планування уроків, проведення дискусій та оцінювання прогресу учнів. Ці нотатки містять додаткову інформацію, запропоновані вправи та поради щодо адаптації матеріалу до різних навчальних середовищ.

Щоб допомогти здобувачам освіти опанувати спеціалізовану лексику з кібербезпеки, до посібника включено вичерпний глосарій. Цей ресурс слугує швидким довідником для ключових термінів і технічної мови, що зустрічаються в модулях.

Introduction

"English for Cybersecurity” is a comprehensive course designed to equip students with the language skills and specialised knowledge necessary for effective communication in the field of cybersecurity.

The course consists of eight modules covering basic concepts, technical terminology, communication strategies and case studies related to cybersecurity. These modules are carefully structured to gradually develop your language skills while deepening your understanding of cybersecurity concepts.

Each module contains a selection of reading materials. The texts are selected to introduce students to authentic language used in the context of cybersecurity, providing valuable insights into the specific linguistic nuances of the industry.

but a comprehensive glossary. This resource serves as a quick reference for key terms and technical language encountered in the modules.

Before starting with the reading materials, students will be given pre-reading activities that activate relevant vocabulary and concepts. The post-reading activities encourage reflection, reflection and application of the knowledge gained.

Interactive exercises and thought-provoking questions are integrated throughout the modules to improve language skills and critical thinking. These elements are designed to promote engagement, collaborative learning and practical application of cybersecurity language concepts.

Each module has a special section dedicated to case studies, allowing students to apply language skills in real-life cybersecurity scenarios. The case studies are carefully designed to simulate authentic situations, developing problem-solving skills and reinforcing language acquisition.

Comprehensive teaching notes are provided for teachers and facilitators to plan lessons, lead discussions and assess learner progress. These notes include additional information, suggested activities and tips for adapting the material to different learning environments.

A comprehensive glossary is included to help learners master specialised cybersecurity vocabulary. This resource serves as a quick reference for key terms and technical language used in the modules.

ЗМІСТ

MODULE 1
THE HISTORY OF INTERNET

UNIT 1

Pre-Reading Tasks and Activities:

1. Take a moment to think about the impact of the internet on your life. Jot down some notes on how it has changed the way you communicate, work, learn, or access information.
2. Research and find out who is considered the "father of the internet." What were their contributions and how did they shape the early development of the internet?
3. Make a list of at least five key milestones in the history of the internet. These could be major events, inventions, or technological advancements that played a significant role in its evolution.
4. Watch a short video or read an article about the origins of the internet. Take notes on the key points and any interesting facts or anecdotes you come across.
5. Discuss with a friend or family member their thoughts on how the internet has transformed society. Share your own perspective as well.

The Internet was born around 1960‟s where its access was limited to few scientist, researchers and the defense only. Internet user base have evolved exponentially. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980‟s the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only confined to defense setups, large international companies and research communities.

In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle. The GUIs were written so well that the user don’t have to bother how the internet was functioning. They have to simply make few click over the hyperlinks or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or whether the data can accessed by another person who is connected to the internet or whether the data packet sent over the internet can be spoofed and tempered.

The focus of the computer crime shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pace. Every second around 25 computer became victim to cyber attack and around 800 million individuals are effected by it till 2013.

Post-Reading Activities for the topic "The History of the Internet":

1. Create a multimedia presentation: Use tools like PowerPoint, Prezi, or Google Slides to create a visually engaging presentation summarizing the key points and milestones in the history of the internet. Include images, videos, and relevant facts to enhance your presentation.

2. Design a timeline: Create a visually appealing timeline that highlights the major events and developments in the history of the internet. You can use online tools like Canva or draw it by hand. Add descriptions and images to make it informative and captivating.

3. Write a newspaper article: Imagine you are a journalist reporting on a significant event in the history of the internet. Write a newspaper article that captures the essence of the event, including its impact on society and any relevant details. Be creative and use a catchy headline to grab readers' attention.

4. Conduct an interview: Pretend you are interviewing one of the pioneers of the internet, such as Tim Berners-Lee or Vint Cerf. Write a script for the interview, including questions about their contributions, challenges faced, and their thoughts on the future of the internet. You can also record yourself acting out the interview or perform it live with a partner.

5. Create a digital museum exhibit: Design a virtual museum exhibit showcasing the history of the internet. Use platforms like Google Sites or Wix to create an interactive experience. Include text, images, videos, and interactive elements to engage visitors and provide an immersive learning experience.

6. Organize a debate: Divide students into teams and assign them different perspectives on the impact of the internet. Have a structured debate where each team presents arguments and counterarguments. Encourage critical thinking and respectful discussion about the positive and negative effects of the internet on society.

7. Write a letter to the future: Imagine you are writing a letter to someone in the future, say 50 years from now. Reflect on the history of the internet and its impact on society. Share your thoughts, predictions, and hopes for how the internet will continue to evolve and shape the world.

8. Create an infographic: Summarize the key points and milestones in the history of the internet using an infographic. Use online tools like Piktochart or Canva to create visually appealing graphics that convey information in a concise and engaging manner.

9. Conduct a survey: Design a survey to gather insights on how the internet has impacted people's lives. Ask questions about how it has changed communication, education, work, and entertainment. Analyze the results and present your findings in a report or presentation.

10. Write a short story: Use your imagination to write a fictional story set in a time when the internet was just beginning to emerge. Explore the possibilities and challenges of this new technology through the eyes of your characters. Consider how it affects their lives, relationships, and the world around them.

INTERNET ADDRESS. DNS

Pre-reading questions:

1. What is the Internet? How does it work?
2. Have you heard of the term "DNS" before? If yes, what do you know about it? If no, what do you think it might stand for?

Pre-reading task:

Research and find out the full form of DNS and its purpose in the context of the Internet.

Internet Addresses

With so many devices connected to the internet, we require some mechanism to uniquely identify every device that is connected to the internet. Also we require some centralized system which takes care of this mechanism so that the signs which are used to identify each device are not duplicate; else the whole purpose is defeated. To take care of this, we have a centralized authority known as Internet Assigned Numbers Authority (IANA), which is responsible for assigning a unique number known as IP(Internet Protocol) address. An IP address is a 32-bit binary number which is divided into four octets and each octet consists of 8 binary digits and these octet are separated by a dot(.). An example of an IP address is

11110110.01011010.10011100.1111100

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 256 i.e. 11111111 and in total have 28= 256 different combinations.

Again to remember this 32-bit address in binary is bit difficult, so for the better understanding of the human being, it is expressed in a decimal format. But this decimal format is for human understanding only and the computer understands it in binary format only. In decimal, the above IP address is expressed as 123.45.78.125

These octets are used to create and separate different classes. An IP address consists of two parts viz. **Network** and **Host.** Network part identifies the network different network and the host part identifies a device of a particular network.

This address uniquely identifies a devices connected to the internet similar to the postal system where we identify any house by fist identifying the county, then state, district, post office, cluster/block and finally the house number. These IP addresses are classified into five categories based on the availability of IP range.

DNS

Whenever we browse any website in the internet, we type name something like www.uou.ac.in and we rarely deal with IP address like 104.28.2.92 but the fact is even if we type http:\\ 104.28.2.92 in the URL, it will land us to the same webpage. The fact is we are very comfortable using and remembering the names instead of a number. Moreover, these IP address changes over time and some of the sites have multiple IP address. Also, the transfer of the data over internet is only possible using IP addresses because the routing of the packet of data sent over internet is done using IP address.

There is a server called **Domain Name System(DNS)** which take cares of this translation job to simplify and to save us from remembering these changing IP address numbers, the DNS. Whenever you type an address like http:\\www.uou.ac.in, there is a process called DNS name resolution, takes place in the background. The computer keeps the track of recently visited sites and locally maintains a database in DNS cache. In case, the IP address of the site you have requested for is not found in the DNS cache of your local computer, then the next probable place to find it is DNS server of your Internet Service Provider(ISP). These DNS servers of ISP also maintain the cache of the recently visited pages. Just in case, the information is not found here also, the DNS server of the ISP forward the query to the root nameservers. The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located. There are currently 13 rootname servers. They are:

Let us now discuss, how this internet works? How the email you sent to your friend is received by your friend‟s computer located at another country/continent. When you are working in your laptop/desktop in your home without connecting to the internet, your computer is a standalone system. But, whenever you connect to the internet by dialling to your Internet Service Provider(ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, through which the entire data route, and the user. The ISP connects to the internet backbone at Network Access Points(NAP). These NAPs are the provided by the large telecommunication companies at various regions. These large telecommunication companies connect the countries and the continents by building and maintaining the large backbone infrastructure to route data from NAP to NAP. ISPs are connected to this backbone at NAP and are responsible build and manage network locally. So when you dial internet through modem, you first become part of the local ISP, which in turn connects to the internet backbone through NAP. The data is routed through this backbone and sent to the destination NAP, where the ISP of your friend‟s network is located. As soon as your friend dials his modem to connect to the internet, the data is delivered to your friend‟s computer.

Post-reading questions:
1. What is the role of DNS in the functioning of the Internet?
2. How does DNS convert domain names into IP addresses?
3. What are the advantages and disadvantages of using DNS?

Post-reading task:
Create a diagram illustrating the DNS resolution process, from a user typing in a domain name to the retrieval of the corresponding IP address.
Activities:
1. Conduct a group discussion on the importance of DNS in the Internet's infrastructure.
2. Role-play a scenario where a DNS server encounters a problem. Discuss the potential impact and alternative solutions.
3. Research and present a case study on a major DNS outage or attack that occurred in recent years. Discuss the consequences and lessons learned from it.

UNIT 2

Pre-reading questions:
1. What do you understand by the term "Internet infrastructure"?
2. How do you think the internet infrastructure enables the functioning of the World Wide Web (WWW)?
3. How do you think the internet infrastructure has evolved over time?

Pre-reading tasks:
1. Make a list of key components or elements that you think are part of the internet infrastructure.
2. Research and compare different internet service providers (ISPs) and their roles in maintaining the internet infrastructure.
3. Think of some examples where a disruption in the internet infrastructure could have significant consequences.

Internet Infrastructure

Internet, as the name suggests, in a network of network i.e. it is a collection of several small, medium and large networks. This clearly indicates to one fact, nobody is a single owner of the internet and it is one of the proven example of collaborative success. Now you must be surprised how such a large network which is spread across the continents can run without the any problem. Yes it is correct that to monitor such a large network, we require an international body which can frame the rules, regulation and protocols to join and use this network. Therefore, an international organization, known as “The Internet Society” was formed in 1992 to take care of such issues.

Let us now discuss, how this internet works? How the email you sent to your friend is received by your friend‟s computer located at another country/continent. When you are working in your laptop/desktop in your home without connecting to the internet, your computer is a standalone system. But, whenever you connect to the internet by dialling to your Internet

Service Provider(ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, through which the entire data route, and the user. The ISP connects to the internet backbone at Network Access Points(NAP). These NAPs are the provided by the large telecommunication companies at various regions. These large telecommunication companies connect the countries and the continents by building and maintaining the large backbone infrastructure to route data from NAP to NAP. ISPs are connected to this backbone at NAP and are responsible build and manage network locally. So when you dial internet through modem, you first become part of the local ISP, which in turn connects to the internet backbone through NAP. The data is routed through this backbone and sent to the destination NAP, where the ISP of your friend‟s network is located. As soon as your friend dials his modem to connect to the internet, the data is delivered to your friend‟s computer.

World Wide Web

Sometimes we interchangeably use the term internet and world wide web or simply the web, as it is popularly known as. But web is only one of the several the utilities that internet provides. Some of the popular service that internet provides other then web is e-mail, use net, messaging service, FTP, etc. The web use HTTP protocol to communicate over internet and to exchange information. The web was developed at CERN (Europeen de Reserches Nucleaires), Switzerland) by a UK scientist Tim Berners-Lee in 1989. It consists of all the public web sites and all the devices that access the web content. WWW is an information sharing model which is developed to exchange information over the internet. There are plenty of public websites, which is a collection of web pages, available over the internet. These web-pages contain plenty of information in a form of text, videos, audio and picture format. These web pages are access using a application software called a web browser. Some of the examples of the popular web browser are: Internet explorer, Chrome, Safari, Firefox, etc.

Post-reading questions:

1. Explain the different layers of the internet infrastructure and how they interact with each other.
2. How do domain names and IP addresses contribute to the functioning of the WWW?
3. What are the challenges or vulnerabilities associated with the internet infrastructure and how can they be mitigated?

Post-reading tasks:

1. Create a diagram illustrating the layers of the internet infrastructure and explain the role of each layer.
2. Research and analyze a real-life example of a cyber attack that targeted the internet infrastructure or impacted the functioning of the WWW. Discuss the consequences and proposed solutions.
3. Conduct a SWOT (strengths, weaknesses, opportunities, threats) analysis of the internet infrastructure, focusing on potential risks and opportunities for improvement.

INTRODUCTION TO CYBER CRIMES

UNIIT 3

Classification of Cyber Crimes

Pre-Reading Tasks and Questions:

1. What do you already know about cyber crimes? Take a moment to brainstorm and write down your thoughts.
2. Have you ever been a victim of a cyber crime or know someone who has? How did it impact you or the person involved?
3. Research and find out some recent examples of cyber crimes that have made headlines. What were the consequences of these crimes?
4. What are some common types of cyber crimes? List at least three and briefly describe each one.
5. How do you think text classification can help in detecting and preventing cyber crimes? Can you think of any potential challenges or limitations?

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

Insider Attack: An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparitively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and wealness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a varnability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.

External Attack: When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analyzing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker.

Unstructured attacks: These attacks are generally performed by armatures who don't have any predefined motives to perform the cyber attack. Usually these armatures try to test a tool readily available over the internet on the network of a random company.

Structure Attack: These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems (IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at part with those of developed nation. They are targeting large financial organizations, defense and nuclear establishments and they are also into online drugs trading.

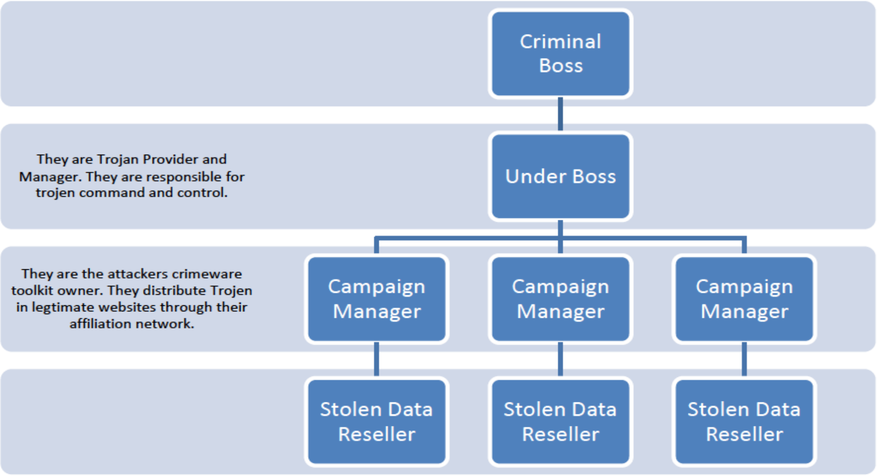

Criminal Boss
They are Trojan Provider and Manager. They are responsible for trojen command and control.
Under Boss
They are the attackers crimeware toolkit owner. They distribute Trojen in legtimate websites through their affiliation network.
Campaign Manager
Campaign Manager
Campaign Manager
Stolen Data Reseller
Stolen Data Reseller
Stolen Data Reseller

Figure 1 : Hierarchical Organisational Structure

The role of all the people in the hierarchy remain changing and it is based on the opportunity. If a hacker who have hacked sensitive data from an organization may use it for financially exploiting the organization himself. In case, the hacker himself have the technical expertise for it, he will do it himself, otherwise he may find a buyer who is interested in that data and have the technical expertise.

There are some cyber criminals offers on-demand and service. The person, organization or a country may contact these cyber criminals for hacking an organization to gain access to some sensitive data , or create massive denial-of–service attack on their competitors. Based on the demand of the customer the hackers write malware, virus, etc. to suit their requirements. An organization effected by a cyber attack, not only faces financial loss, but its reputation is also adversely affected, and the competitor organization will defiantly benefited by it.

Post-Reading Tasks and Questions:

1. Summarize the main points discussed in the text about cyber crimes and the importance of text classification in this context.
2. What are some key challenges in accurately classifying cyber crimes using text classification techniques? How can these challenges be addressed?
3. Reflect on the potential ethical implications of using text classification for detecting and preventing cyber crimes. Are there any concerns or trade-offs to consider?
4. What are some potential future advancements in text classification that could further enhance the detection and prevention of cyber crimes?

5. Imagine you are a cybersecurity expert. How would you leverage text classification techniques to combat cyber crimes? Provide a brief overview of your approach.

UNIT 4

1. What do you understand by the term "cyber crime," and how do you think it differs from traditional forms of crime?
2. Can you name some common types of cyber crimes, and what do you think might motivate individuals to engage in such activities?
3. How do you think advancements in technology have influenced the prevalence and nature of cyber crimes?
4. In your opinion, what are some of the potential risks and consequences of cyber crimes for individuals, organizations, and society as a whole?
5. How do societal, economic, and technological factors contribute to the motivations behind cyber crimes, and what ethical considerations might be at play?

Reasons for Commission of Cyber Crimes

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

a. ***Money****:* People are motivated towards committing cyber crime is to make quick and easy money.

b. ***Revenge****:* Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.

c. ***Fun****:* The amateur do cyber crime for fun. They just want to test the la

d. ***Recognition****:* It is considered to be pride if someone hack the highly secured networks like defense sites or networks.

e. ***Anonymity****-* Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world. It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.

f. ***Cyber Espionage:*** At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

Post-Reading Questions:

1. What are the common motivations for individuals or groups to engage in cyber crimes, and how do these motivations differ from those driving traditional crimes?
2. How do societal, economic, and technological factors contribute to the prevalence of cyber crimes, and what implications do these factors have on cybersecurity measures?
3. In what ways can understanding the motivations behind cyber crimes help in developing more effective prevention and response strategies?

MODULE 2
MALWARE AND ITS TYPES

UNIT 5

1. What is your understanding of the term "malware"?
2. Have you ever encountered any form of malware or experienced issues related to malicious software on your devices?
3. How important do you think it is to have antivirus or anti-malware software installed on your computer or other devices?
4. Can you name any specific types of malware that you are aware of?

MALWARE AND ITS TYPE

Malware stands for "*Malicious Software*" and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

Adware

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

Spyware

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programmes from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

Browser hijacking software

There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

Post-Reading Questions:

1. Define malware and provide examples of different types discussed in the reading.
2. What are the common methods through which malware infiltrates a computer or network?
3. How can users protect themselves from malware attacks?
4. Describe the differences between adware and spyware.
5. In what ways can browser hijacking software impact a user's online experience?
6. Discuss the potential consequences of a malware infection on an individual's personal and financial information.
7. How do cybersecurity experts typically classify or categorize different types of malware?
8. Can you think of any real-world examples or incidents where malware caused significant damage or disruption?

Activities:

1. Malware Scanning Workshop:

Demonstrate the process of scanning for malware using antivirus or anti-malware tools. Perform hands-on malware scanning on sample files to understand the practical aspects of threat detection.

2. Create an Infographic:

In small groups, create an infographic highlighting the key features and prevention tips for different types of malware. Encourage creativity in design and presentation.

UNIT 6

1. What is your understanding of computer viruses, worms, Trojan horses, and shareware?
2. How do you think these types of computer threats differ from each other?
3. Have you ever encountered any computer security issues or malware on your devices?
4. How do you currently protect your computer or devices from malicious software?

Virus. Worms. Trojan Horse. Scareware.

Virus

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention. 20

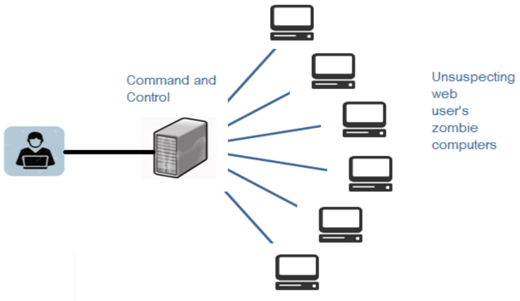
Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke.

Trojan Horse

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of botnet(robot-network), a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojens neither infect the other computers in the network nor do they replicate



Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user‟s computer. As a remedial measure, the message suggests the used download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid.

Post-Reading Questions:

1. Can you describe the main differences between viruses, worms, Trojan horses, and shareware based on what you've learned?
2. How do these types of threats exploit vulnerabilities in computer systems?
3. What are some common methods for preventing or mitigating the risks associated with viruses, worms, Trojan horses, and shareware?
4. Can you provide examples of real-world incidents where these types of threats have caused significant damage or disruption?
5. In what ways can users contribute to a safer online environment in the context of these computer threats?

Activities:

1. **Antivirus Software Evaluation:** Research and evaluate different antivirus software available in the market. Create a comparison chart highlighting features, effectiveness, and user reviews. Discuss which antivirus software would be most suitable for specific scenarios.
2. **Create a Security Guide:** In groups, develop a comprehensive guide for computer users on protecting their systems from viruses, worms, Trojan horses, and the risks associated with shareware. Include practical tips, tools, and resources for maintaining a secure digital environment.

CYBER SECURITY TECHNIQUES 1

UNIT 7

1. What does the term "authentication" mean to you in the context of digital security?
2. How do you currently authenticate yourself in different online platforms or services?
3. Can you identify any challenges or risks associated with weak authentication methods?

4. What are some common types of authentication methods you've come across or used?

CYBER SECURITY TECHNIQUES

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

AUTHENTICATION

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like *One Time Password* (OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an *SMS* or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network. The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the used to the information he requested. The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is go hand-in-hand with authorization. Now, one can easily understand the role of strong password for authorization to ensure cyber security as an easy password can be a cause of security flaw and can bring the whole organization at high risk.

Therefore, the password policy of an organization should be such that employees are forced to use strong passwords (more than 12 characters and combination of lowercase and uppercase alphabets along with numbers and special characters) and prompt user to change their password frequently. In some of the bigger organizations or an organization which deals in sensitive information like defence agencies, financial institutions, planning commissions, etc. a hybrid authentication system is used which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use *VPN* (Virtual Private Network), which is one of the method to provide secure access via hybrid security authentication to the company network over internet.

Post-Reading Questions:

1. Explain the importance of authentication in ensuring digital security. How does it contribute to protecting personal information and sensitive data?
2. Compare and contrast different authentication methods, such as passwords, biometrics, and two-factor authentication (2FA). What are the strengths and weaknesses of each?
3. In what ways can authentication be vulnerable to cyber attacks, and what measures can be taken to enhance its security?
4. How might advancements in technology, such as facial recognition or fingerprint scanning, impact the future of authentication?

5. Reflect on the role of user awareness and education in maintaining effective authentication practices. How can individuals contribute to a more secure digital environment?

Activities:

1. **Authentication Method Analysis:** Research and create a presentation comparing various authentication methods, including their mechanisms, applications, and security considerations.

2.**Password Strength Workshop:** Conduct a hands-on workshop on creating strong passwords and educate peers on the importance of using unique and secure passwords for different accounts.

3.**Security Awareness Campaign:** Develop a social media or poster campaign to raise awareness about the significance of authentication. Include tips for users on strengthening their authentication practices.

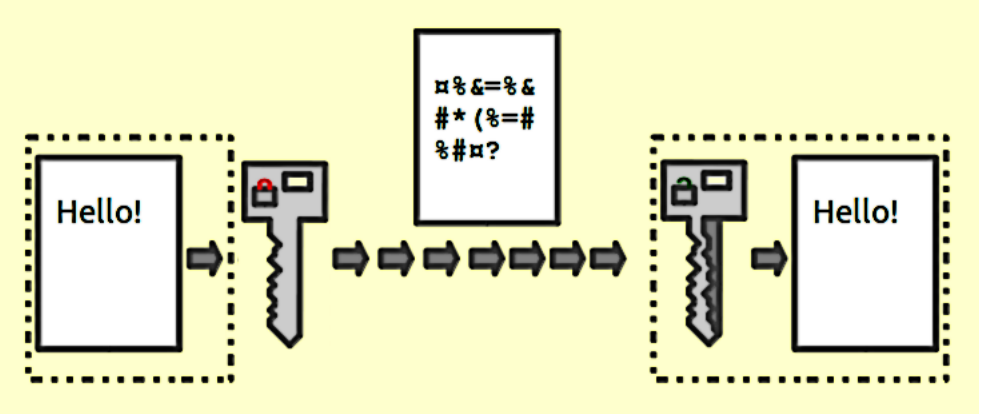
4. **Authentication Technology Showcase**: Organize a showcase where students research and present on emerging authentication technologies, such as biometrics, smart cards, or blockchain-based authentication.

UNIT 8

1. What does the term "encryption" mean to you, and how do you think it is used in the context of digital communication?
2. Can you identify any scenarios or applications where encryption might be crucial for securing information?
3. How familiar are you with the concept of a digital signature, and what purposes do you think it serves in online transactions or communications?
4. In what ways do you currently use or encounter encryption in your digital interactions?

ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.



In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue. To avoid the transfer of key a method called asymmetric key encryption, also known as public key encryption, is used. In asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse‟s two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B‟s public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be send to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

DIGITAL SIGNATURES

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original sender, is required for this purpose.

As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.

Post-Reading Questions:

1. Explain the role of encryption in ensuring the confidentiality and integrity of digital information. How does it contribute to cybersecurity?
2. Compare symmetric and asymmetric encryption methods. What are the advantages and disadvantages of each in different contexts?
3. How does digital signature technology work, and what benefits does it provide in terms of authenticity and non-repudiation?
4. Reflect on the potential risks and challenges associated with the widespread use of encryption. How might it impact law enforcement or privacy concerns?
5. In what industries or applications is encryption particularly crucial, and why?

Ativities:

1. **Encryption Demo and Discussion:** Conduct a demonstration of encryption using a simple example or tool. Discuss the basic principles and mechanics of encryption with your peers.
2. **Case Study Analysis:** Research and present case studies of real-world incidents where encryption played a crucial role in preventing data breaches or securing sensitive information.
3. **Encryption Tools Exploration:** Explore and compare different encryption tools available for various platforms. Evaluate their ease of use, effectiveness, and compatibility with different file types.
4. **Digital Signature Simulation:** Simulate a digital signature process where students sign and verify digital documents using cryptographic keys. Discuss the importance of digital signatures in ensuring the authenticity of digital content.

MODULE 3
CYBER SECURITY TECHNIQUES 2

UNIT 9

1. What do you understand by the term "antivirus," and how do you think it contributes to computer security?
2. Have you ever encountered a situation where your computer was infected with malware? How did you address it?
3. How do you currently protect your devices from viruses or other malicious software?
4. Can you name any antivirus software, and what do you think are their primary functions?

ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

Post-Reading Questions:

1. Explain the key functions of antivirus software and how it helps in protecting computer systems from malware.
2. Compare and contrast different types of malware that antivirus programs commonly target. How do viruses, worms, Trojans, and ransomware differ in their behavior?
3. Reflect on the evolution of antivirus software. How have these programs adapted to changing cybersecurity threats over the years?
4. Discuss the limitations of antivirus software and situations where it may not be fully effective in preventing malware infections.
5. In what ways can user behavior contribute to the effectiveness of antivirus software? What are some best practices for maintaining a secure digital environment?

Tasks and Activities:

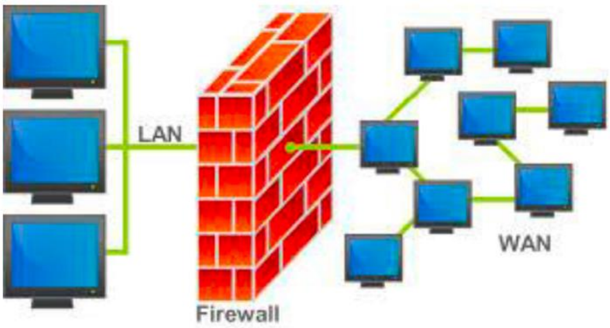
1. **Antivirus Software Review:**Research and compare different antivirus software solutions. Create a chart outlining their features, user reviews, and effectiveness in dealing with various types of malware.
2. **Malware Simulation and Response:** Simulate a malware attack scenario, and have students discuss and implement a response plan using antivirus software. Emphasize the importance of quick and effective action.
3. **Antivirus Effectiveness Survey:** Create a survey to gather opinions from peers and family members about their experiences with antivirus software. Analyze the results and discuss common trends and challenges.
4. **Create an Antivirus Awareness Campaign:** Develop a campaign to raise awareness about the importance of using antivirus software. Include tips for selecting, updating, and maintaining antivirus programs on various devices.

UNIT 10

1. What does the term "firewall" mean in the context of computer security, and why do you think it is important?
2. Have you ever encountered a situation where a firewall played a role in protecting a computer network or system? Share your experience.
3. How familiar are you with the concept of "steganography," and what purposes do you think it serves in the realm of digital communication?
4. Can you speculate on how firewalls and steganography might be interconnected or impact each other in a cybersecurity context?

FIREWALL

It is a hardware/software which acts as a shield between an organization‟s network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.



There are two type of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization‟s network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.

Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations‟ network.

In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow "rules" and "policies" and based on these defined rules the firewalls can follow the following filtering mechanisms.

Proxy- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.

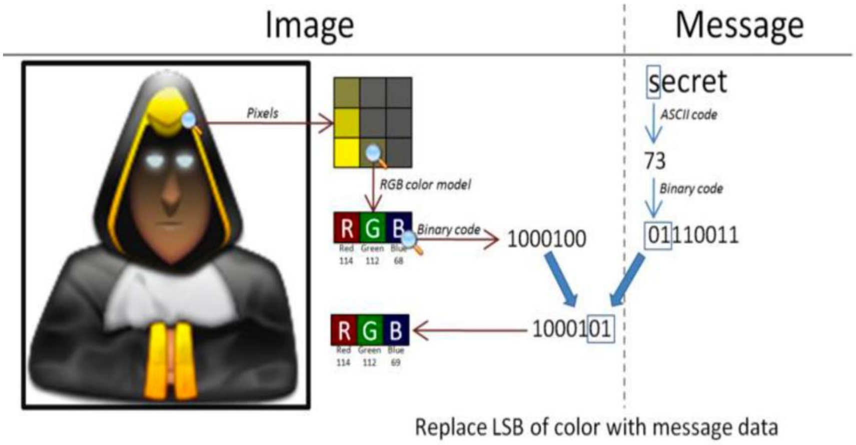
Packet Filtering- based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.

Stateful Inspection: rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.

The firewalls are an essential component of the organizations‟ network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

STEGANOGRAPHY

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.



There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft , digital watermarks for IPR issues, etc.

Let us discuss how the data is secretly embeded inside the cover file(the medium like image, video, audio, etc which is used for embed secret data) without being noticed. Let us take an example of an image file which is used as a cover mediem. Each pixel of a high resolution image is represented by 3 bytes(24 bits). If the 3 least significant bits of this 24 bits are altered and used for hiding the data, the resultant image, after embeded the data into it, will have un-noticible change in the image quality and only a very experienced and tranined eyes can detect this change. In this way, evcery pixel can be used to hide 3 bits of information.

Similerly, introducing a white noise in an audio file at regular or randon interval can be used to hide data in an audio or video files. There are various free softwares available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

Post-Reading Questions:

1. Explain the role of a firewall in computer security. How does it function to protect networks and systems from unauthorized access and potential threats?
2. Compare and contrast hardware firewalls and software firewalls. In what scenarios might one be preferred over the other?
3. Discuss the ethical considerations of using steganography. How can it be used for both legitimate and malicious purposes in the digital realm?
4. How might steganography be employed to bypass or manipulate firewall defenses? What challenges does this pose for cybersecurity professionals?
5. Reflect on the balance between privacy and security when it comes to the use of firewalls and steganography. How can individuals protect their data while also maintaining network security?

Tasks and Activities:

1. **Steganography Workshop:** Conduct a hands-on workshop introducing steganography techniques. Have students hide and reveal messages in digital images or files, exploring the concept of covert communication.
2. **Case Study Analysis:** Research and present case studies where firewalls played a crucial role in preventing cyber attacks. Discuss the impact on the targeted systems and the lessons learned from each incident.
3. **Steganography in Media Analysis:** Analyze real-world examples of steganography in media, such as images or audio files. Discuss the potential applications and risks associated with hiding information in plain sight.

UNIT 11
INVESTIGATING CYBERCRIMES: INTRODUCTION TO CYBER FORENSIC

1. What does the term "computer forensics" mean to you, and how do you think it contributes to digital investigations?
2. Have you ever heard of or encountered computer forensics in the context of law enforcement or cybersecurity? Share your thoughts.
3. How do you think computer forensics might differ from traditional forensic science? Are there any unique challenges in the digital realm?
4. In what scenarios do you think computer forensics is crucial, and why?

COMPUTER FORENSICS

In the presiding chapters, we have discussed the prevention techniques for cyber attack. What if one have encounter cyber attack? What Next? The next step is to report the cyber crime. But if a person is exposed to cyber forensic principles, the chances that the person accidently destroy the vital cyber evidences are minimized. Cyber forensic is a branch of science which deals with tools and techniques for investigation of digital data to find evidences against a crime which can be produced in the court of law. It is a practice of preserving, extracting, analyzing and documenting evidence from digital devices such as computers, digital storage media, smartphones, etc. so that they can be used to make expert opinion in legal/administrative matters.

The computer forensic plays a vital role in an organization as the our dependency on computing devices and internet is increasing day-by-day. According to a survey conducted by University of California7, 93% of all the informaiton generated during 1999 was generated in digital form, on computers, only 7% of the remaining information was generated using other sources like paper etc. It not always easy to collect evidences as the data may be temperd, deleted, hidden or encrypted. Digital foransic investigation is a highly skilled task which needs the expose of various tools, techniques and guidelines for fininding and recovering the digital evidances from the crime scene or the digital equipments used in the crime. With digital equipments like computation speed, the possibility of use of these devices in cyber crime cannot be ruled out. A forancis investigator must not only have deep understanding of the working of these devices and also hands-on exposure to the tools for accurate data retrival so that the value and intrigity of the data is preserved.

A computer can be used intentionally or unintentionally to cyber crime. The intentional use is to use your computer to send hate mails or installing cracked version of an otherwise licenced software into your computer. Unintentional use is the computer you are using contains virus and it is spread into the network and outside the network causing major loss to someone in financial terms. Simillerly a computer can be directly used to commit a digital crime. For example, your computer is used to access the sensitive and classified data and the data is sent someone inside/outside the network who can use this data for him own benefit. The indirect use of computer is when while downloading a crack of a software, a trozan horse is stored in the computer, while creates a backdoor in the network to facilitate hacker. Now the hacker logs into your computer and use it for committing cyber crime. An experienced computer forensic investigator plays a crucial role in distinguishing direct and indirect attack. Computer forensic experts are also useful for recovery of accidental data loss, to detect industrial espionage, counterfeiting, etc.

In large organization, as soon as a cyber crime is detected by the incident handling team, which is responsible for monitoring and detection of security event on a computer or computer network, initial incident management processes are followed8.

This is an in-house process. It follows **following steps**:

1. ***Preparation:*** The organization prepares guidelines for incident response and assigns roles and the responsibilities of each member of the incident response team. Most of the large organizations earn a reputation in the market and any negative sentiment may negatively affect the emotions of the shareholders. Therefore, an effective communication is required to declare the incident. Hence, assigning the roles based on the skill-set of a member is important.

2. ***Identification****:* based on the traits the incident response team verifies whether an event had actually occurred. One of the most common procedures to verify the event is examining the logs. Once the occurrence of the event is verified, the impact of the attack is to be assessed.

3. ***Containment:*** based on the feedback from the assessment team, the future course of action to respond to the incident is planned in this step.

4. ***Eradication:*** In this step, the strategy for the eradication or mitigate of the cause of the threat is planned and executed.

5. ***Recovery:*** it is the process of returning to the normal operational state after eradication of the problem.

6. ***Lesson Learned:*** if a new type of incident is encounter, it is documented so that this knowledge can be used to handle such situations in future.

The second step in the process is forensic investigation is carried out to find the evidence of the crime, which is mostly performed by 3rd party companies.

The computer forensic **investigation involves following steps:**

1. ***Identify incident and evidence*****:** this is the first step performed by the system administrator where he tries to gather as much information as possible about the incident. Based on this information the scope and severity of the attack is assessed. Once the evidence of the attack is discovered, the backup of the same is taken for the investigation purpose. The forensic investigation is never performed on the original machine but on the data that is restored from the backup.

2. ***Collect and preserve evidence****:* Various tools like Helix, WinHex, FKT Imager, etc. are used to capture the data. Once the backup of the data is obtained, the custody of the evidence and the backup is taken. MD5(message digest) hash of the backup is calculated and matched with the original one to check the integrity of the data. Other important sources of information like system log, network information, logs generated by Intrusion Detection Systems(IDS), port and process information are also captured.

3. ***Investigate:*** The image of the disk is restored from the backup and the investigation is performed by reviewing the logs, system files, deleted and updates files, CPU uses and process logs, temporary files, password protected and encrypted files, images, videos and data files for possible stegnographic message, etc.

4. ***Summarize and Presentation:*** The summery of the incident is presented in chronological order. Based on the investigation, conclusions are drawn and possible cause is explained.

While carrying out the digital forensic investigation, rules and procedure must be applied. Specially while capturing the evidence. It should be ensured that the actions that are taken for capturing the data do not change the evidence. The integrity of the data should be maintained. It must be ensured that the devices used for capturing the backup are free from contamination.

Moreover, all the activities related to seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review9. Prevention is always better than cure. It is always recommended to fine tune your intrusion detection system like firewall occasionally perform penetration tests on your network to avoid pray to hacker. Last but not the least, report the crime.

Post-Reading Questions:

1. Explain the goals and objectives of computer forensics. How does it contribute to solving cybercrimes and ensuring digital security?
2. Discuss the ethical considerations and challenges associated with conducting computer forensic investigations. How can investigators balance privacy concerns with the need for digital evidence?
3. Reflect on the evolution of computer forensics in response to advancements in technology. How has it adapted to address emerging cyber threats?
4. In what ways does computer forensics contribute to legal proceedings, and what role does digital evidence play in court cases?
5. How might the field of computer forensics be impacted by the constant evolution of technology and the increasing sophistication of cybercriminals?

Tasks and Activities:

1. **Legal and Ethical Dilemma Discussion:** Facilitate a discussion on the legal and ethical dilemmas faced by computer forensic professionals. Explore real-world cases and discuss the decisions made by investigators.
2. **Interview with a Computer Forensics Expert:** Arrange a virtual or in-person interview with a professional in the field of computer forensics. Prepare questions in advance and share insights with the class.

UNIT 12

1. What steps would you take if you were a victim of cybercrime or witnessed a cyber attack?
2. How do you think reporting a cybercrime differs from reporting a traditional crime?
3. Are you aware of any specific platforms or organizations that handle cybercrime reporting?
4. What do you think are the challenges individuals and organizations face when reporting cybercrimes?

REPORTING A CYBERCRIME

Some of the companies do not report a cyber crime incident because they fear this will harm their reputation amongst its shareholders. Some of the data are very sensitive and its disclosure may impact their business negatively. But, the fact is until and unless a cyber crime incident is reported, the cyber criminals will never be crabbed by the law enforcement agencies. This will further worsen the conditions and encourage the criminals to repeat these types of incidents with the same or the other organizations. So it is very important to identify and prosecute them. This will help not only to identify the existing threats to the economy and the infrastructure but also new threats are identified. Depending on the scope of a cyber crime, the cyber crime should be reported to nearest cyber cell of your locality, state cyber cell, central investigating agencies like CBI, IB or the international bodies like Interpol.

Post-Reading Questions:

1. Outline the importance of reporting cybercrimes. How does timely reporting contribute to addressing and preventing cyber threats?
2. Discuss the potential impact of unreported cybercrimes on individuals, businesses, and society as a whole.
3. Explain the role of law enforcement agencies, cybersecurity organizations, and government bodies in handling reported cybercrimes.
4. Reflect on the challenges and barriers people might face when reporting cybercrimes. How can these challenges be addressed to encourage more reporting?
5. Explore the legal and ethical considerations associated with reporting cybercrimes. How can reporting mechanisms balance the need for justice with user privacy?

Tasks and Activities:

1. **Create a Cybercrime Reporting Guide:** In groups, create a comprehensive guide on how to report different types of cybercrimes. Include information on reporting platforms, essential details to provide, and steps to take after reporting.

2. **Interview with a Cybersecurity Professional:** Arrange an interview with a cybersecurity professional or law enforcement officer specializing in cybercrime investigations. Prepare questions related to the reporting process and share insights with the class.

3. **Legal and Ethical Debate:** Organize a debate discussing the legal and ethical considerations of reporting cybercrimes. Explore topics such as user privacy, data protection, and the role of law enforcement.

MODULE 4
PASSWORD SEQURE. VERIFICATION. USING FREE ANTIVIRUS

UNIT 13

1. How would you describe the importance of having secure passwords in the context of digital security?
2. What challenges do you typically encounter when creating and managing passwords for various online accounts?
3. What do you understand about two-step verification, and in what situations have you encountered or used it?

4. Why might individuals choose to use free antivirus software, and what considerations should be taken into account when selecting such tools?

GUIDELINES FOR SECURE PASSWORD, TWO STEP VERIFICATION AND USING FREE ANTIVIRUS. GENERATING SECURE PASSWORD

Guideline for setting secure Password

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

Basics

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.
- Things to avoid
- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

Tips

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

  Bad Passwords:
- Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree"

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in. Remember, don't re-use a password.
- Protecting your password
- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

- Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?
- Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the users name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

- None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody elses.
- "mItWdOtW4Me" - Monday is the worst day of the week for me.

How would a potential hacker get hold of my password anyway?

There are four main techniques hackers can use to get hold of your password:

1. Steal it. That means looking over your shoulder when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.

2. Guess it. It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.

3. A brute force attack. This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A

Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
4. A dictionary attack. A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

Post-Reading Questions:

1. Summarize the key guidelines for creating a secure password. How do these guidelines contribute to better digital security?
2. Explain the concept of two-step verification and discuss its advantages in enhancing account security.
3. Compare and contrast free antivirus software with paid alternatives. What factors should users consider when deciding on antivirus solutions?
4. Reflect on the role of user behavior in maintaining secure passwords and effective two-step verification. How can individuals contribute to their own cybersecurity?
5. How might advancements in technology impact the effectiveness of secure password practices and two-step verification methods?

Tasks and Activities:

1. **Secure Password Workshop**: Conduct a workshop on creating secure passwords. Provide guidelines and practical tips, and have students create and analyze strong passwords.

2.**Two-Step Verification Simulation:** Simulate the two-step verification process using common platforms. Discuss the experience and the additional layer of security it provides.

3. **Antivirus Software Comparison:** Research and compare different free antivirus software options. Create a visual chart highlighting features, user reviews, and effectiveness in handling various types of malware.

4. **Password Security Awareness Campaign:** Develop an awareness campaign promoting secure password practices within the school or community. Include posters, social media posts, and informational sessions.

5. **Create a Two-Step Verification Guide:** In groups, create a comprehensive guide on how to set up and use two-step verification for various online accounts. Include step-by-step instructions and practical tips.

6. **Cybersecurity Presentation:** Prepare a presentation on the importance of secure passwords, two-step verification, and the use of free antivirus software. Include real-world examples and case studies.

UNIT 14

1. Have you ever used a password manager before? If yes, what was your experience? If not, what do you think the advantages might be?
2. How do you currently manage your passwords for various online accounts? What challenges do you face in doing so?
3. What concerns or reservations might individuals have about using a password manager?
4. Why is the security of your passwords crucial in today's digital landscape?

USING PASSWORD MANAGER

We use passwords to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft, which is easily accomplished when passwords are compromised. The need of the hour is good password management. Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials? Password managers are one of the best ways to store, back up and manage your passwords. A good password is hard to remember and that‟s where a password manager

comes in handy. It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

What is a password manager? A password manager is software that helps a user to manage passwords and important information so that it can be accessed any time and anywhere. An excellent password manager helps to store information securely without compromising safety. All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

Why you should use it? If you find it hard to remember passwords for every website and don‟t want to go through the „Forgot password?‟ routine off and on, then a password manager is what you are looking for. These are designed to store all kinds of critical login information related to different websites.

How does it work? Password managers may be stored online or locally. Online password managers store information in an online cloud, which can be accessed any time from anywhere. Local password managers store information on the local server, which makes them less accessible. Both have their own advantages, and the manager you use would depend on your need. Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don‟t have to worry about online issues. Both these options can also be combined and used as two-factor authentication so that data is even more secure.

Some popular Password managers The passwords are saved using different encryptions based on the services that the companies provide. The best password managers use a 256-bit (or more) encryption protocol for better security, which has been accepted by the US National Security Agency for top secret information handling. If you have considered using a password manager and haven‟t decided on one, this section features the top five.

1. KeePassX: KeePassX is an open source, cross-platform and light weight password management application published under the terms of the GNU General Public License. It was built based on the Qt Libraries. KeePassX stores information about user names, passwords and other login information in a secure database. KeePassX uses its own random password generator, which makes it easier to create strong passwords for better security. It also includes a powerful and quick search tool with which a keyword of a website can be used to find login credentials that have been stored in the database. It allows users to customise groups, making it more user friendly. KeePassX is not limited to storing only usernames and passwords but also free-form notes and any kind of confidential text files.

Features

- *Simple user interface:* The left pane tree structure makes it easy to distinguish between different groups and entries, while the right pane shows more detailed information.
- *Portable media access:* Its portability makes it easy to use since there's no need to install it on every computer.
- *Search function:* Searches in the complete database or in every group.
- *Auto fill:* There"s no need to type in the login credentials; the application does it whenever the Web page is loaded. This keeps it secure from key loggers.
- *Password generator:* This feature helps to generate strong passwords that make it difficult for dictionary attacks. It can be customised.
- *Two factor authentication:* It enables the user to either unlock the database by a master password or by a key from a removable drive.
- *Adds attachments:* Any type of confidential document can be added to the database as an attachment, which allows users to secure not just passwords.
- *Cross-platform support:* It works on all supported platforms. KeePassX is an open source application, so its source code can be compiled and used for any operating system.
- *Security:* The password database is encrypted with either the AES encryption or the Twofish algorithm, which uses 256-bit key encryption.
- *Expiration date*: The entries can be expired, based on a user defined date.
- *Import and export of entries: Entries:* from PwManager or Kwallet can be imported, and entries can be exported as text files.
- *Multi-language support:* It supports 15 languages.

2. **Clipperz:** Clipperz is a Web-based, open source password manager built to store login information securely. Data can be accessed from anywhere and from any device without any installation. Clipperz also includes an offline version when an Internet connection is not available.

Clipperz

Features

- *Direct login*: Automatically logs in to any website without typing login credentials, with just one click.
- *Offline data*: With one click, an encrypted local copy of the data can be created as a HTML page.
- *No installation:* Since it's a Web-based application, it doesn't require any installation and can be accessed from any compatible browser.
- *Data import:* Login data can be imported from different supported password managers.
- *Security:* The database is encrypted using JavaScript code on the browser and then sent to the website. It requires a passphrase to decrypt the database without which data cannot be accessed.
- *Support:* Works on any operating system with a major browser that has JavaScript enabled.

3. Password Gorilla: Password Gorilla is an open source, cross-platform, simple password manager and personal vault that can store login information and notes. Password Gorilla is a Tcl/Tk application that runs on Linux, Windows and Mac OS X. Login information is stored in the database, which can be accessed only using a master password. The passwords are SHA256 protected and the database is encrypted using the Twofish algorithm. The key stretching feature makes it difficult for brute force attacks.

Password manager

Features

- *Access to favorite sites:* A list of favorite Web pages can be accessed quickly from the convenient „tray" icon.
- *Quick fill:* Passwords and other information can be clicked and dragged onto forms for quick filling out.
- *Search bar*: The quick search bar allows users to search passwords that are needed.
- *Password generator:* Passwords with user-defined options can be generated with just a click.
- *Quick launch:* Favourite websites can be launched by right-clicking the tray icon.

Password Safe: Password Safe is a simple and free open source application initiated by Bruce Schneier and released in 2002. Now Password Safe is hosted on

SourceForge and developed by a group of volunteers. It's well known for its ease of use. It is possible to organize passwords based on user preference, which makes it easy for the user to remember. The whole database backup and a recovery option are available for ease of use. Passwords are kept hidden, making it difficult for shoulder surfing. Password Safe is licensed under the Artistic license.

Features

- Ease of use: The GUI is very simple, enabling even a beginner to use it.
- Multiple databases: It supports multiple databases. And different databases can be created for each category.
- Safe decryption: The decryption of the password database is done in the RAM, which leaves no trace of the login details in the hard drive.
- Password generator: Supports the generation of strong, lengthy passwords.
- Advanced search: The advanced search function allows users to search within the different fields.
- Security: Uses the Twofish algorithm to encrypt the database.

Post-Reading Questions:

1. Summarize the key benefits of using a password manager. How can it address common challenges associated with password management?
2. What security features do password managers typically provide, and how do they contribute to overall digital security?
3. Discuss the potential risks or drawbacks of using a password manager and how users can mitigate these concerns.
4. Reflect on how the use of a password manager aligns with best practices for secure password management. What additional measures can individuals take to enhance their digital security?
5. In what ways can password managers contribute to the convenience and efficiency of managing numerous passwords?

Tasks and Activities:

1. **Password Manager Exploration:** Explore and compare different password manager tools available in the market. Evaluate their features, user interface, and security measures. Create a report or presentation on your findings.
2. **Password Manager Tutorial:** Create a step-by-step tutorial on how to set up and use a specific password manager. Include screenshots and practical tips for users.

3. **Password Strength Analysis:** Use a password manager to analyze the strength of passwords for various accounts. Discuss how the manager helps in creating and maintaining strong, unique passwords.

CONFIGURING FIREWALL ON COMPUTER

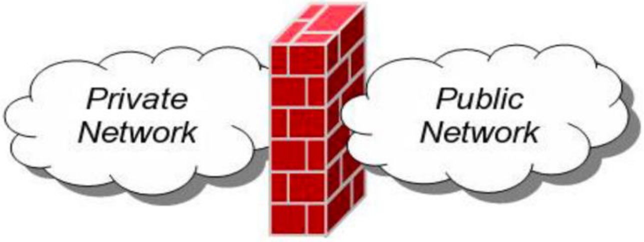
UNIT 15

1. Have you ever used or configured a firewall on a Mac computer? What was your experience?
2. What is your understanding of the purpose and function of a firewall in the context of computer security?
3. How important do you think it is to have a firewall on your Mac, considering the security landscape of the digital world?
4. What challenges or concerns might you anticipate when working with a firewall on a Mac computer?

CONFIGURING FIREWALL ON MAC COMPUTER

Every Mac ships with a built-in firewall - a service that can be configured to disallow information from entering your Mac. But what is a firewall, and why do you need to use it on your Mac?

Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac. This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.

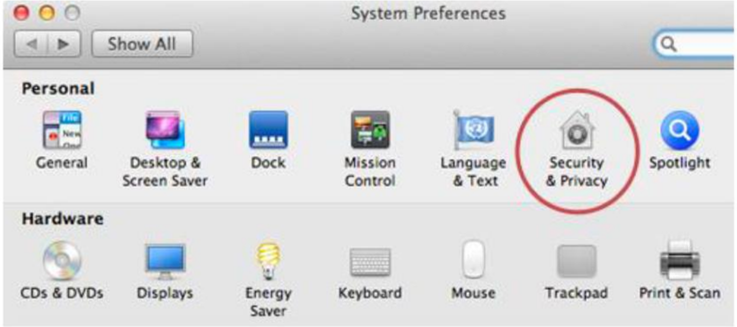


A firewall can help prevent bad packets from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans.

Turning on and Configuring the Mac OS X Firewall

Here's how to turn on and configure your Mac's built-in firewall:

1. From the Apple menu, select **System Preferences**. The window shown below appears.



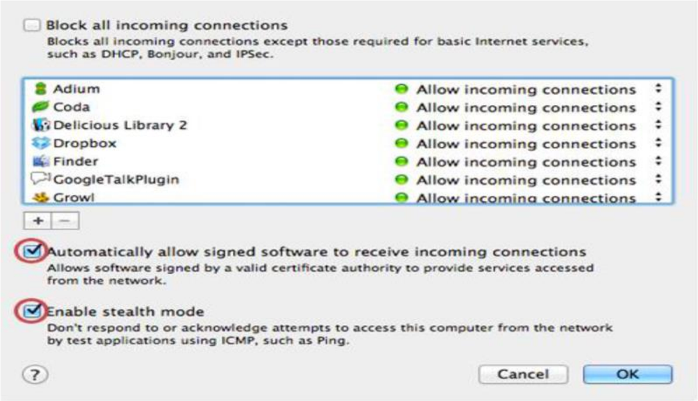
2. Select **Security & Privacy**.

3. Click the **Firewall** tab.

4. Click the lock icon and authenticate with your administrator username and password. The window shown below appears.

5. Click **Start**. The firewall turns on - you'll know it's enabled when you see the green light and the **Firewall: On** message, as shown below.

Click **Advanced**. The window shown below appears.



☐ Block all incoming connections

Blocks all incoming connections except those required for basic Internet services, such as DHCP, Bonjour, and IPSec.

Adium	● Allow incoming connections
Coda	● Allow incoming connections
Delicious Library 2	● Allow incoming connections
Dropbox	● Allow incoming connections
Finder	● Allow incoming connections
GoogleTalkPlugin	● Allow incoming connections
Growl	● Allow incoming connections

☑ Automatically allow signed software to receive incoming connections

Allows software signed by a valid certificate authority to provide services accessed from the network.

☑ Enable stealth mode

Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

7. Select the **Automatically allow signed software to receive incoming connections** checkbox. This allows the applications on your Mac to communicate with the outside world.

8. Select the **Enable stealth mode** checkbox. This prevents your Mac from responding to port scans and ping requests.

9. Click **OK** to close the *Advanced* settings.

10. Close System Preferences. Your Mac is now protected by the built-in firewall!

Post-Reading Questions:

1. Summarize the key functions of the firewall on a Mac computer. How does it contribute to the security of the operating system?
2. Explain the significance of configuring firewall settings based on the specific needs and usage patterns of your Mac.
3. Discuss any limitations or drawbacks of using the built-in firewall on a Mac and how users can address them.
4. Reflect on the potential risks of not having a firewall or misconfiguring firewall settings on a Mac. How might it impact the security of your system?
5. How can users strike a balance between maintaining a secure system with a firewall and ensuring smooth access to necessary network resources on a Mac.

Tasks and Activities:

Comparison with Other Firewalls: Research and compare the built-in firewall on a Mac with other third-party firewall solutions available for macOS. Create a pros and cons list and discuss which might be suitable for different scenarios.
Mac Firewall Presentation: Assign groups to create presentations explaining different aspects of the firewall on a Mac, including its features, configuration options, and security implications.

.
UNIT 16

Pre-Reading Questions:

1. Have you ever used Windows Firewall in Windows 7? What was your experience with it?
2. What do you think is the purpose of a firewall in an operating system?
3. How important do you consider firewall settings in ensuring the security of your computer?
4. What challenges or concerns do you anticipate when working with a firewall on your operating system?

WORKING WITH WINDOWS FIREWALL IN WINDOWS7

Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the **Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**. The main difference between them is the complexity of the rules configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service.

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This features ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be configured on different interfaces. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

- Public
- Home/Work - private network
- Domain - used within a domain

We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall** By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature trough Windows Firewall" option.

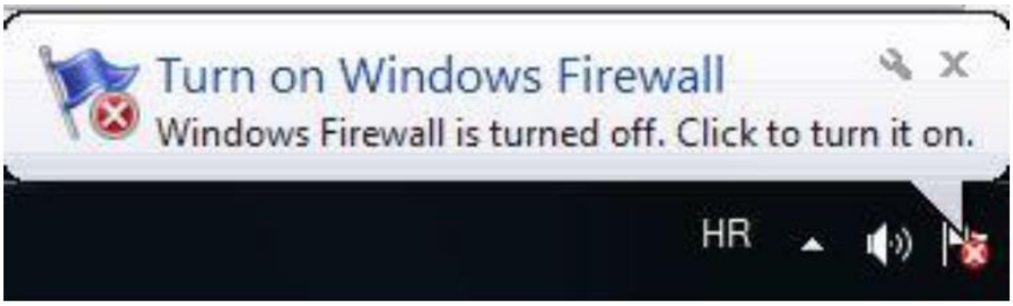
Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.

Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.



Turn on Windows Firewall

Windows Firewall is turned off. Click to turn it on.

Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security, which will be covered in next section.

Post-Reading Questions:

1. Summarize the key functions of Windows Firewall in Windows 7. How does it contribute to the security of the operating system?

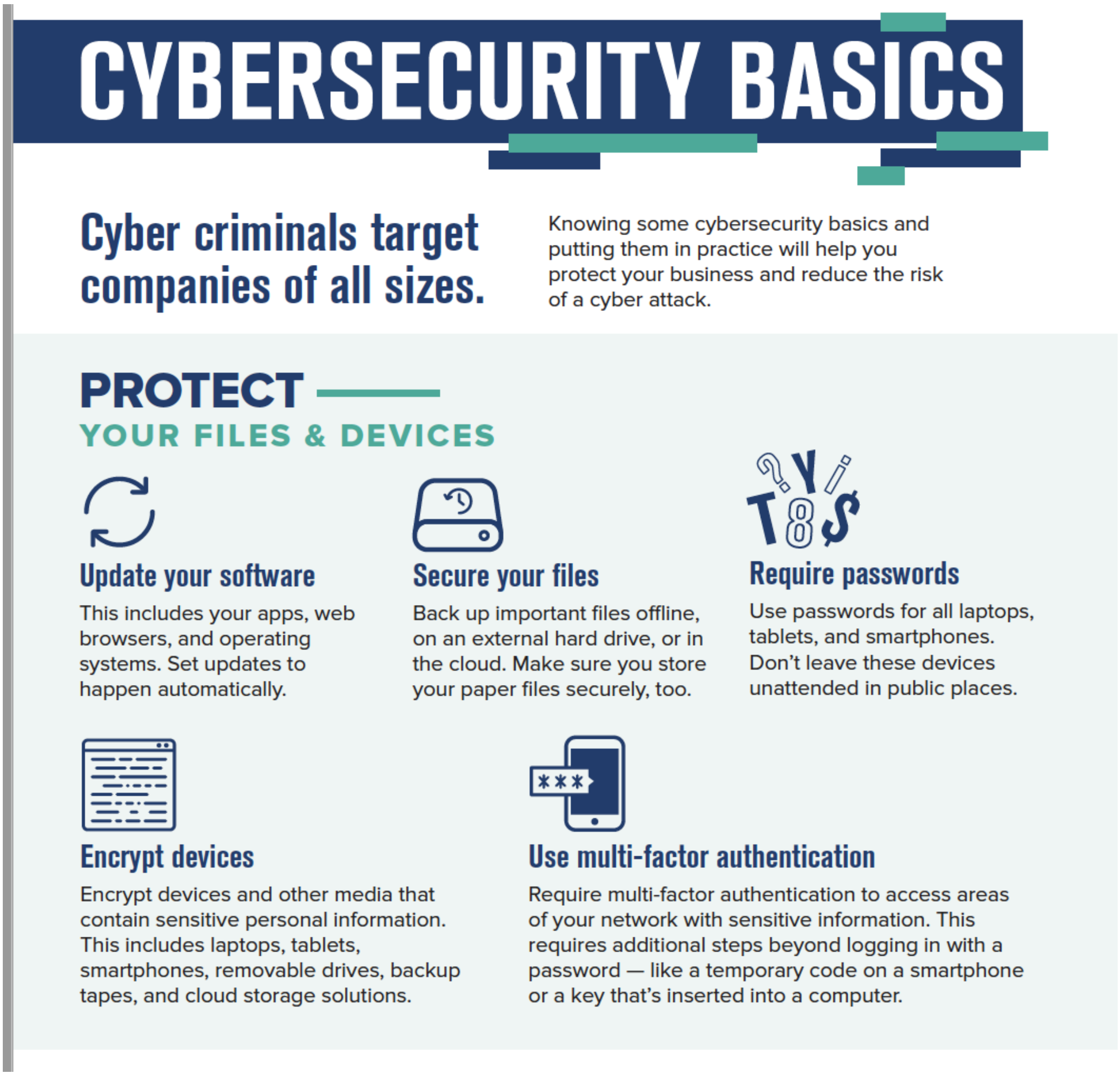
2. Explain the significance of configuring firewall settings based on the specific needs and usage patterns of your computer.
3. Discuss any limitations or drawbacks of using Windows Firewall and how users can address them.
4. Reflect on the potential risks of not having a firewall or misconfiguring firewall settings. How might it impact the security of your system?
5. How can users strike a balance between maintaining a secure system with a firewall and ensuring smooth access to necessary network resources?

Tasks and Activities:

1. **Security Audit and Review:** Conduct a security audit of a Windows 7 system, reviewing the firewall settings. Identify areas for improvement and discuss best practices for maintaining a secure configuration.
2. **Comparison with Other Firewalls:** Research and compare Windows Firewall in Windows 7 with other third-party firewall solutions. Create a pros and cons list and discuss which might be suitable for different scenarios.
3. **Windows Firewall Presentation:** Create presentations explaining different aspects of Windows Firewall in Windows 7, including its features, configuration options, and security implications.

CASE STUDY 1

1. What are the key principles and objectives of cybersecurity? Provide examples of how these principles can be applied in real-world scenarios.
2. How does encryption contribute to data security? Explore different encryption algorithms and their effectiveness in protecting data at rest and in transit.
3. What are the ethical considerations surrounding cybersecurity? Explore the ethical dilemmas faced by cybersecurity professionals and the potential consequences of unethical behavior in the field.



CYBERSECURITY BASICS

Cyber criminals target companies of all sizes.

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT

YOUR FILES & DEVICES

Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Case study task 1: Research and analyze the impact of a recent cyber attack on a well-known organization. Identify the vulnerabilities that were exploited and assess the potential repercussions for the organization and its customers.

Case study task 2: Study the evolution of malware, from simple computer viruses to sophisticated ransomware attacks. Assess the impact of malware on individuals, businesses, and society as a whole.

Case study task 3: Investigate the role of employee training and awareness programs in mitigating cyber threats. Analyze examples where employee negligence or lack of understanding led to data breaches, and propose strategies for improving cybersecurity awareness within organizations.

Activity 1: Conduct a risk assessment for a small business, identifying potential cyber threats and vulnerabilities. Develop a plan to mitigate these risks and prioritize the necessary security measures.

Activity 2: Create a computer security incident response plan for a fictitious organization. Identify the steps to be taken in the event of a cybersecurity incident, such as detecting, containing, and recovering from a breach.

Activity3: Conduct a vulnerability scan of a networked environment using appropriate tools. Interpret the scan results and propose remediation measures to address the identified vulnerabilities.

CASE STUDY 2

Case Study: Securing Your Business Wireless Network

Introduction:

XYZ Corporation, a thriving business with a growing workforce, relies heavily on a robust wireless network infrastructure to facilitate seamless communication, data access, and collaboration. Recognizing the critical importance of securing sensitive business information, the IT department has implemented a comprehensive strategy based on an informative infographic.

Infographic Overview:

The infographic provides an overview of key components for securing the business wireless network. It covers aspects such as encryption protocols, access controls, device management, and user education. The objective is to ensure a secure and reliable wireless environment that aligns with the company's commitment to safeguarding confidential data.

Current Scenario:

1. Wireless Network Architecture:

- XYZ Corporation's wireless network encompasses multiple access points across various office locations, supporting both employee and guest networks.

2. **Current Security Measures:**

- The existing security measures include WPA2 encryption, password-protected access points, and a basic access control list. However, recent security concerns have prompted a reevaluation of the current strategy.

Challenges and Concerns:

1. Increasing Cyber Threats:

- The rise in cyber threats targeting businesses underscores the need for an upgraded wireless security infrastructure.

2. **Growing Workforce:**

- With an expanding workforce, managing access and ensuring secure connections for all devices has become increasingly complex.

3. BYOD (Bring Your Own Device) Culture:

- The growing trend of employees bringing personal devices to work poses potential security risks and challenges in device management.

Infographic-Based Strategy:

1. Encryption Upgrade:

- The infographic recommends upgrading to WPA3 encryption, which provides stronger security features, including improved protection against brute-force attacks and enhanced encryption protocols.

2. Access Control Enhancements:

- Implement role-based access controls (RBAC) to ensure that employees have access only to the resources necessary for their roles. Additionally, explore the use of a RADIUS server for centralized authentication.

3. Device Management Solutions:

- Integrate Mobile Device Management (MDM) solutions to streamline the management of company-owned and BYOD devices. This includes enforcing security policies, managing software updates, and remotely wiping devices if necessary.

4. User Education and Awareness:

- Develop an ongoing user education program based on the infographic's recommendations. This includes raising awareness about the importance of strong passwords, recognizing phishing attempts, and reporting suspicious activities.

Implementation Plan:

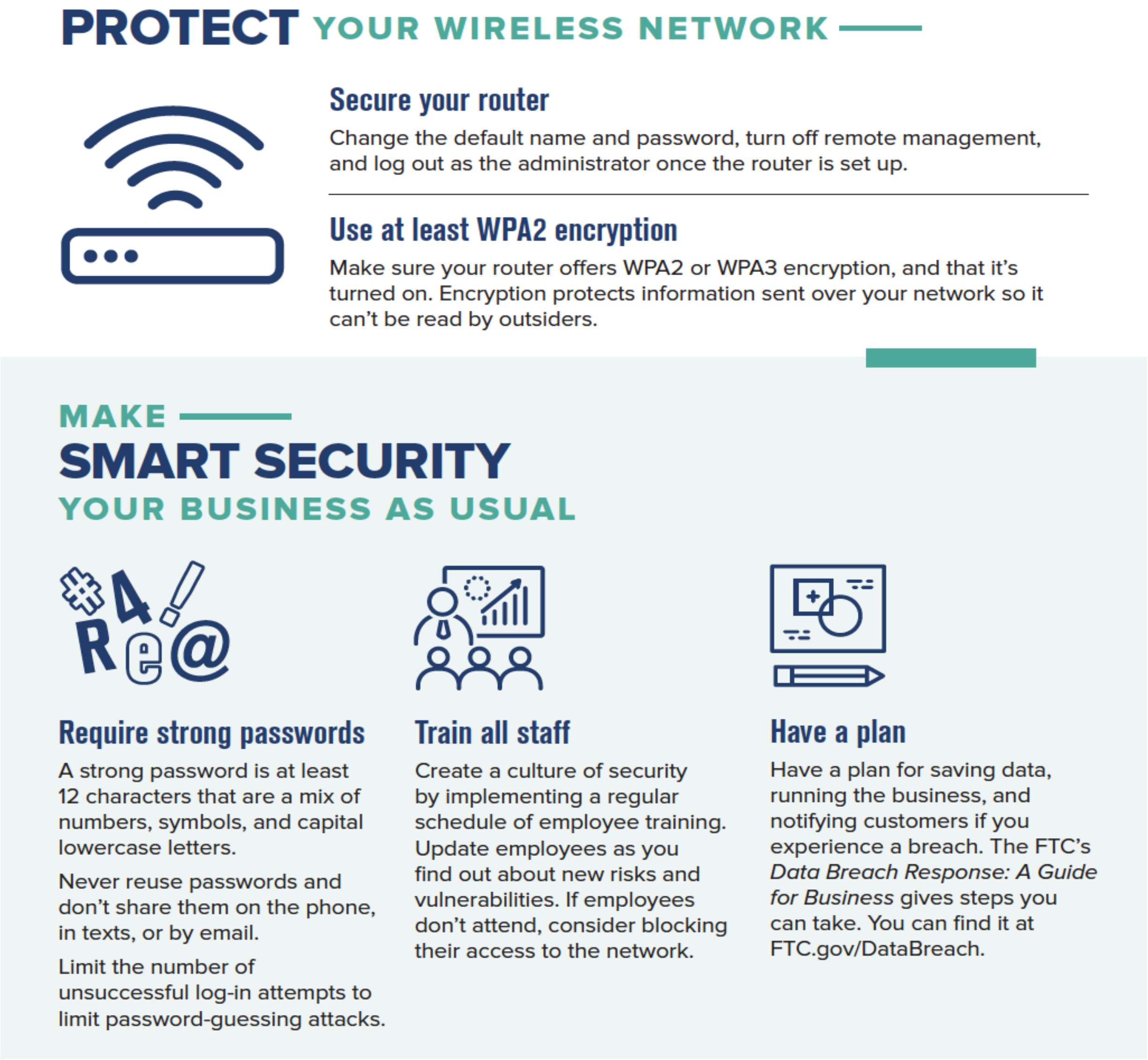
1. Phase 1: Encryption Upgrade (Month 1-2): - Schedule a comprehensive upgrade of encryption protocols on all access points to WPA3. Conduct thorough testing to ensure minimal disruption to operations.
2. Phase 2: Access Control Implementation (Month 3-4): Roll out role-based access controls gradually. Collaborate with department heads to define role profiles and access requirements. Communicate changes to employees and provide necessary training.
3. Phase 3: Device Management Integration (Month 5-6): - Integrate a Mobile Device Management solution to manage devices efficiently. Implement policies for device security, application management, and remote device wiping. Conduct user training sessions on MDM usage.
4. Phase 4: User Education (Ongoing): - Launch an ongoing user education program, utilizing the infographic's content. This includes regular security awareness sessions, email campaigns, and distributing printed materials throughout the office.

Results and Monitoring:

1. Regular Security Audits: - Conduct regular security audits to assess the effectiveness of the implemented measures. This includes penetration testing, vulnerability assessments, and continuous monitoring of network activities.
2. User Feedback and Incident Reporting: - Encourage employees to provide feedback on the new security measures and report any suspicious activities promptly. Implement a secure and anonymous reporting system.

Conclusion:

By adopting a phased approach based on the recommendations provided in the infographic, XYZ Corporation aims to enhance the security posture of its business wireless network. This proactive strategy aligns with industry best practices, ensuring a resilient and protected digital environment for the organization.



PROTECT YOUR WIRELESS NETWORK

Secure your router

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan

Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC's *Data Breach Response: A Guide for Business* gives steps you can take. You can find it at FTC.gov/DataBreach.

CASE STUDY 3

1. Framework Overview:

What are the key components highlighted in the NIST Cybersecurity Framework infographic? How does the infographic visually represent the core functions of the NIST framework?

2. Core Functions:

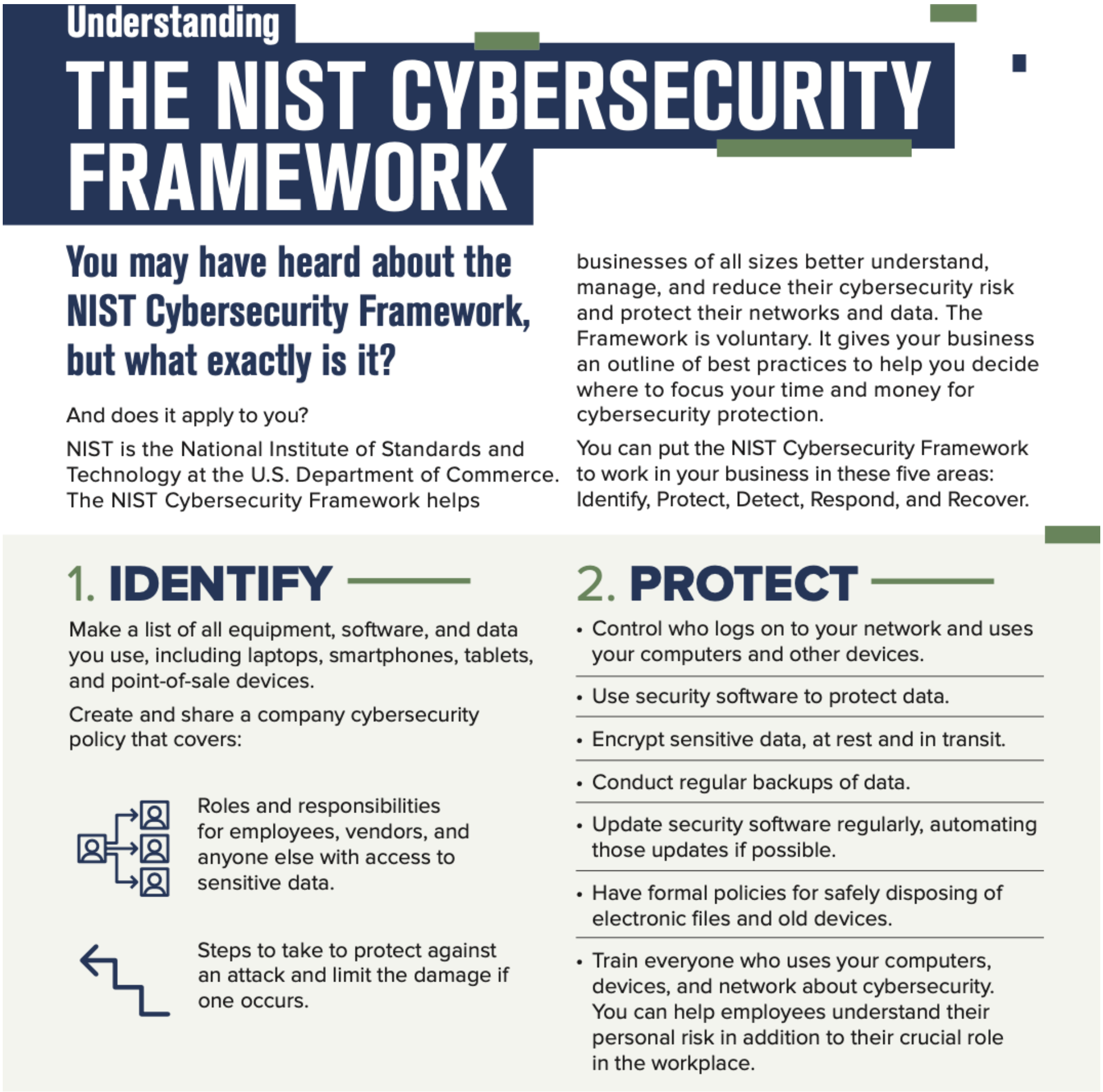
What are the primary core functions outlined in the NIST Cybersecurity Framework, and how are they depicted in the infographic?
Can you identify any specific cybersecurity activities associated with each core function?

3. Implementation Tiers:

If the infographic includes information on implementation tiers, how are these tiers visually represented?
What do the different implementation tiers signify in terms of an organization's cybersecurity maturity?

4. Identifying Assets and Risks:

Does the infographic provide insights into the importance of identifying and prioritizing assets and risks?
How are asset management and risk assessment visually represented in the context of the NIST framework?



Understanding THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:

Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.

Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

Case Study Tasks: Implementing the NIST Cybersecurity Framework

Task 1: Current State Assessment
- Conduct a comprehensive assessment of the organization's current cybersecurity posture.
- Identify existing cybersecurity practices, policies, and controls in place.
- Document any recent cybersecurity incidents and their impact on the organization.

Task 2: Mapping to NIST Framework
- Use the NIST Cybersecurity Framework to map the organization's current cybersecurity practices to the core functions (Identify, Protect, Detect, Respond, Recover).
- Identify gaps and areas where the organization aligns well with the framework.

Task 3: Determining Priorities and Risks
- Prioritize cybersecurity functions and activities based on the organization's specific risks and business objectives.
- Conduct a risk assessment to identify critical assets, vulnerabilities, and potential threats.

Task 4: Establishing Implementation Tiers
- Evaluate the organization's current cybersecurity maturity and determine the appropriate implementation tier.
- Define a roadmap for moving to a higher implementation tier based on the organization's goals and resources.

Task 5: Developing Action Plans
- Develop detailed action plans for each core function, outlining specific tasks, responsible parties, and timelines.
- Include measures for protecting, detecting, responding to, and recovering from cybersecurity incidents.

These case study tasks are designed to guide the practical application of the NIST Cybersecurity Framework within an organization, fostering a systematic and strategic approach to enhancing cybersecurity measures.

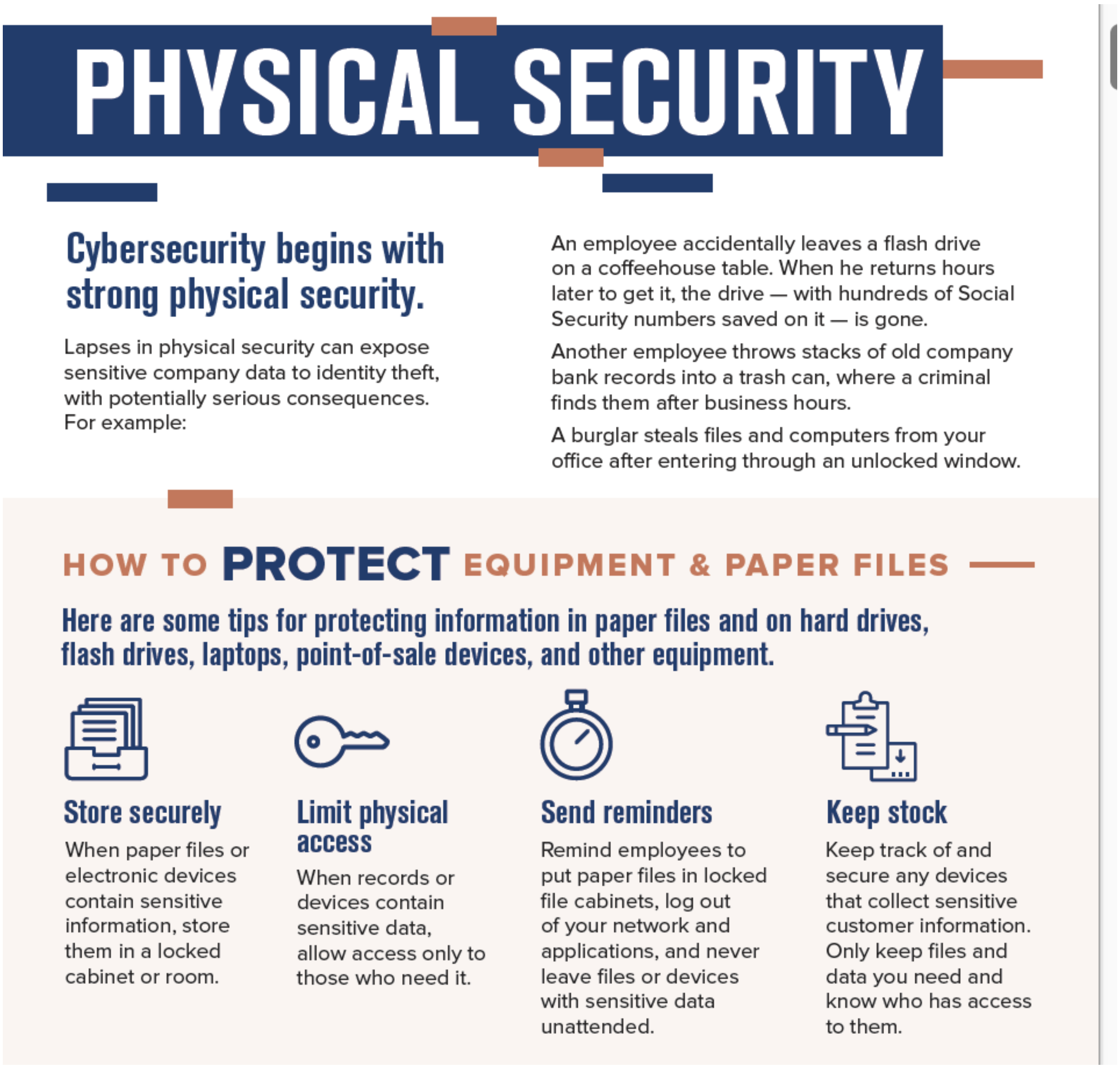
CASE STTUDY 4
PHYSICAL SECURITY (equipment and paper files)
Discussion Questions

1. Overview of Physical Security:
-What is the main focus or theme of the physical security infographic?
- Can you identify the key elements or components highlighted in the infographic?

2. Security Layers:
- Does the infographic present different layers or aspects of physical security?
- How do these layers work together to create a comprehensive security strategy?

3. Access Control Measures:
- Are there specific access control measures featured in the infographic? What methods or technologies are highlighted?
- How do access control measures contribute to the overall physical security of a facility?

4. Surveillance and Monitoring:
- Does the infographic emphasize the role of surveillance and monitoring in physical security?
- What types of surveillance technologies or practices are depicted?



PHYSICAL SECURITY

Cybersecurity begins with strong physical security.

Lapses in physical security can expose sensitive company data to identity theft, with potentially serious consequences. For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive — with hundreds of Social Security numbers saved on it — is gone.

Another employee throws stacks of old company bank records into a trash can, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

Store securely

When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

Limit physical access

When records or devices contain sensitive data, allow access only to those who need it.

Send reminders

Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

Keep stock

Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.

Case Study Tasks: Enhancing Physical Security Measures

These case study tasks are designed to guide the organization through a systematic process of assessing, enhancing, and maintaining physical security measures. They cover various aspects, from technology integration to stakeholder communication, fostering a comprehensive approach to physical security.

Task 1: Current Physical Security Assessment

- Conduct a comprehensive assessment of the organization's current physical security measures.
- Identify existing security layers, access control systems, surveillance technologies, and emergency response protocols.

Task 2: Threat and Vulnerability Analysis

- Perform a threat and vulnerability analysis specific to the organization's physical environment.

- Identify potential threats, assess vulnerabilities, and prioritize areas requiring immediate attention.

Task 3: Access Control System Evaluation
- Evaluate the effectiveness of the current access control system.
- Identify strengths and weaknesses, and propose enhancements or updates to align with industry best practices.

Task 4: Surveillance Technology Audit
- Audit the organization's surveillance technologies, including cameras and monitoring systems.
- Determine if the current technology meets the organization's needs and recommend any necessary upgrades.

Task 5: Security Personnel Training and Evaluation
- Assess the training programs for security personnel.
- Develop a plan to enhance training and evaluate the proficiency of security personnel in responding to security incidents.

Task 6: Technology Integration Plan
- Develop a plan for integrating advanced technologies into existing physical security measures.
- Explore possibilities such as smart access control systems, biometrics, and artificial intelligence for improved security.

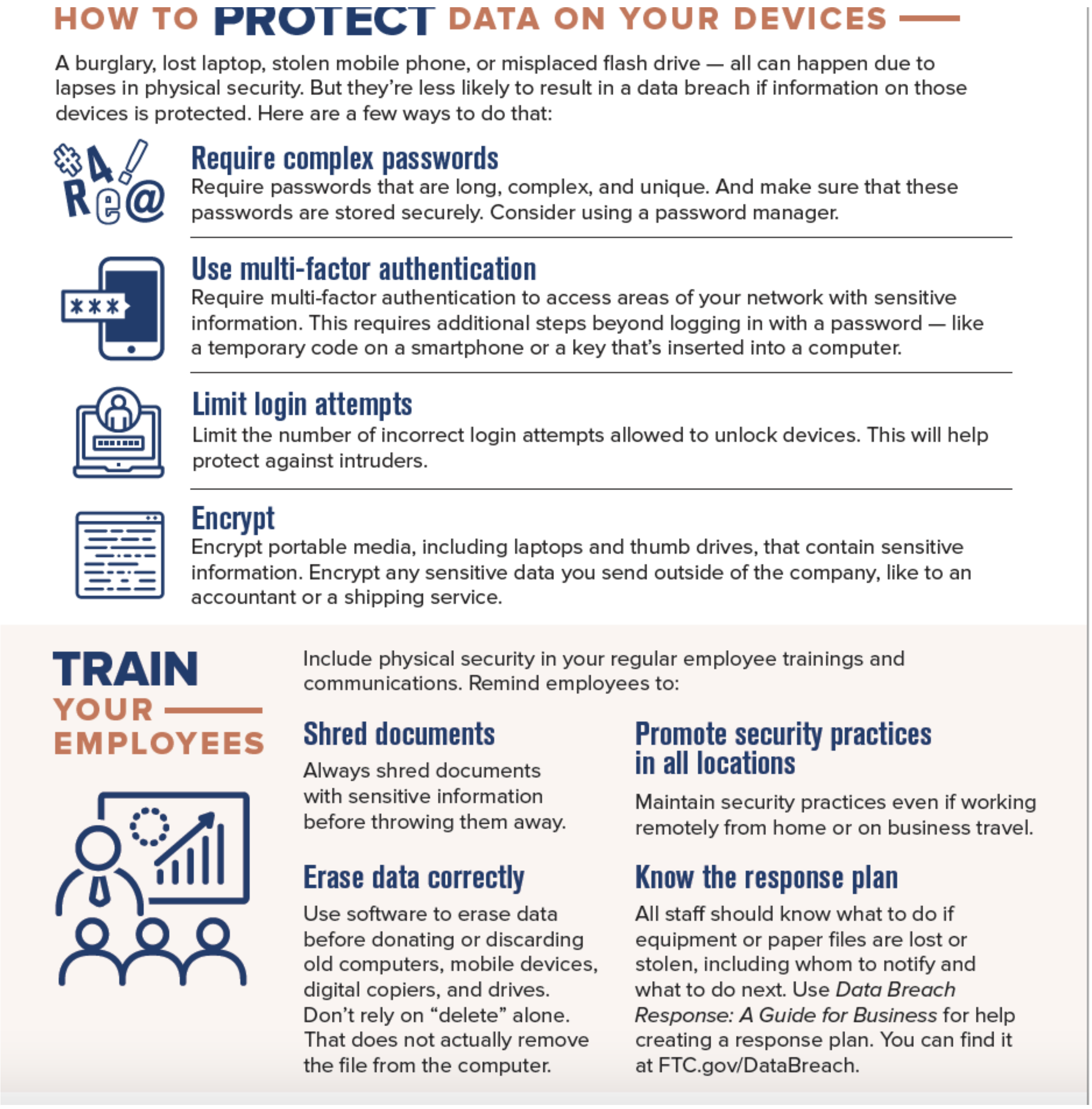
Task 7: Continuous Improvement Plan
- Establish a continuous improvement plan for physical security measures.
- Implement regular reviews, assessments, and updates to adapt to evolving threats and organizational changes.

Task 8: Stakeholder Communication and Buy-In
- Develop a communication plan to engage key stakeholders, including employees, management, and external partners.
- Seek buy-in for proposed physical security enhancements and communicate the importance of a secure environment.

CASE STUDY 5
PHYSICAL SECURITY (protecting data and devises)

Discussion Questions:

1. How does the infographic illustrate the concept of layered physical security?
2. Can you identify specific layers and their respective functions?
3. Access Control Technologies:
4. What access control technologies are highlighted in the infographic?
5. How do these technologies contribute to restricting unauthorized entry?
6. Surveillance Methods:
7. How is the role of surveillance in physical security depicted in the infographic?
8. Can you identify various surveillance methods presented?
9. Security Personnel:
10. What emphasis does the infographic place on the role of security personnel?



HOW TO PROTECT DATA ON YOUR DEVICES

A burglary, lost laptop, stolen mobile phone, or misplaced flash drive — all can happen due to lapses in physical security. But they're less likely to result in a data breach if information on those devices is protected. Here are a few ways to do that:

Require complex passwords

Require passwords that are long, complex, and unique. And make sure that these passwords are stored securely. Consider using a password manager.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Limit login attempts

Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.

Encrypt

Encrypt portable media, including laptops and thumb drives, that contain sensitive information. Encrypt any sensitive data you send outside of the company, like to an accountant or a shipping service.

TRAIN YOUR EMPLOYEES

Include physical security in your regular employee trainings and communications. Remind employees to:

Shred documents

Always shred documents with sensitive information before throwing them away.

Erase data correctly

Use software to erase data before donating or discarding old computers, mobile devices, digital copiers, and drives. Don't rely on "delete" alone. That does not actually remove the file from the computer.

Promote security practices in all locations

Maintain security practices even if working remotely from home or on business travel.

Know the response plan

All staff should know what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. Use *Data Breach Response: A Guide for Business* for help creating a response plan. You can find it at FTC.gov/DataBreach.

These case study tasks are designed to guide the organization through the practical implementation of physical security measures for data and devices, drawing insights from the provided infographic.

Task 1: Infographic Analysis:
Analyze the provided infographic on physical security for data and devices.
Identify key elements such as access controls, surveillance, and emergency response depicted in the infographic.

Task 2: Current Security Assessment:
Conduct a thorough assessment of the organization's current physical security measures for data and devices.
Compare existing practices with those highlighted in the infographic to identify gaps.

Task 3: Access Control Enhancement:
Implement improvements to the access control system based on the recommendations from the infographic.
Consider measures such as biometric access, smart card authentication, or role-based access controls.

Task 4: Surveillance Technology Upgrade:
Upgrade surveillance technologies in alignment with the infographic's suggestions.
Consider advancements such as high-resolution cameras, analytics, and real-time monitoring.

Task 5: Security Personnel Training:
Enhance training programs for security personnel, incorporating elements highlighted in the infographic.
Include modules on emergency response, situational awareness, and adherence to security protocols.

CASE STUDY 6
Tech Support Scams

Discussion Questions:
Scammer techniques:

1. How does the infographic illustrate the techniques used by scammers in tech support scams?
2. Can you identify specific tactics scammers employ to gain victims' trust?

Credit Card Information:

1. How is the process of extracting credit card information portrayed in the infographic?
2. What are the common methods scammers use to convince victims to provide their credit card details?

Remote Access to Computer:

1. Explore the infographic's depiction of scammers gaining remote access to victims' computers.
2. What vulnerabilities or tactics are exploited to convince individuals to grant remote access?

Installation of Malware:

1. How is the installation of malware presented in the infographic?
2. Can you identify the potential consequences and risks associated with the installation of malware on a victim's computer?

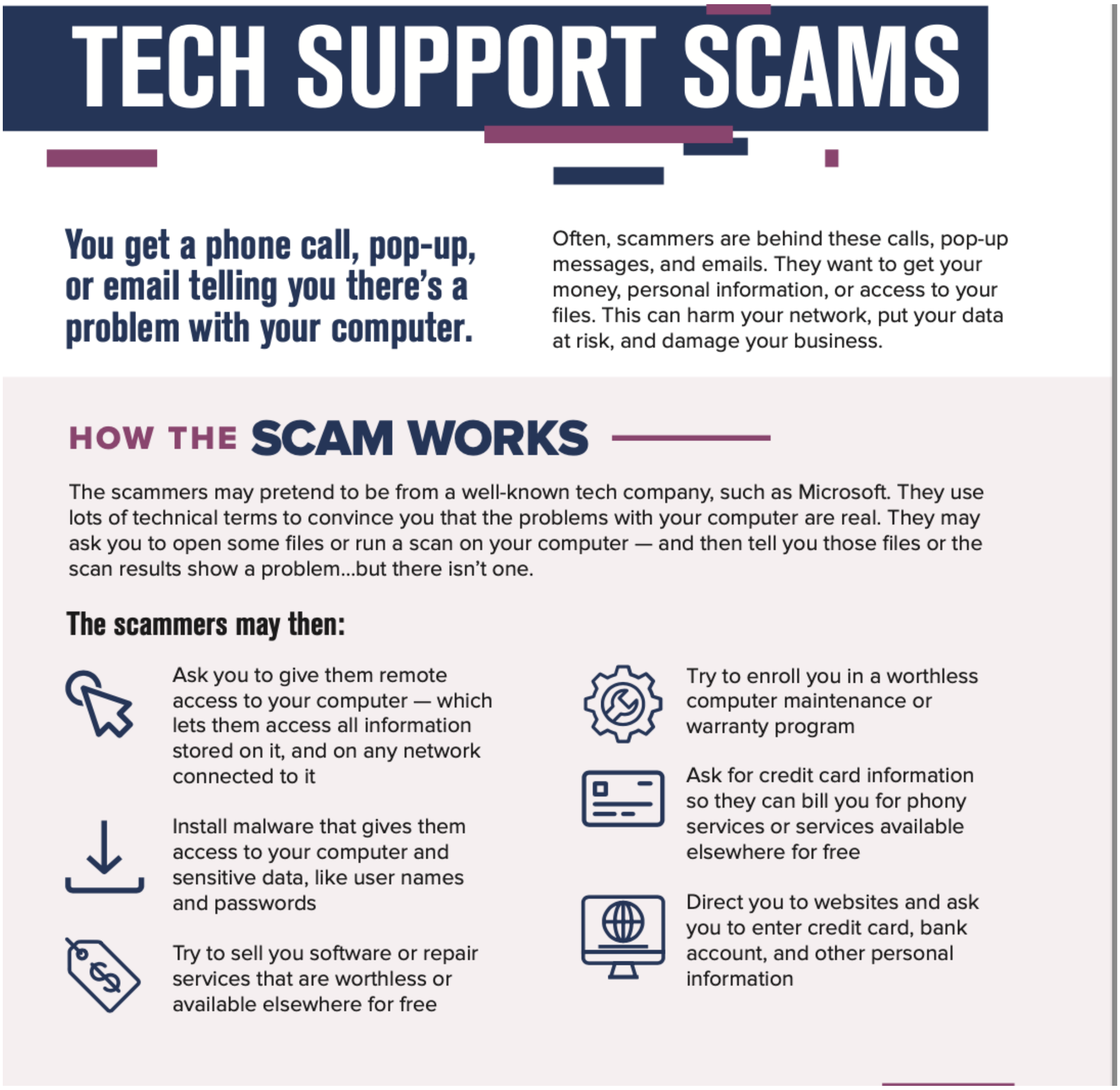
Case Study Tasks: Understanding and Preventing Tech Support Scams

These case study tasks aim to guide participants through a comprehensive analysis of the tech support scam infographic, fostering understanding, and encouraging the development of preventive measures and awareness campaigns.

Task 1: Infographic Analysis:
Examine the provided infographic on tech support scams.
Identify key elements and visual representations that explain how scammers operate.

Task 2: Scammer Techniques Analysis:

List and analyze specific techniques used by scammers to deceive individuals in tech support scams.
Explore the psychological aspects and social engineering tactics highlighted in the infographic.



TECH SUPPORT SCAMS

You get a phone call, pop-up, or email telling you there's a problem with your computer.

Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

HOW THE SCAM WORKS

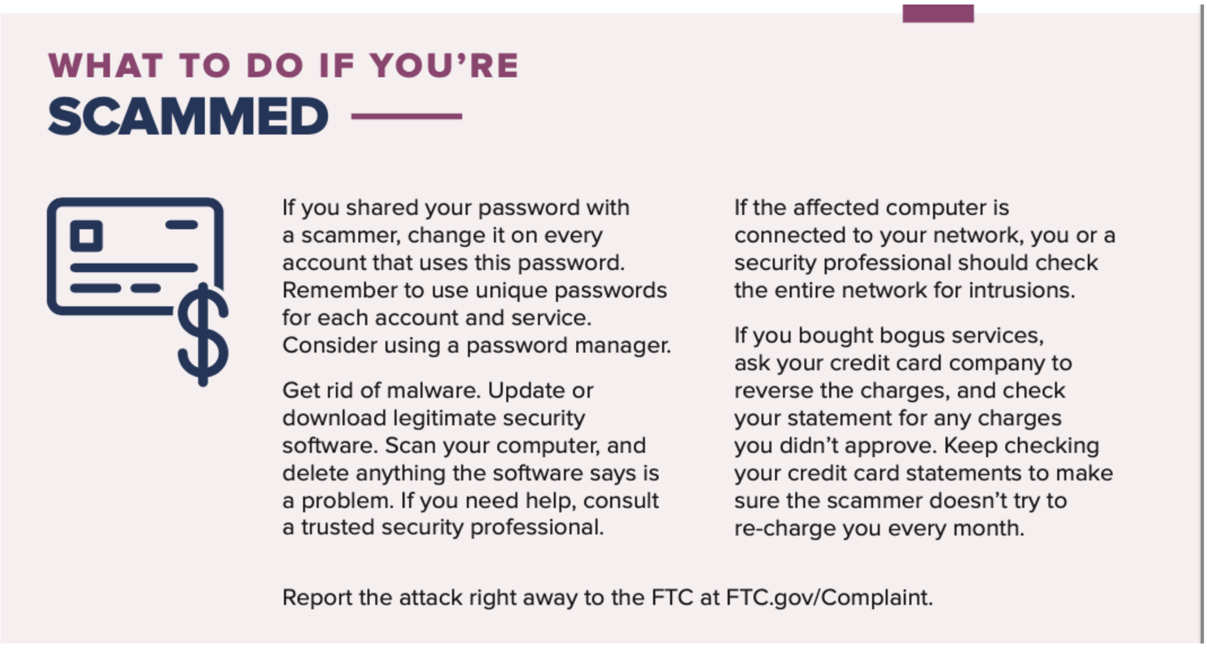
The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn't one.

The scammers may then:

- Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it
- Install malware that gives them access to your computer and sensitive data, like user names and passwords
- Try to sell you software or repair services that are worthless or available elsewhere for free
- Try to enroll you in a worthless computer maintenance or warranty program
- Ask for credit card information so they can bill you for phony services or services available elsewhere for free
- Direct you to websites and ask you to enter credit card, bank account, and other personal information

Task 3: Credit Card Information Process:
Investigate how the infographic illustrates the process of scammers extracting credit card information.
Identify the stages involved and potential vulnerabilities that victims may overlook**.**

Task 4: Remote Access Illustration:
Examine the infographic's depiction of scammers gaining remote access to victims' computers.
Discuss the methods scammers use to convince individuals to grant remote access.



WHAT TO DO IF YOU'RE

SCAMMED

If you shared your password with a scammer, change it on every account that uses this password. Remember to use unique passwords for each account and service. Consider using a password manager.

Get rid of malware. Update or download legitimate security software. Scan your computer, and delete anything the software says is a problem. If you need help, consult a trusted security professional.

If the affected computer is connected to your network, you or a security professional should check the entire network for intrusions.

If you bought bogus services, ask your credit card company to reverse the charges, and check your statement for any charges you didn't approve. Keep checking your credit card statements to make sure the scammer doesn't try to re-charge you every month.

Report the attack right away to the FTC at FTC.gov/Complaint.

Task 5: Malware Installation Process:
Explore the infographic's presentation of how scammers install malware on victims' computers. Identify the potential consequences and risks associated with the installation of malware.

Task 6: Warning Signs Identification:
Identify and discuss warning signs or red flags depicted in the infographic.
Develop a checklist that individuals can use to recognize potential tech support scams.

CASE STUDY 7

EMAIL AUTHENTIFICATION

Discussion Questions:

These discussion questions aim to foster a deeper understanding of the key concepts and practices related to email authentication as presented in the infographic, encouraging participants to explore the significance, challenges, and future trends in this critical aspect of cybersecurity.

Authentication Methods:

1. How does the infographic illustrate different methods of email authentication?
2. Can you identify specific technologies or protocols mentioned for ensuring email authenticity?

Benefits of Email Authentication:

1. Explore the benefits highlighted in the infographic regarding email authentication.
2. How can implementing strong email authentication methods enhance cybersecurity?

Email Spoofing and Phishing Mitigation:

1. Discuss how the email authentication methods presented in the infographic contribute to mitigating email spoofing and phishing.
2. Can you identify specific scenarios where these methods are particularly effective?

Sender Reputation and Trustworthiness:

1. Examine how email authentication contributes to establishing sender reputation and trustworthiness.
2. How might businesses and individuals benefit from a positive sender reputation?

Challenges in Email Authentication Implementation:

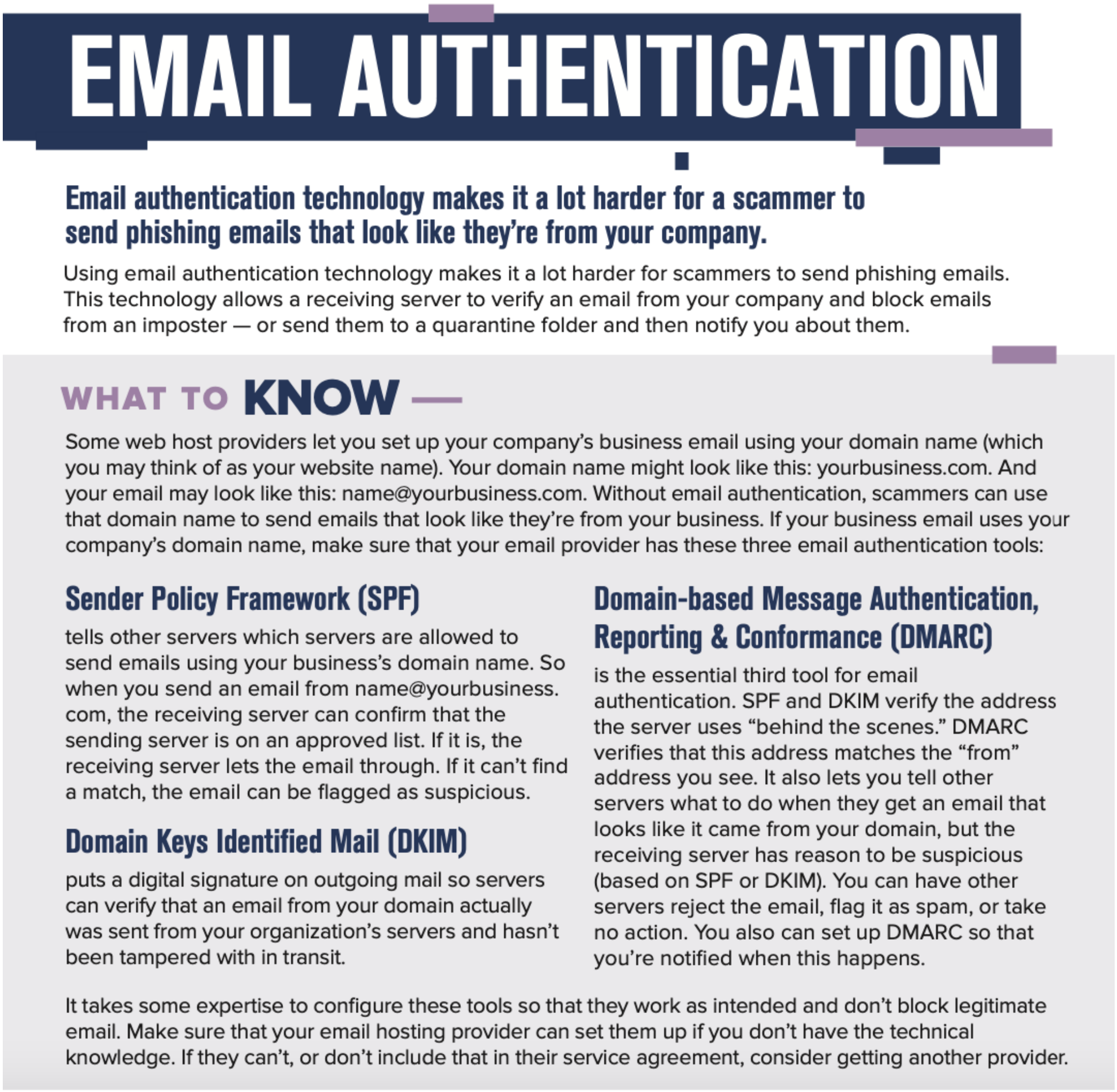
1. Identify any challenges or limitations mentioned in the infographic regarding the implementation of email authentication.
2. How can organizations address these challenges?

Implications for Business Communication:

1. Discuss the implications of email authentication for business communication.
2. How can strong email authentication practices positively impact communication within and outside an organization?

Consumer Awareness:

1. Explore the role of consumer awareness in the effectiveness of email authentication.
2. How can educating users about email authentication contribute to a safer online environment?



EMAIL AUTHENTICATION

Email authentication technology makes it a lot harder for a scammer to send phishing emails that look like they're from your company.

Using email authentication technology makes it a lot harder for scammers to send phishing emails. This technology allows a receiving server to verify an email from your company and block emails from an imposter — or send them to a quarantine folder and then notify you about them.

WHAT TO KNOW —

Some web host providers let you set up your company's business email using your domain name (which you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. Without email authentication, scammers can use that domain name to send emails that look like they're from your business. If your business email uses your company's domain name, make sure that your email provider has these three email authentication tools:

Sender Policy Framework (SPF)

tells other servers which servers are allowed to send emails using your business's domain name. So when you send an email from name@yourbusiness.com, the receiving server can confirm that the sending server is on an approved list. If it is, the receiving server lets the email through. If it can't find a match, the email can be flagged as suspicious.

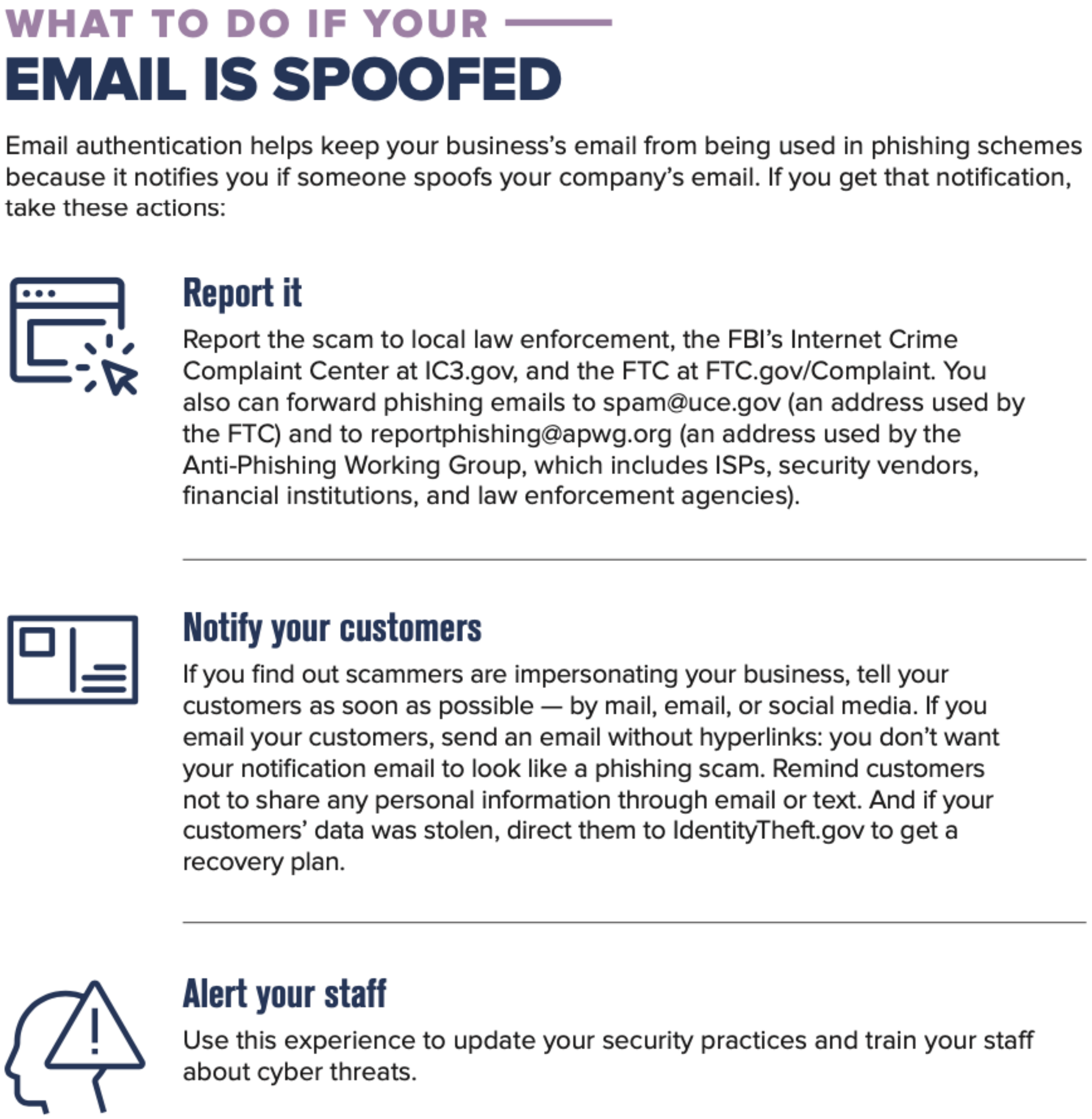
Domain Keys Identified Mail (DKIM)

puts a digital signature on outgoing mail so servers can verify that an email from your domain actually was sent from your organization's servers and hasn't been tampered with in transit.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

is the essential third tool for email authentication. SPF and DKIM verify the address the server uses "behind the scenes." DMARC verifies that this address matches the "from" address you see. It also lets you tell other servers what to do when they get an email that looks like it came from your domain, but the receiving server has reason to be suspicious (based on SPF or DKIM). You can have other servers reject the email, flag it as spam, or take no action. You also can set up DMARC so that you're notified when this happens.

It takes some expertise to configure these tools so that they work as intended and don't block legitimate email. Make sure that your email hosting provider can set them up if you don't have the technical knowledge. If they can't, or don't include that in their service agreement, consider getting another provider.



WHAT TO DO IF YOUR EMAIL IS SPOOFED

Email authentication helps keep your business's email from being used in phishing schemes because it notifies you if someone spoofs your company's email. If you get that notification, take these actions:

Report it

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

Notify your customers

If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks: you don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. And if your customers' data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

These case study tasks are designed to guide participants through a practical exploration of email authentication practices, covering implementation, challenges, benefits, and strategies for improvement based on insights from the infographic.

Task 1: Infographic Analysis:
Examine the provided infographic on email authentication.
Identify key components, protocols, and technologies highlighted in the infographic.

Task 2: Authentication Methods Exploration:
Research and elaborate on different methods of email authentication introduced in the infographic.
Compare the strengths and weaknesses of each method in ensuring email security.

Task 3: Benefits Identification:
Identify and list the benefits associated with implementing robust email authentication practices.

Discuss how these benefits contribute to overall cybersecurity and trust in email communication.

Task 4: SPF (Sender Policy Framework) Implementation:
Develop a step-by-step guide for implementing SPF (Sender Policy Framework) based on the information provided in the infographic.
Discuss potential challenges and considerations during the implementation process.

Task 5: Emerging Trends Exploration:
Research and discuss emerging trends in email authentication highlighted in the infographic.
Evaluate the potential impact of these trends on the future of email security.

Task 6: Recommendations for Future Implementation:
Based on the information provided, formulate recommendations for organizations looking to enhance their email authentication practices in the future.
Consider technological advancements and evolving threats.

CASE STUDY 8
Vendor Security

Discussion Questions:
Vendor Onboarding Process:

1. How does the infographic depict the vendor onboarding process concerning security measures?
2. What steps are highlighted to ensure that vendors align with security requirements?

Key Security Requirements for Vendors:

1. Identify and discuss the key security requirements outlined in the infographic for vendors.
2. How do these requirements contribute to overall organizational security?

Risk Assessment Strategies:

1. Explore the strategies mentioned in the infographic for assessing and managing security risks associated with vendors.
2. How can organizations effectively evaluate the security posture of their vendors?

Security Audits and Compliance:

1. Examine the role of security audits and compliance in the vendor security framework.
2. How do these measures help ensure that vendors adhere to security standards?

Data Protection Measures:

1. Discuss the measures presented in the infographic to protect sensitive data shared with vendors.
2. How can organizations balance collaboration with vendors while safeguarding confidential information?

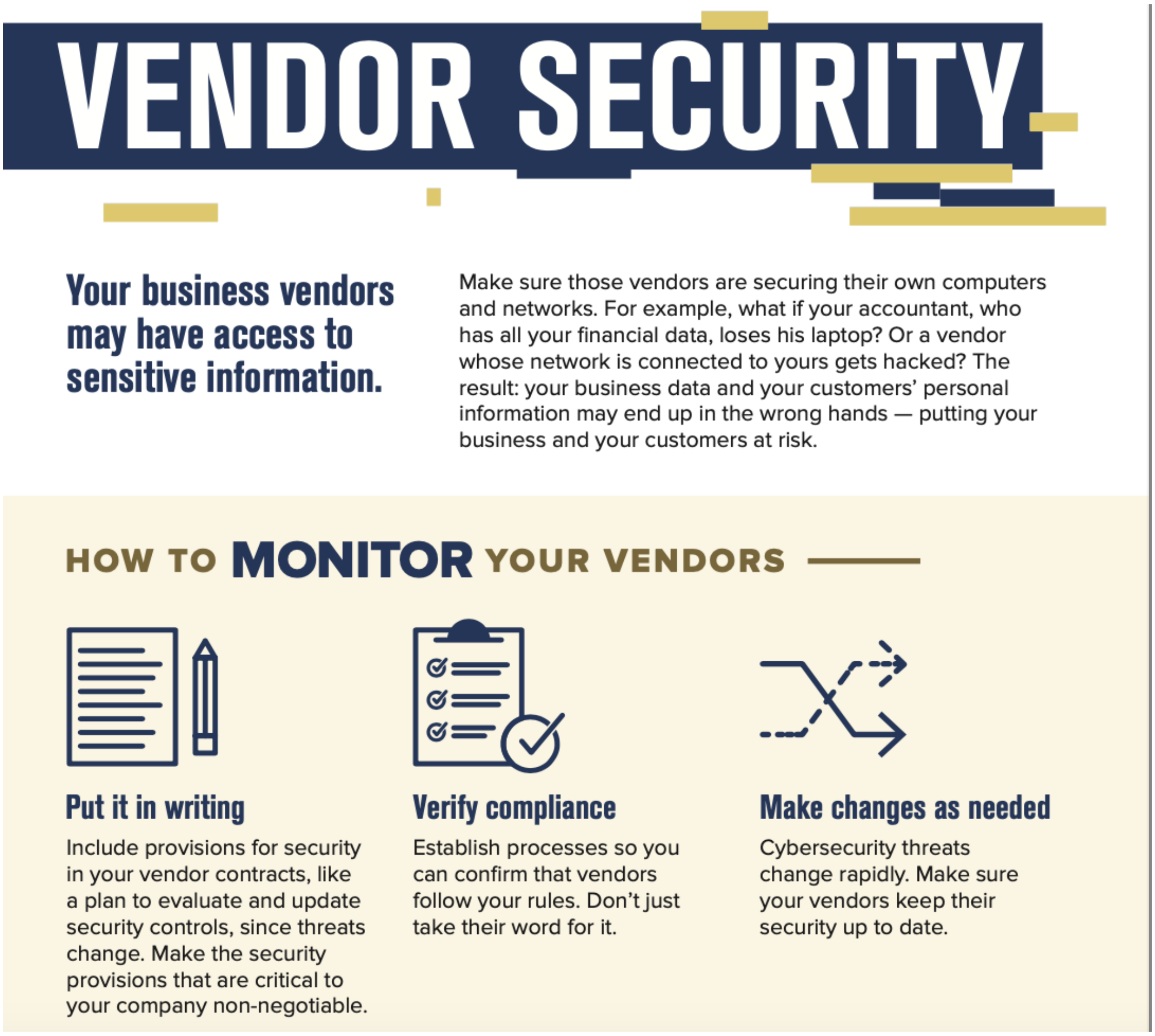
Incident Response Collaboration:

1. Explore how the infographic illustrates collaboration between organizations and vendors in incident response.
2. What proactive steps are recommended to enhance incident response capabilities in a joint setting?

Continuous Monitoring Strategies:

1. Identify strategies for continuous monitoring of vendor security highlighted in the infographic.

2. How does ongoing monitoring contribute to a dynamic and responsive security framework?



VENDOR SECURITY

Your business vendors may have access to sensitive information.

Make sure those vendors are securing their own computers and networks. For example, what if your accountant, who has all your financial data, loses his laptop? Or a vendor whose network is connected to yours gets hacked? The result: your business data and your customers' personal information may end up in the wrong hands — putting your business and your customers at risk.

HOW TO **MONITOR** YOUR VENDORS

Put it in writing

Include provisions for security in your vendor contracts, like a plan to evaluate and update security controls, since threats change. Make the security provisions that are critical to your company non-negotiable.

Verify compliance

Establish processes so you can confirm that vendors follow your rules. Don't just take their word for it.

Make changes as needed

Cybersecurity threats change rapidly. Make sure your vendors keep their security up to date.

These case study tasks are designed to guide participants through practical steps to enhance vendor security practices, leveraging insights from the provided infographic. The tasks cover areas such as onboarding, risk assessment, communication, training, and continuous improvement.

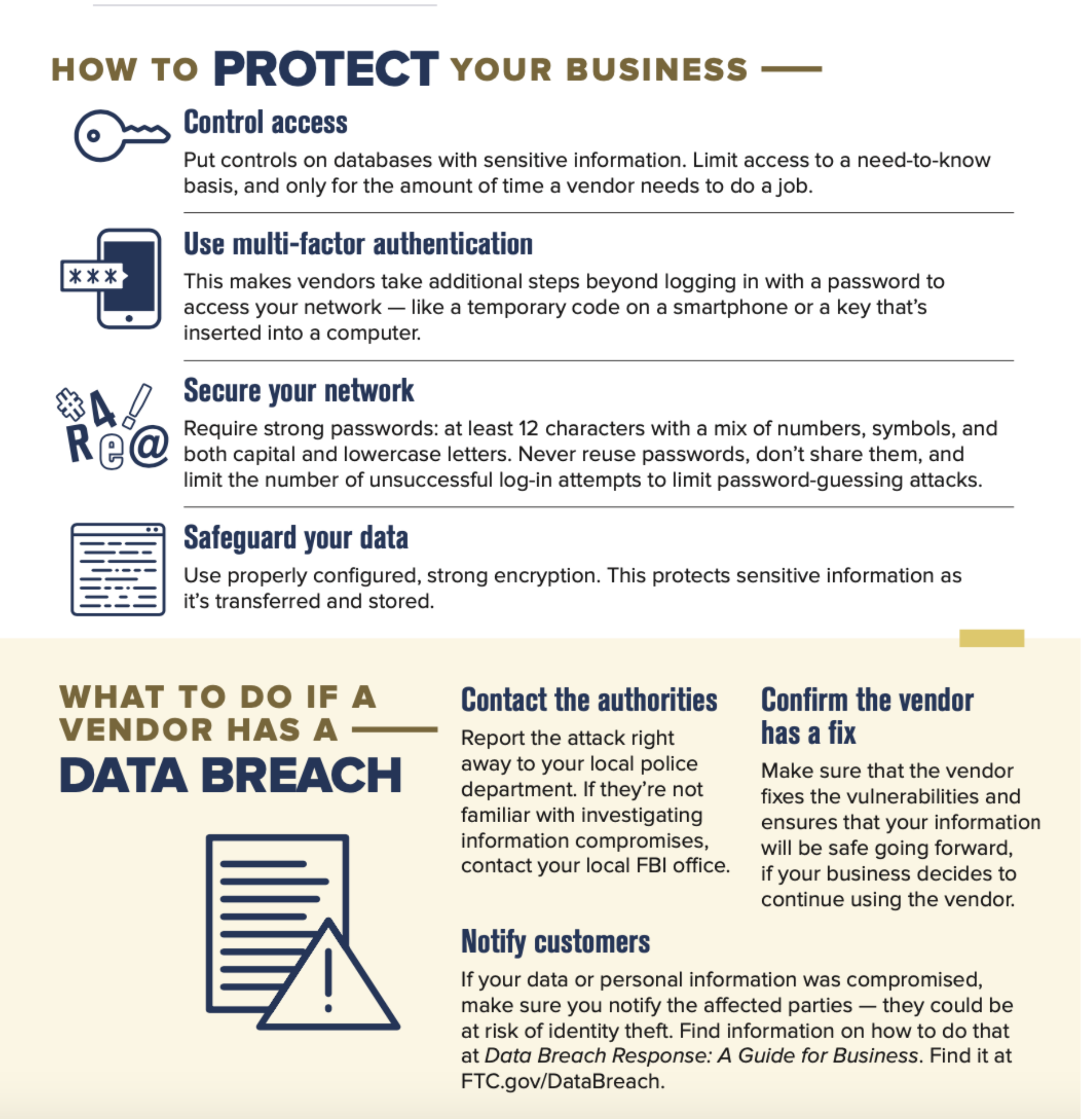
Case Study Tasks: Strengthening Vendor Security Practices

Task 1: Infographic Analysis:
Examine the provided infographic on vendor security.
Identify and list key components, practices, and recommendations highlighted in the infographic.

Task 2: Vendor Onboarding Review:
Evaluate your organization's current vendor onboarding process.
Identify areas for improvement based on the vendor onboarding practices discussed in the infographic.

Task 3: Security Requirements Assessment:
Assess the existing security requirements for vendors within your organization.
Compare and contrast these requirements with those outlined in the infographic. Identify potential gaps.

Task 4: Risk Assessment Simulation:
Conduct a simulated risk assessment for a fictional vendor, incorporating strategies presented in the infographic.
Identify potential security risks and propose mitigation measures.



HOW TO PROTECT YOUR BUSINESS

Control access

Put controls on databases with sensitive information. Limit access to a need-to-know basis, and only for the amount of time a vendor needs to do a job.

Use multi-factor authentication

This makes vendors take additional steps beyond logging in with a password to access your network — like a temporary code on a smartphone or a key that's inserted into a computer.

Secure your network

Require strong passwords: at least 12 characters with a mix of numbers, symbols, and both capital and lowercase letters. Never reuse passwords, don't share them, and limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Safeguard your data

Use properly configured, strong encryption. This protects sensitive information as it's transferred and stored.

WHAT TO DO IF A VENDOR HAS A DATA BREACH

Contact the authorities

Report the attack right away to your local police department. If they're not familiar with investigating information compromises, contact your local FBI office.

Confirm the vendor has a fix

Make sure that the vendor fixes the vulnerabilities and ensures that your information will be safe going forward, if your business decides to continue using the vendor.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business*. Find it at FTC.gov/DataBreach.

TEACHERS NOTES

UNIT 1

1. **Organize a debate:** Divide students into teams and assign them different perspectives on the impact of the internet. Have a structured debate where each team presents arguments and counterarguments. Encourage critical thinking and respectful discussion about the positive and negative effects of the internet on society.

UNIT 2

1. **Role-play activity**: Divide participants into groups representing different stakeholders of the internet infrastructure (e.g., ISPs, domain name registrars, network administrators). Each group should discuss their responsibilities, challenges, and possible collaborations to ensure a robust and reliable infrastructure.

2. **Debate:** Organize a debate on the topic, "Should the internet infrastructure be managed and regulated by a global governing body?" Encourage participants to research and present arguments for and against central governance of the internet infrastructure.

3. **Simulation exercise:** Design a simulation where participants take on the role of network administrators responsible for troubleshooting and fixing various issues related to the internet infrastructure. Provide them with hypothetical scenarios and challenges to solve within a given time frame.

UNIT 3

1. **Group Discussion:** Divide the class into groups and ask each group to brainstorm and discuss the potential reasons why individuals or groups might engage in cyber crimes. Encourage them to consider factors such as financial gain, political motives, personal vendettas, and technological curiosity. Research and Present: Assign each student or group a specific type of cyber crime (e.g., phishing, identity theft, ransomware, etc.) and have them research the motivations behind such crimes. They can then present their findings to the class and engage in a Q&A session to foster deeper understanding.

2. **Ethical Dilemma Scenarios:** Present students with hypothetical scenarios where individuals might be tempted to engage in cyber crimes due to various reasons. Ask them to critically analyze the ethical implications and consequences of such actions.

3. **Case Studies Analysis:** Provide students with case studies of high-profile cyber crime incidents and ask them to analyze the potential reasons behind the perpetration of these crimes. Encourage them to consider the psychological, social, and economic factors that could drive individuals to commit cyber crimes.Interactive

4. **Polling:** Use a digital polling platform to conduct a real-time survey in the classroom, asking students to anonymously vote on the most common motivations for committing cyber crimes. This can lead to rich discussions about the prevalence of different motives.These pre-reading questions, tasks, and activities are designed to stimulate students' critical thinking and analysis before delving into the topic of reasons for committing cyber crimes.

UNIT 4

Post-Reading Tasks: Reflective Writing: Ask students to write a reflective essay or journal entry discussing their insights gained from the reading. They can explore how their understanding of cyber crimes and the motivations behind them has evolved and how it relates to their own ethical considerations.Role-Playing Scenarios: Create role-playing scenarios where students take on the roles of different stakeholders involved in cyber crimes, such as hackers, law enforcement officers, victims, and policymakers. This will help them empathize with various perspectives and consider the complexities of cyber crime motivations .Analyze Real-Life Examples: Provide students with recent examples of cyber crimes reported in the news and ask them to analyze the potential motivations behind these incidents based on the knowledge gained from their reading.

UNIT 5

1. **Research and Report:** Assign each student a specific type of malware (e.g., adware, spyware, browser hijacking software) to research in-depth. Have them prepare a short report summarizing how it works, common characteristics, and methods of prevention.

2. **Case Study Analysis:** Provide a case study involving a real-world malware incident. Ask students to analyze the case, identify the type of malware involved, and propose preventive measures that could have been implemented.

2. **Interactive Simulation:** Use online interactive simulations or virtual labs to demonstrate how malware spreads and the impact it can have on a computer system. Discuss the findings and lessons learned as a class.

UNIT 6

1. **Research and Presentation:** Divide the class into small groups and assign each group one type of threat (virus, worm, Trojan horse, shareware) to research. Have each group create a short presentation explaining the characteristics, methods of infection, and potential risks associated with their assigned threat.
2. **Security Awareness Campaign:**Design a poster or infographic that educates people on best practices for avoiding viruses, worms, Trojan horses, and the risks associated with using shareware. Display these around the school or share them online.
3. **Case Study Analysis:** Provide students with case studies of historical cyberattacks involving viruses, worms, Trojan horses, or shareware. Ask them to analyze and present the key details, impacts, and lessons learned from these incidents.

UNIT 7

These activities aim to engage students in exploring the importance of authentication, understanding different methods, and fostering critical thinking about the security implications of various approaches.

1. **Case Study Discussion:** Analyze real-world examples of security breaches related to weak authentication. Discuss the consequences and explore what could have been done differently to prevent or mitigate these incidents.
2. **Design a Secure Authentication System:** In groups, design a secure authentication system for a hypothetical online service, considering factors such as usability, scalability, and resistance to common attacks.

UNIT 8

These activities aim to enhance students' understanding of encryption and digital signatures, promote critical thinking about their implications, and encourage practical exploration of encryption tools and technologies.

1. **Debate on Privacy vs. Security:** Organize a debate discussing the balance between privacy and security in the context of widespread encryption. Explore the ethical and legal implications of strong encryption on individual privacy and national security.
2. **Create an Encryption Guide:** In groups, create a comprehensive guide on encryption for individuals, covering the basics, practical applications, and best practices for implementing encryption in various contexts.

UNIT 9

These activities aim to deepen students' understanding of antivirus software, encourage critical thinking about its role in cybersecurity, and provide practical insights into selecting and using such tools effectively.

1. **Interview with a Cybersecurity Expert:** Arrange a virtual or in-person interview with a cybersecurity professional specializing in antivirus technology. Prepare questions in advance and share insights with the class.
2. **Case Study Analysis:** Research and present case studies of notable malware incidents, highlighting how antivirus software played a role in preventing or mitigating the impact.

UNIT 10

These activities aim to engage students in practical exploration, critical thinking, and discussions about firewalls and steganography, fostering a deeper understanding of their roles in cybersecurity.

1. **Firewall Configuration Simulation:** Simulate a scenario where students must configure a firewall to protect a network from various types of cyber threats. Discuss the decision-making process behind different firewall settings.
2. **Firewall Effectiveness Debate:** Organize a debate discussing the effectiveness of firewalls in today's evolving cybersecurity landscape. Explore different perspectives on the role of firewalls and potential alternatives.
3. **Create a Steganography Challenge:** Challenge students to create and solve steganography puzzles. This activity encourages creativity and critical thinking while exploring the intricacies of hidden communication.

UNIT 11

These activities aim to provide students with hands-on experience, critical thinking opportunities, and insights into the multifaceted nature of computer forensics in the realm of digital investigations.

1. **Digital Crime Scene Simulation:** Create a simulated digital crime scene where students act as computer forensic investigators. Provide them with a case scenario, and guide them through the process of collecting and analyzing digital evidence.
2. **Digital Evidence Preservation Workshop:** Conduct a workshop on the proper techniques for preserving digital evidence. Include topics such as chain of custody, documentation, and maintaining forensic integrity.

3. **Case Study Analysis:** Research and present case studies where computer forensics played a crucial role in solving cybercrimes. Analyze the methodologies employed and the impact on the legal outcomes.
4. **Mock Trial:** Organize a mock trial where students play the roles of attorneys, witnesses, and computer forensic experts. Develop a case involving digital evidence and explore its presentation in a legal setting.

UNIT 12

These activities aim to engage students in discussions, hands-on exercises, and research to deepen their understanding of the importance of reporting cybercrimes and the processes involved in reporting such incidents.

1. **Cybercrime Reporting Scenarios:** Present students with different cybercrime scenarios, and ask them to discuss and plan how they would report each incident. Emphasize the importance of providing necessary information.
2. **Mock Reporting Exercise:** Conduct a mock cybercrime reporting exercise where students take on roles as victims, witnesses, and law enforcement officers. Simulate the reporting process to enhance understanding.
3. **Analysis of Reporting Platforms:** Research and analyze existing cybercrime reporting platforms. Evaluate their accessibility, user-friendliness, and the efficiency of their reporting processes. Present findings to the class.

UNIT 13

These activitY aims to provide practical experiences, enhance understanding, and empower individuals with the knowledge and skills to implement secure password practices, two-step verification, and effective antivirus measures.

Role Play: Password Recovery Scenarios: Create scenarios where students role-play password recovery situations. Discuss the importance of verifying identity during the recovery process.

UNIT 14

These activities aim to provide students with practical experiences, deepen their understanding of password managers, and empower them with the knowledge and skills to improve their digital security.

1. **Security Awareness Campaign:** Develop an awareness campaign promoting the use of password managers. Include educational materials, infographics, and presentations to highlight the importance and benefits.
2. **Role-Play: Password Recovery with a Password Manager:** Simulate scenarios where students role-play using a password manager for password recovery. Discuss the importance of master passwords and recovery options.
3. **Create a Password Policy:** In groups, create a password policy for an organization or community, incorporating the use of a password manager. Consider factors such as password complexity, rotation, and account recovery.
4. **Cybersecurity Panel Discussion:** Organize a panel discussion with cybersecurity experts to discuss the role of password managers in enhancing digital security. Encourage questions and discussions from the audience.

UNIT 15

These activities aim to engage students in hands-on experiences, critical thinking, and practical applications to deepen their understanding of working with the firewall on a Mac computer.

1. **Case Study Analysis**: Research and present case studies where the use or misconfiguration of a firewall on a Mac had a significant impact on the security of the system. Discuss the lessons learned from each case.
2. **Firewall Rule Creation:** In a controlled environment, have students create custom firewall rules for specific applications or services on a Mac. Discuss the purpose and implications of each rule.
3. **Security Audit and Review:** Conduct a security audit of a Mac system, reviewing the firewall settings. Identify areas for improvement and discuss best practices for maintaining a secure configuration.
4. **Troubleshooting Scenarios:** Create hypothetical scenarios where students must troubleshoot firewall-related issues on a Mac. Encourage them to identify and solve problems related to blocked or allowed connections.

UNIT 16

These activities aim to engage students in hands-on experiences, critical thinking, and practical applications to deepen their understanding of working with Windows Firewall in Windows 7.

1. **Case Study Analysis:** Research and present case studies where the use or misconfiguration of a firewall had a significant impact on the security of a system. Discuss the lessons learned from each case.
2. **Firewall Rule Creation:** In a controlled environment, have students create custom firewall rules for specific applications or services. Discuss the purpose and implications of each rule.
3. **Troubleshooting Scenarios:** Create hypothetical scenarios where students must troubleshoot firewall-related issues. Encourage them to identify and solve problems related to blocked or allowed connections.

GLOSSARY

A

access control — The means and mechanisms of managing access to and use of resources by users. There are three primary forms of access control: DAC, MAC, and RBAC. DAC (Discretionary Access Control) manages access through the use of on-object ACLs (Access Control Lists), which indicate which users have been granted (or denied) specific privileges or permissions on that object. MAC (Mandatory Access Control) restricts access by assigning each subject and object a classification or clearance level label; resource use is then controlled by limiting access to those subjects with equal or superior labels to that of the object. RBAC (Role Base Access Control) controls access through the use of job labels, which have been assigned the permissions and privilege needed to accomplish the related job tasks. (Also known as authorization.)

anti-virus (anti-malware) — A security program designed to monitor a system for malicious software. Once malware is detected, the AV program will attempt to remove the offending item from the system or may simply quarantine the file for further analysis by an administrator. It is important to keep AV software detection databases current in order to have the best chance of detecting known forms of malware.

antivirus software — A software program that monitors a computer system or network communications for known examples of malicious code and then attempts to remove or quarantine the offending items. (Also known as Malware Scanner.) Most anti-virus (AV) products use a pattern recognition or signature matching system to detect the presence of known malicious code. Some AV products have adopted technologies to potentially detect new and unknown malware. These technologies include anomaly detection (i.e. watch for programs which violate specific rules), behavioral detection (i.e. watch for programs that have behaviors that are different from the normal baseline of behavior of the system), and heuristic detection (i.e. watch for programs that exhibit actions which are known to be those of confirmed malware; it is a type of technological profiling).

APT (Advanced Persistent Threat) — A security breach that enables an attacker to gain access or control over a system for an extended period of time usually without the owner of the system being aware of the violation. Often an APT takes advantage of numerous unknown vulnerabilities or zero day attacks, which allow the attacker to maintain access to the target even as some attack vectors are blocked.

asset — Anything that is used in and is necessary to the completion of a business task. Assets include both tangible and intangible items such as equipment, software code, data, facilities, personnel, market value and public opinion.

authentication — The process of proving an individual is a claimed identity. Authentication is the first element of the AAA services concept, which includes Authentication, Authorization, and Accounting. Authentication occurs after the initial step of identification (i.e. claiming an identity). Authentication is accomplished by providing one or more authentication factors—Type 1: something you know (e.g. password, PIN, or combination), Type 2: something you have (e.g. smart card, RSA SecureID FOB, or USB drive), and Type 3: something you are (e.g. biometrics—fingerprint, iris scan, retina scan, hand geometry, signature verification, voice recognition, and keystroke dynamics).

authorization — The security mechanism determining and enforcing what authenticated users are authorized to do within a computer system. The dominant forms of authorization are DAC, MAC and RBAC. DAC (Discretionary Access Control) manages access using ACL (Access Control Lists) on each resource object where users are listed along with the permissions or privileges granted or denied them. MAC (Mandatory Access Control) manages access using labels of classification or clearance on both subjects and objects, and only those subjects with equal or superior clearance are allowed to access resources. RBAC (Role Based Access Control) manages access using labels of a job role that has been granted the permissions and privileges needed to accomplish a specific job or role.

B

backing up — Creating a duplicate copy of data onto a separate physical storage device or online/cloud storage solution. A backup is the only insurance against data loss. With a backup, damaged or lost data files can be restored. Backups should be created on a regular, periodic basis such as daily. A common strategy is based on the 3-2-1 rule: you should have three copies of your data - the original and 2 backups; you should use 2 different types of media (such as a physical media (such as a hard drive or tape) and a cloud storage solution); and do not store the three copies of data in 1 plane (i.e. backups should be stored offsite). It is important to store backups for disaster recovery at an offsite location in order to insure they are not damaged by the same event that would damage the primary production location. However, additional onsite backups can be retained for resolving minor issues such as accidental file deletion or hard drive failure.

BCP (Business Continuity Planning) — A business management plan used to resolve issues that threaten core business tasks. (Also known as Business Continuity Management.) The goal of BCP is to prevent the failure of mission critical processes when they have be harmed by a breach or accident. Once core business tasks have been stabilized, BCP dictates the procedure to return the environment back to normal conditions. BCP is used when the normal security policy has failed to prevent harm from occurring, but before the harm has reached the level of fully interrupting mission critical processes, which would trigger the Disaster Recovery Process (DRP).

behavior monitoring — Recording the events and activities of a system and its users. The recorded events are compared against security policy and behavioral baselines to evaluate compliance and/or discover violations. Behavioral monitoring can include the tracking of trends, setting of thresholds and defining responses. Trend tracking can reveal when errors are increasing requiring technical support services, when abnormal load levels occur indicating the presence of malicious code, or when production work levels increase indicating a need to expand capacity. Thresholds are used to define the levels of activity or events above which are of concern and require a response. The levels below the threshold are recorded but do not trigger a response. Responses can be to resolve conflicts, handle violations, prevent downtime or improve capabilities.

blacklist — A security mechanism prohibiting the execution of those programs on a known malicious or undesired list of software. The blacklist is a list of specific files known to be malicious or otherwise are unwanted. Any program on the list is prohibited from executing while any other program, whether benign or malicious, is allowed to execute by default. (See whitelist.)

block cipher — A type of symmetric encryption algorithm that divides data into fixed length sections and then performs the encryption or decryption operation on each block. The action of dividing a data set into blocks enables the algorithm to encrypt data of any size.

botnet — A collection of innocent computers which have been compromised by malicious code in order to run a remote control agent granting an attacker the ability to remotely take advantage of the system's resources in order to perform illicit or criminal actions. These actions include DoS flooding attacks, hosting false Web services, spoofing DNS, transmitting SPAM, eavesdropping on network communications, recording VOIP communications and attempting to crack encryption or password hashes. Botnets can be comprised of dozens to over a million individual computers. The term botnet is a shortened form of robotic network.

bug — An error or mistake in software coding or hardware design or construction. A bug represents a flaw or vulnerability in a system discoverable by attackers and used as point of compromise. Attacks often use fuzzing technique (i.e. randomize testing tools) to locate previously unknown bugs in order to craft new exploits.

BYOD (Bring Your Own Device) — A company's security policy dictating whether or not workers can bring in their own devices into the work environment, whether or not such devices can be connected to the company network and to what extent that connection allows interaction with company resources. A BYOD policy can range from complete prohibition of personal devices being brought into the facility to allowing any device to be connected to the company network with full access to all company resources. Generally, a BYOD policy puts reasonable security limitations on which devices can be used on company property and severely limits access to sensitive company network resources. BYOD should address concerns such as data ownership, asset tracking, geo location, patching and upgrades, security applications (such as malware scanners, firewalls and IDS), storage segmentation, appropriate vs inappropriate applications, on-boarding, off-boarding, repair/replacement due to damage, legal concerns, internal investigations and law enforcement investigations and forensics.

C

ciphertext — The unintelligible and seeming random form of data that is produced by the cryptographic function of encryption. Ciphertext is produced by a symmetric algorithm when a data set is transformed by the encryption process using a selected key. Ciphertext can converted back into its original form (i.e. plain text) by performing the decryption process using the same symmetric encryption algorithm and the key used during the encryption process. (Also known as cryptogram.)

clickjacking — A malicious technique by which a victim is tricked into clicking on a URL, button or other screen object other than that intended by or perceived by the user. Clickjacking can be performed in many ways; one of which is to load a web page transparently behind another visible page in such a way that the obvious links and objects to click are facades, so clicking on an obvious link actually causes the hidden page's link to be selected.

cloud computing — A means to offer computing services to the public or for internal use through remote services. Most cloud computing systems are based on remote virtualization where the application or operating environment offered to customers is hosted on the cloud provider's computer hardware. There are a wide range of cloud solutions including software applications (examples include e-mail and document editing), custom code hosting (namely execution platforms and web services) as well as full system replacements (such as remote virtual services to host databases or file storage). (See SaaS, PaaS, and IaaS.) Most forms of cloud computing are considered public cloud as they are provided by a third party. However, private cloud (internally hosted), community cloud (a group of companies' privately hosted cloud), a hosted private cloud (the cloud servers are owned and managed by a third party but hosted in the facility of the customer) and hybrid cloud (a mixture of public and private) are also options.

CND (Computer Network Defense) — The establishment of a security perimeter and of internal security requirements with the goal of defending a network against cyberattacks, intrusions and other violations. A CND is defined by a security policy and can be stress tested using vulnerability assessment and penetration testing measures.

cracker — The proper term to refer to an unauthorized attacker of computers, networks and technology instead of the misused term “hacker.” However, this term is not as widely used in the media; thus, the term hacker has become more prominent in-spite of the terms misuse. (See hacker.)

critical infrastructure — The physical or virtual systems and assets that are vital to an organization or country. If these systems are compromised, the result would be catastrophic. If an organization's mission critical processes are interrupted, this could result in the organization ceasing to exist. If a country's critical infrastructure is destroyed, it will have severe negative impact on national security, economic stability, citizen safety and health, transportation and communications.

CVE (Common Vulnerabilities and Exposures) — An online database of attacks, exploits and compromises operated by the MITRE organization for the benefit of the public. It includes any and all attacks and abuses known for any type of computer system or software product. Often new attacks and exploits are documented in a CVE long before a vendor admits to the issue or releases an update or patch to resolve the concern.

cryptography — The application of mathematical processes on data-at-rest and data-in-transit to provide the security benefits of confidentiality, authentication, integrity and non-repudiation. Cryptography includes three primary components: symmetric encryption, asymmetric encryption and hashing. Symmetric encryption is used to provide confidentiality. Asymmetric encryption is used to provide secure symmetric key generation, secure symmetric key exchange (via digital envelopes created through the use of the recipient's public key) verification of source, verification/control of recipient, digital signature (a combination of hashing and use of the sender's private key) and digital certificates (which provides third-party authentication services). Hashing is the cryptographic operation that produces a representational value from an input data set. A before and after hash can be compared in order to detect protection of or violation of integrity.

cyberattack — Any attempt to violate the security perimeter of a logical environment. An attack can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets. Cyberattacks can be initiated through exploitation of a vulnerability in a publicly exposed service, through tricking a user into opening an infectious attachment, or even causing automated installation of exploitation tools through innocent website visits. (Also known as drive-by download.)

cyber ecosystem — The collection of computers, networks, communication pathways, software, data and users that comprise either a local private network or the world-wide Internet. It is the digital environment within which software operates and data is manipulated and exchanged.

cyberespionage — The unethical act of violating the privacy and security of an organization in order to leak data or disclose internal/private/confidential information. Cyberespionage can be performed by individuals, organization or governments for the direct purpose of causing harm to the violated entity to benefit individuals, organizations or governments.

cybersecurity — The efforts to design, implement, and maintain security for an organization's network, which is connected to the Internet. It is a combination of logical/technical-, physical- and personnel-focused countermeasures, safeguards and security controls. An organization's cybersecurity should be defined in a security policy, verified through evaluation techniques (such as vulnerability assessment and penetration testing) and revised, updated and improved over time as the organization evolves and as new threats are discovered.

cyber teams — Groups of professional or amateur penetration testing specialists who are tasked with evaluating and potentially improving the security stance of an organization. Common cyber teams include the red, blue and purple/white teams. A red team is often used as part of a multi-team penetration test (i.e. security evaluation), which is responsible for attacking the target which is being defended by the blue team. A purple team or white team is either used as a reference between the attack/red and defense/blue teams; or this team can be used as an interpreter of the results and activities of the red and blue teams in order to maximize their effectiveness in the final results.

D

data breach — The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.

data integrity — A security benefit that verifies data is unmodified and therefore original, complete and intact. Integrity is verified through the use of cryptographic hashing. A hashing algorithm generates a fixed length output known as a hash value, fingerprint or MAC (Message Authenticating Code), which is derived from the input data but which does not contain the input data. This makes hashing a one-way operation. A hash is calculated before an event, and another hash is calculated after the event (an event can be a time frame of storage (i.e. data-at-rest) or an occurrence of transmission (i.e. data-in-transit); the two hashes are then compared using an XOR Boolean operation. If the two hashes exactly match (i.e. the XOR result is zero), then the data has retained its integrity.

However, if the two hashes do not match exactly (i.e. the XOR result is a non-zero value), then something about the data changed during the event.

data mining — The activity of analyzing and/or searching through data in order to find items of relevance, significance or value. The results of data mining are known as meta-data. Data mining can be a discovery of individual important data items, a summary or overview of numerous data items or a consolidation or clarification of a collection of data items.

data theft — The act of intentionally stealing data. Data theft can occur via data loss (physical theft) or data leakage (logical theft) event. Data loss occurs when a storage device is lost or stolen. Data leakage occurs when copies of data is possessed by unauthorized entities.

DDoS (Distributed Denial of Service) Attack — An attack which attempts to block access to and use of a resource. It is a violation of availability. DDOS (or DDoS) is a variation of the DoS attack (see DOS) and can include flooding attacks, connection exhaustion, and resource demand. The distinction of DDOS from DOS is that the attack traffic may originate from numerous sources or is reflected or bounced off of numerous intermediary systems. The purpose of a DDoS attack is to significantly amplify the level of the attack beyond that which can be generated by a single attack system in order to overload larger and more protected victims. DDoS attacks are often waged using botnets. (See botnet.)

decrypt — The act which transforms ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption) back into its original plaintext or cleartext form. Ciphertext is produced by a symmetric encryption algorithm when a data set is transformed by the encryption process using a selected key. Ciphertext can converted back into its original form (i.e. plaintext) by performing the decryption process using the same symmetric encryption algorithm and the same key used during the encryption process.

digital certificate — A means by which to prove identity or provide authentication commonly by means of a trusted third-party entity known as a certificate authority. A digital certificate is based on the x.509 v3 standard. It is the public key of a subject signed by the private key of a certificate authority with clarifying text information such as issuer, subject identity, date of creation, date of expiration, algorithms, serial number and thumbprint (i.e. hash value).

digital forensics — The means of gathering digital information to be used as evidence in a legal procedure. Digital forensics focuses on gathering, preserving and analyzing the fragile and volatile data from a computer system and/or network. Computer data that is relevant to a security breach and/or criminal action is often intermixed with standard benign data from business functions and personal activities. Thus, digital forensics can be challenging to properly collect relevant evidence while complying with the rules of evidence in order to ensure that such collected evidence is admissible in court.

DLP (Data Loss Prevention) — A collection of security mechanisms which aim at preventing the occurrence of data loss and/or data leakage. Data loss occurs when a storage device is lost or stolen while data leakage occurs when copies of data is possessed by unauthorized entities. In both cases, data is accessible to those who should not have access. DLP aims at preventing such occurrences through various techniques such as strict access controls on resources, blocking the use of email attachments, preventing network file exchange to external systems, blocking cut-and-paste, disabling use of social networks and encrypting stored data.

DMZ (Demilitarized Zone) — A segment or subnet of a private network where resources are hosted and accessed by the general public from the Internet. The DMZ is isolated from the private network using a firewall and is protected from obvious abuses and attacks from the Internet using a firewall. A DMZ can be deployed in two main configurations. One method is the screened subnet configuration, which has the structure of I-F-DMZ-F-LAN (i.e. internet, then firewall, then the DMZ, then another firewall, then the private LAN). A second method is the multi-homed firewall configuration, which has the structure of a single firewall with three interfaces, one connecting to the Internet, a second to the DMZ, and a third to the private LAN.

DOS (Denial of Service) — An attack that attempts to block access to and use of a resource. It is a violation of availability. DOS (or DoS) attacks include flooding attacks, connection exhaustion and resource demand. A flooding attack sends massive amounts of network traffic to the target overloading the ability of network devices and servers to handle the raw load. Connection exhaustion repeatedly makes connection requests to a target to consume all system resources related to connections, which prevents any other connections from being established or maintained. A resource demand DoS repeatedly requests a resource from a server in order to keep it too busy to respond to other requests.

drive-by download — A type of web-based attack that automatically occurs based on the simple act of visiting a malicious or compromised/poisoned Web site. A drive-by download is accomplished by taking advantage of the default nature of a Web browser to execute mobile code, most often JavaScript, with little to no security restrictions. A drive-by download can install tracking tools, remote access backdoors, botnet agents, keystroke loggers or other forms of malicious utilities. In most cases, the occurrence of the infection based on the drive-by download is unnoticed by the user/victim.

E

eavesdropping — The act of listening in on a transaction, communication, data transfer or conversation. Eavesdropping can be used to refer to both data packet capture on a network link (also known as sniffing or packet capture) and to audio recording using a microphone (or listening with ears).
encode — The act which transforms plaintext or cleartext (i.e. the original form of normal standard data) into ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption). Ciphertext is produced by a symmetric encryption algorithm when a data set is transformed by the encryption process using a selected key (i.e. to encrypt or encode). Ciphertext can converted back into its original form (i.e. plaintext) by performing the decryption process using the same symmetric encryption algorithm and the same key used during the encryption process (i.e. decrypt or decode).
encryption key — The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process. A key is a number defined by its length in binary digits. Generally, the longer the key length, the more security (i.e. defense against confidentiality breaches) it provides. The length of the key also determines the key space, which is the range of values between the binary digits being all zeros and all ones from which the key can be selected.

F

firewall — A security tool, which may be a hardware or software solution that is used to filter network traffic. A firewall is based on an implicit deny stance where all traffic is blocked by default. Rules, filters or ACLs can be defined to indicate which traffic is allowed to cross the firewall. Advanced firewalls can make allow/deny decisions based on user authentication, protocol, header values and even payload contents.

H

hacker — A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities. A hacker may be ethical and authorized (the original definition) or may be malicious and unauthorized (the altered but current use of the term). Hackers can range from professionals who are skilled programmers to those who have little to no knowledge of the specifics of a system or exploit but who can follow directions; in this instance, they are called script kiddies.
hacktivism — Attackers who hack for a cause or belief rather than some form of personal gain. Hacktivism is often viewed by attackers as a form of protest or fighting for their perceived “right” or “justice.” However, it is still an illegal action in most cases when the victim’s technology or data is abused, harmed or destroyed.
honeypot — A trap or decoy for attackers. A honeypot is used to distract attackers in order to prevent them from attacking actual production systems. It is a false system that is configured to look and function as a production system and is positioned where it would be encountered by an unauthorized entity who is seeking out a connection or attack point. A honeypot may contain false data in order to trick attackers into spending considerable time and effort attacking and exploiting the false system. A honeypot may also be able to discover new attacks or the identity of the attackers.

I

IaaS (Infrastructure-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to craft virtual networks within their computing environment. An IaaS solution enables a customer to select which operating systems to install into virtual machines/nodes as well as the structure of the network including use of virtual switches, routers and firewalls. It also provides complete freedom as to the software or custom code run on the virtual machines. An IaaS solution is the most flexible of all the cloud computing services; it allows for significant reduction in hardware by the customer in their own local facility. It is the most expensive form of cloud computing service.
identity cloning — A form of identity theft in which the attacker takes on the identity of a victim and then attempts to live and act as the stolen identity. Identity cloning is often performed in order to hide the birth country or a criminal record of the attacker in order to obtain a job, credit or other secured financial instrument.
identity fraud — A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.
IDS (Intrusion Detection System) — A security tool that attempts to detect the presence of intruders or the occurrence of security violations in order to notify administrators, enable more detailed or focused logging or even trigger a response such as disconnecting a session or blocking an IP address. An IDS is considered a more passive security tool as it detects compromises after they are already occurring rather than preventing them from becoming successful.
information security policy — A written account of the security strategy and goals of an organization. A security policy is usually comprised of standards, policies (or SOPs – Standard Operating Procedures) and guidelines. All hardware, software, facilities and personnel must abide by the terms of the security policy of an organization. (Also known as security policy.)

insider threat — The likelihood or potential that an employee or another form of internal personnel may pose a risk to the stability or security of an organization. An insider has both physical access and logical access (through their network logon credentials). These are the two types of access that an outside attacker must first gain before launching malicious attacks whereas an insider already has both of these forms of access. Thus, an insider is potentially a bigger risk than an outsider if that insider goes rogue or is tricked into causing harm.

IPS (Intrusion Prevention System) — A security tool that attempts to detect the attempt to compromise the security of a target and then prevent that attack from becoming successful. An IPS is considered a more active security tool as it attempts to proactively respond to potential threats. An IPS can block IP addresses, turn off services, block ports and disconnect sessions as well as notify administrators.

ISP (Internet Service Provider) — The organization that provides connectivity to the Internet for individuals or companies. Some ISPs offer additional services above that of just connectivity such as e-mail, web hosting and domain registration.

J

JBOH (JavaScript-Binding-Over-HTTP) — A form of Android-focused mobile device attack that enables an attacker to be able to initiate the execution of arbitrary code on a compromised device. A JBOH attack often takes place or is facilitated through compromised or malicious apps.

K

keylogger — Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard. A keylogger can be a software solution or a hardware device used to capture anything that a user might type in including passwords, answers to secret questions or details and information form e-mails, chats and documents.

L

LAN (Local Area Network) — An interconnection of devices (i.e. a network) that is contained within a limited geographic area (typically a single building). For a typical LAN, all of the network cables or interconnection media is owned and controlled by the organization unlike a WAN (Wide Area Network) where the interconnection media is owned by a third party.

link jacking — A potentially unethical practice of redirecting a link to a middle-man or aggregator site or location rather than the original site the link seemed to indicate it was directed towards. For example, a news aggregation service may publish links that seem as if they point to the original source of their posted articles, but when a user discovers those links via search or through social networks, the links redirect back to the aggregation site and not the original source of the article.

M

malware (malicious software) — Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system. Malware includes a wide range of types of malicious programs including: virus, worm, Trojan horse, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware and spyware/adware.

O

outsider threat — The likelihood or potential that an outside entity, such as an ex-employee, competitor or even an unhappy customer, may pose a risk to the stability or security of an organization. An outsider must often gain logical or physical access to the target before launching malicious attacks.

outsourcing — The action of obtaining services from an external entity. Rather than performing certain tasks and internal functions, outsourcing enables an organization to take advantages of external entities that can provide services for a fee. Outsourcing is often used to obtain best-of-breed level service rather than settling for good-enough internal operations. It can be expensive and increases an organization's security risk due to the exposure of internal information and data to outsiders.

OWASP (Open Web Application Security Project) — An Internet community focused on understanding web technologies and exploitations. Their goal is to help anyone with a website improve the security of their site through defensive programming, design and configuration. Their approach includes understanding attacks in order to know how to defend against them. OWASP offers numerous tools and utilities related to website vulnerability evaluation and discovery as well as a significant amount of training and reference material related to all things web security.

P

PaaS (Platform-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to operate custom code or applications. A PaaS operator determines which operating systems or execution environments are offered. A PaaS system does not allow the customer to change operating systems, patch the OS or alter the virtual network space. A PaaS system allows the customer to reduce hardware deployment in their own local facility and to take advantage of on-demand computing (also known as pay as you go).

packet sniffing — The act of collecting frames or packets off of a data network communication. This activity allows the evaluation of the header contents as well as the payload of network communications. Packet sniffing requires that the network interface card be placed into promiscuous mode in order to disable the MAC (Media Access Control) address filter which would otherwise discard any network communications not intended for the specific local network interface. (Also known as sniffing or eavesdropping.)

patch — An update or change or an operating system or application. A patch is often used to repair flaws or bugs in deployed code as well as introduce new features and capabilities. It is good security practice to test all updates and patches before implementation and attempt to stay current on patches in order to have the latest version of code that has the fewest known flaws and vulnerabilities.

patch management — The management activity related to researching, testing, approving and installing updates and patches to computer systems, which includes firmware, operating systems and applications. A patch is an update, correction, improvement or expansion of an existing software product through the application of new code issued by the vendor. Patch management is an essential part of security management in order to prevent downtime, minimize vulnerabilities and prevent new untested updates from interfering with productivity.

payment card skimmers — A malicious device used to read the contents of an ATM, debit or credit card when inserted into a POS (Point of Sale) payment system. A skimmer may be an internal component or an external addition. An attacker will attempt to use whatever means to imbed their skimmer into a payment system that will have the highest likelihood of not being detected and thus gather the most amount of financial information from victims. (See POS intrusions.)

pen testing — A means of security evaluation where automated tools and manual exploitations are performed by security and attack experts. This is an advanced form of security assessment that should only be used by environments with a mature security infrastructure. A penetration test will use the same tools, techniques and methodologies as criminal hackers, and thus, it can cause downtime and system damage. However, such evaluations can assist with securing a network by discovering flaws that are not visible to automated tools based on human (i.e. social engineering) or physical attack concepts. (Also known as penetration testing or ethical hacking.)

phishing — A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smart phone apps. The goal of a phishing attack may be to learn logon credentials, credit card information, system configuration details or other company, network, computer or personal identity information. Phishing attacks are often successful because they mimic legitimate communications from trusted entities or groups such as false emails from a bank or a retail website.

PKI (Public Key Infrastructure) — A security framework (i.e. a recipe) for using cryptographic concepts in support of secure communications, storage and job tasks. A PKI solution is a combination of symmetric encryption, asymmetric encryption, hashing and digital certificate-based authentication.

POS (Point of Sale) intrusions — An attack that gains access to the POS (Point of Sale) devices at a retail outlet enabling an attacker to learn payment card information as well as other customer details. POS intrusions can occur against a traditional brick-and-mortar retail location as well as any online retail websites. (See payment card skimmers.)

R

ransomware — A form of malware that holds a victim's data hostage on their computer typically through robust encryption. This is followed by a demand for payment in the form of Bitcoin (an untraceable digital currency) in order to release control of the captured data back to the user.

restore — The process of returning a system back to a state of normalcy. A restore or restoration process may involve formatting the main storage device before re-installing the operating system and applications as well as copying data from backups onto the reconstituted system.

risk assessment — The process of evaluating the state of risk of an organization. Risk assessment is often initiated through taking an inventory of all assets, assigning each asset a value, and then considering any potential threats against each asset. Threats are evaluated for their exposure factor (EF) (i.e. the amount of loss that would be caused by the threat causing harm) and frequency of occurrence (i.e. ARO—Annualized Rate of Occurrence) in order to calculate a relative risk value known as the ALE (Annualized Loss Expectancy). The largest ALE indicates the biggest concern or risk for the organization.

risk management — The process of performing a risk assessment and evaluating the responses to risk in order to mitigate or otherwise handle the identified risks. Countermeasures, safeguards or security controls are to be selected that may eliminate or reduce risk, assign or transfer risk to others (i.e. outsourcing or buying insurance) or avoid and deter risk. The goal is to reduce risk down to an acceptable or tolerable level.

S

SaaS (Software-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to use a provided application. Examples of a SaaS include online e-mail services or online document editing systems. A user of a SaaS solution is only able to use the offered application and make minor configuration tweaks. The SaaS provider is responsible for maintaining the application.

sandboxing — A means of isolating applications, code or entire operating systems in order to perform testing or evaluation. The sandbox limits the actions and resources available to the constrained item. This allows for the isolated item to be used for evaluation while preventing any harm or damage to be caused to the host system or related data or storage devices.

SCADA (Supervisory Control and Data Acquisition) — A complex mechanism used to gather data and physical world metrics as well as perform measurement or management actions of the monitored systems for the purposes of automatic large complex real-world processes such as oil refining, nuclear power generation or water filtration. SCADA can provide automated control over very large complex systems whether concentrated in a single physical location or spread across long distances.

security control — Anything used as part of a security response strategy which addresses a threat in order to reduce risk. (Also known as countermeasure or safeguard.)

security perimeter — The boundary of a network or private environment where specific security policies and rules are enforced. The systems and users within the security boundary are forced into compliance with local security rules while anything outside is not under such restrictions. The security perimeter prevents any interactions between outside entities and internal entities that might violate or threaten the security of the internal systems.

SIEM (Security Information and Event Management) — A formal process by which the security of an organization is monitored and evaluated on a constant basis. SIEM helps to automatically identify systems that are out of compliance with the security policy as well as to notify the IRT (Incident Response Team) of any security violating events.

sniffing — See packet sniffing and eavesdropping.

social engineering — An attack focusing on people rather than technology. This type of attack is psychological and aims to either gain access to information or to a logical or physical environment. A social engineering attack may be used to gain access to a facility by tricking a worker into assisting by holding the door when making a delivery, gaining access into a network by tricking a user into revealing their account credentials to the false technical support staff or gaining copies of data files by encouraging a worker to cut-and-paste confidential materials into an e-mail or social networking post.

SPAM — A form of unwanted or unsolicited messages or communications typically received via e-mail but also occurring through text messaging, social networks or VoIP. Most SPAM is advertising, but some may include malicious code, malicious hyperlinks or malicious attachments.

spear phishing — A form of social engineering attack that is targeted to victims who have an existing digital relationship with an online entity such as a bank or retail website. A spear phishing message is often an e-mail although there are also text message and VoIP spear phishing attacks as well, which looks exactly like a legitimate communication from a trusted entity. The attack tricks the victim into clicking on a hyperlink to visit a company website only to be re-directed to a false version of the website operated by attackers. The false website will often look and operate similarly to the legitimate site and focus on having the victim provide their logon credentials and potentially other personal identity information such as answers to their security questions, an account number, their social security number, mailing address, email address and/or phone number. The goal of a spear phishing attack is to steal identity information for the purpose of account takeover or identity theft.

spoof (spoofing) — The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP address, MAC address and email address.

spyware — A form of malware that monitors user activities and reports them to an external their party. Spyware can be legitimate in that it is operated by an advertising and marketing agency for the purpose of gathering customer demographics. However, spyware can also be operated by attackers using the data gathering tool to steal an identity or learn enough about a victim to harm them in other ways.

supply chain — The path of linked organizations involved in the process of transforming original or raw materials into a finished product that is delivered to a customer. An interruption of the supply chain can cause a termination of the production of the final product immediately or this effect might not be noticed until the materials already in transit across the supply chain are exhausted.

T

threat assessment — The process of evaluating the actions, events and behaviors that can cause harm to an asset or organization. Threat assessment is an element of risk assessment and management. (Also known as threat modeling and threat inventory.)

Trojan Horse (Trojan) — A form of malware where a malicious payload is imbedded inside of a benign host file. The victim is tricked into believing that the only file being retrieved is the viewable benign host. However, when the victim uses the host file, the malicious payload is automatically deposited onto their computer system.
two-factor authentication — The means of proving identity using two authentication factors usually considered stronger than any single factor authentication. A form of multi-factor authentication. Valid factors for authentication include Type 1: Something you know such as passwords and PINs; Type 2: Something you have such as smart cards or OTP (One Time Password) devices; and Type 3: Someone you are such as fingerprints or retina scans (aka biometrics).
two-step authentication — A means of authentication commonly employed on websites as an improvement over single factor authentication but not as robust as two-factor authentication. This form of authentication requires the visitor provide their username (i.e. claim an identity) and password (i.e. the single factor authentication) before performing an additional step. The additional step could be receiving a text message with a code, then typing that code back into the website for confirmation. Alternatives include receiving an e-mail and needing to click on a link in the message for confirmation, or viewing a pre-selected image and statement before typing in another password or PIN. Two-step is not as secure as two-factor because the system provides one of the factors to the user at the time of logon rather than requiring that the user provide both.

U

unauthorized access — Any access or use of a computer system, network or resource which is in violation of the company security policy or when the person or user was not explicitly granted authorization to access or use the resource or system

V

VPN (Virtual Private Network) — A communication link between systems or networks that is typically encrypted in order to provide a secured, private, isolate pathway of communications.
virus — A form of malware that often attaches itself to a host file or the MBR (Master Boot Record) as a parasite. When the host file or MBR is accessed, it activates the virus enabling it to infect other objects. Most viruses spread through human activity within and between computers. A virus is typically designed to damage or destroy data, but different viruses implement their attack at different rates, speeds or targets. For example, some viruses attempt to destroy files on a computer as quickly as possible while others may do so slowly over hours or days. Others might only target images or Word documents (.doc/.docx).
vishing — A form of phishing attack which takes place over VoIP. In this attack, the attacker uses VoIP systems to be able to call any phone number with no toll-charge expense. The attacker often falsifies their caller-ID in order to trick the victim into believing they are receiving a phone call from a legitimate or trustworthy source such as a bank, retail outlet, law enforcement or charity. The victims do not need to be using VoIP themselves in order to be attacked over their phone system by a vishing attack. (See phishing.)
vulnerability — Any weakness in an asset or security protection which would allow for a threat to cause harm. It may be a flaw in coding, a mistake in configuration, a limitation of scope or capability, an error in architecture, design, or logic or a clever abuse of valid systems and their functions.

W

whitelist — A security mechanism prohibiting the execution of any program that is not on a pre-approved list of software. The whitelist is often a list of the file name, path, file size and hash value of the approved software. Any code that is not on the list, whether benign or malicious, will not be able to execute on the protected system. (See blacklist.)
Wi-Fi — A means to support network communication using radio waves rather than cables. The current Wi-Fi or wireless networking technologies are based on the IEE 802.11 standard and its numerous amendments, which address speed, frequency, authentication and encryption.
worm — A form of malware that focuses on replication and distribution. A worm is a self-contained malicious program that attempts to duplicate itself and spread to other systems. Generally, the damage caused by a worm is indirect and due to the worm's replication and distribution activities consuming all system resources. A worm can be used to deposit other forms of malware on each system it encounters.

Z

zombie — A term related to the malicious concept of a botnet. The term zombie can be used to refer to the system that is host to the malware agent of the botnet or to the malware agent itself. If the former, the zombie is the system that is blinding performing tasks based on instructions from an external and remote hacker. If the latter, the zombie is the tool that is performing malicious actions such as DoS flooding, SPAM transmission, eavesdropping on VoIP calls or falsifying DNS resolutions as one member of a botnet.

REFERENCES

1.Belton, P. How the tech industry is redesigning the future workplace / P. Belton. — 1 May 2015. — URL: http://www.bbc. com/ news/business-32523448

2.Cellan-Jones, R. A computing revolution in schools / R. Cel-lan-Jones. — 1 September 2014. — URL: http://www.bbc.com/ news/technology-29010511 (a)

3.Cellan-Jones, R. The 12 tech months of 2014 / R. Cellan-Jones. — 29 December 2014. — URL: http://www.bbc.com/news/ technology-30591570 (b)

4.Cellan-Jones, R. Microsoft headset to help blind people navigate cities / R. Cellan-Jones. - 6 November 2014. - URL: http:// www.bbc.com/news/technology-29913637

5.European e-Government Action Plan 2011—2015. - URL: http://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015

6.Evans, V. Software Engineering / V. Evans. - Express Pub-lishing, 2014. — (Career path).

7.Facebook's government user data requests up 24 %. —5 November 2014. - URL: http://www.bbc.com/news/busi-ness-29910101

8.Fitzgerald, P. English for ICT studies in Higher Education Studies / P. Fitzgerald, M. McCullagh, C. Tabor. — Garnet Educa-tion, 2011.

9. Google purpose-bui robot cars tested on public roads. -15 May 2015. - URL: http://www.bbc.com/news/technol-ogy-32750810

10.Hill, D. English for Information Technology: Level 2: Course book / D. Hill. - Pearson Education Limited, 2014.

11. ICT systems and their usage. - URL: http://www.bbc.co.uk/schools/gcsebitesize/ict/system/Oictsystemsrevl.shtml

12. Is cyber-warfare really that scary? — 6 May 2015. - URL: http://www.bbc.com/news/world-32534923

13. Jeans made that will prevent "digital pickpocketing". -17 December 2014. - URL: http://www.bbc.com/news/technol-
ogy-30513497

14. Kelion, L. "Email epidemic" is damaging UK productivity, says expert / L. Kelion. — 7 May 2015. - URL: http://www.bbc. com/news/technology-32622224 (a)

15. Kelion, L. CES 2015: The robots moving in to your house /L. Kelion. — 8 January 2015. — URL: http://www.bbc.com/news/ technology-30708953 (b)

16. Kelion, L. Moore's Law: Beyond the first law of computing /L. Kelion. — 17 April 2015. - URL: http://www.bbc.com/news/technology-32335003

17. Kellaway, L. How the computer changed the office forever /L. Kellaway. — 1 August 2013. — URL: http://www.bbc.com/ news/magazine-23509153

18. Kleinman, Z. Tech rivals join Microsoft in fight over US data demand / Z. Kleinman. – 16 December 2014. - URL: http:// www.bbc.com/news/technology-30494562

Kleinman, Z. Tech rivals join Microsoft in fight over US data demand / Z. Kleinman. -16 December 2014. - URL: http://www.bbc.com/news/technology-30494562

19. Mandebvu, S. What is ICT / S. Mandebvu. - 20 June 2014. - URL: http://www.slideshare.net/sammydhi01/what-is-ict-40492687

20.Moskvitch, K. Skype: How the online chat revolution changed lives / K. Moskvitch. — 28 August 2013. — URL: http://www.bbc. com/news/technology-23862352

21.Ricca-McCarthy, T. English for Telecoms and Information Technology (SB+MultiROM) / T. Ricca-McCarthy, M. Duck-worth. - Oxford : Oxford University Press, 2013. - (Oxford Express Series).

22. Rouse, M. Software development / M. Rouse. -April2010. — URL: http://whatis.techtarget.com/reference/Learn-IT-Software-development

23. Self-destructing virus kills off PCs. - 5 May 2015. - URL:http://www.bbc.com/news/technology-32591265 24. Shaw, K. Internet of Things 24.Shaping IT's Future / K. Shaw. -22 October 2014. — URL: http://www.webopedia.com/Blog/ internet-of-things-it-future.html

25. Shiels, M. Rise of the virtual conference / M. Shiels. —20 April 2010. — URL: http://news.bbc.co.uk/2/hi/technol-0gy/8608417.stm

26.Simmons, D. Europol kills off shape-shifting "Mystique" malware / D. Simmons. — 9 April 2015. — URL: http://www.bbc. com/news/technology-32218381 (a)

26.Simmons, D. IBM and Apple want to share how you are with others / D. Simmons. — 14 April 2015. — URL: http://www.bbc.