

# Cybersecurity For Beainners



# Course Description

This course provides an introduction to the essential concepts and practices of cybersecurity. In 60 minutes, you will gain a solid foundation in understanding various threats, vulnerabilities, and countermeasures to enhance your online security: empowering you to protect yourself and your digital assets from potential threats. The course covers topics such as network security, cryptography, and secure web browsing. By the end of this course, participants will have a better understanding of how to safeguard personal information, maintain data integrity and mitigate cyber risks.

# Course Requirements:

No prior knowledge of cybersecurity is required. Participants should have access to a computer or mobile device with an internet connection to access the course materials.

By the end of this course, you will have a solid understanding of fundamental cybersecurity concepts and practices. You will be equipped with the knowledge to make informed decisions regarding your online security and protect yourself from potential threats.

While this course provides an excellent introduction to cybersecurity, it is important to continue learning and staying updated on the evolving landscape of cyber threats and security best practices.

# Key Concepts Covered

**This course covers essential concepts that form the basis of cybersecurity knowledge. Participants will learn about:**

- Understand the concept of cybersecurity and its importance in protecting electronic devices, networks, and sensitive information from unauthorized access, theft, or damage.**
- Identify common types of cyber threats and attacks, such as broken access control, malware, phishing, ransomware, and social engineering, and understand their potential impact on individuals and organizations.**
- Recognize the importance of practicing secure online behavior, including creating strong and unique passwords, using two-factor authentication, safe browsing practices, and protecting personal information on social media.**

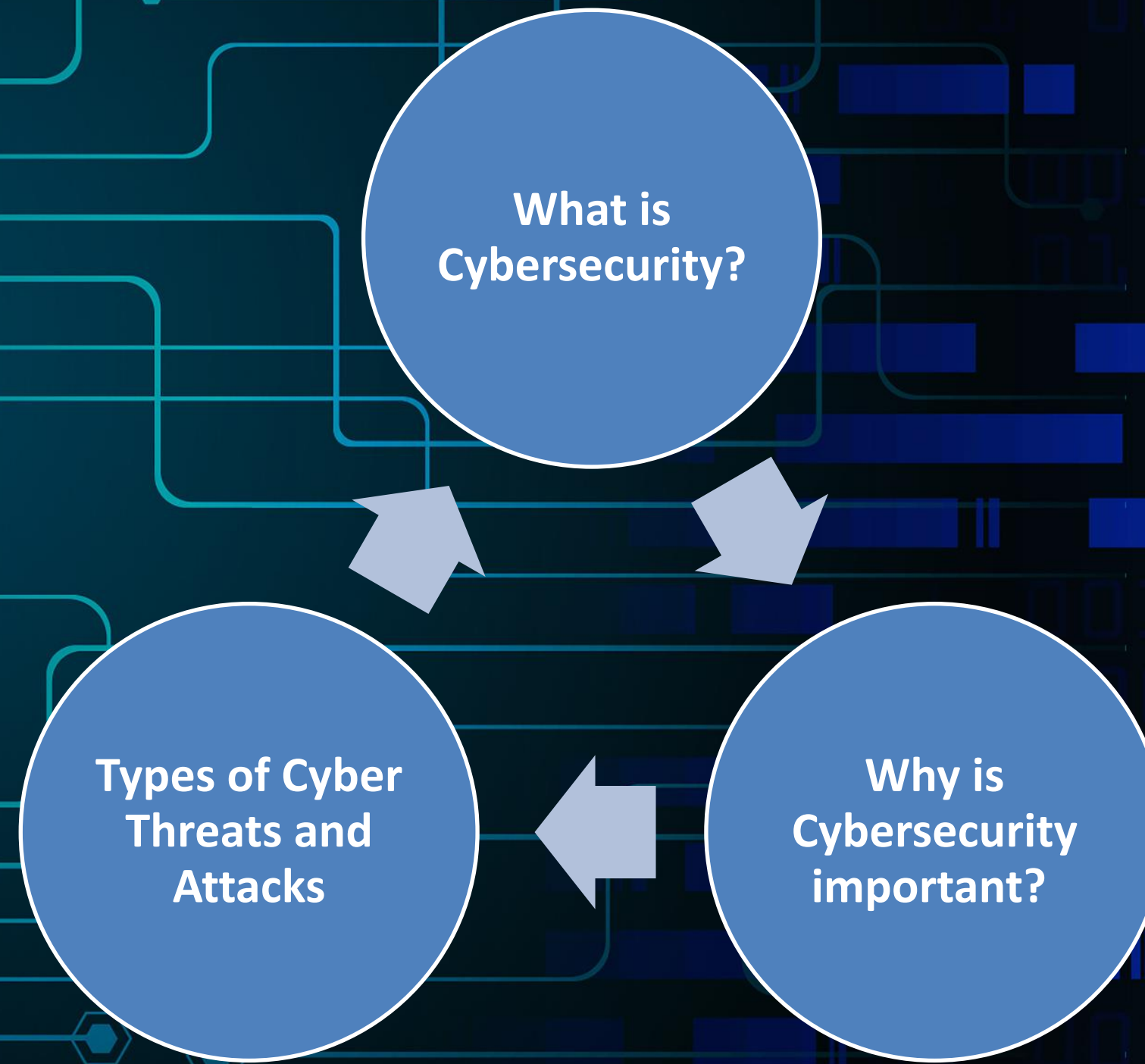
# Key Concepts Covered cont.

- Learn strategies to secure devices, including keeping software and operating systems up to date, installing and using antivirus/anti-malware software, understanding firewall basics, and encrypting sensitive data.
- Explore essential tips for maintaining a secure online presence, such as securing home Wi-Fi networks, regularly backing up data, and being aware of potential risks and vulnerabilities in the digital landscape.

# Benefits Of Taking This Course

- By completing the Introduction to Cybersecurity module, participants will gain a solid foundation in understanding the importance of cybersecurity and its practical application. They will develop the necessary knowledge and skills to protect themselves, their personal data, and digital assets from cyber threats. Furthermore, this course serves as a stepping stone for individuals interested in pursuing further studies or a career in cybersecurity.
- Overall, this course equips participants with the knowledge and awareness needed to navigate the complex landscape of cybersecurity, enabling them to make informed decisions to enhance their personal and professional cybersecurity posture.

# Section 1: Introduction to Cybersecurity



# What Is Cybersecurity?

- **Cybersecurity is the practice of protecting electronic devices, networks, and sensitive information from unauthorized access, theft, or damage. With the increasing reliance on technology in our daily lives, cybersecurity has become a critical issue that affects everyone, from individuals to businesses and governments.**
- **The consequences of a cyber attack can be devastating, ranging from financial losses to reputational damage and even physical harm. It is crucial to understand the potential risks and take proactive measures to safeguard against them.**



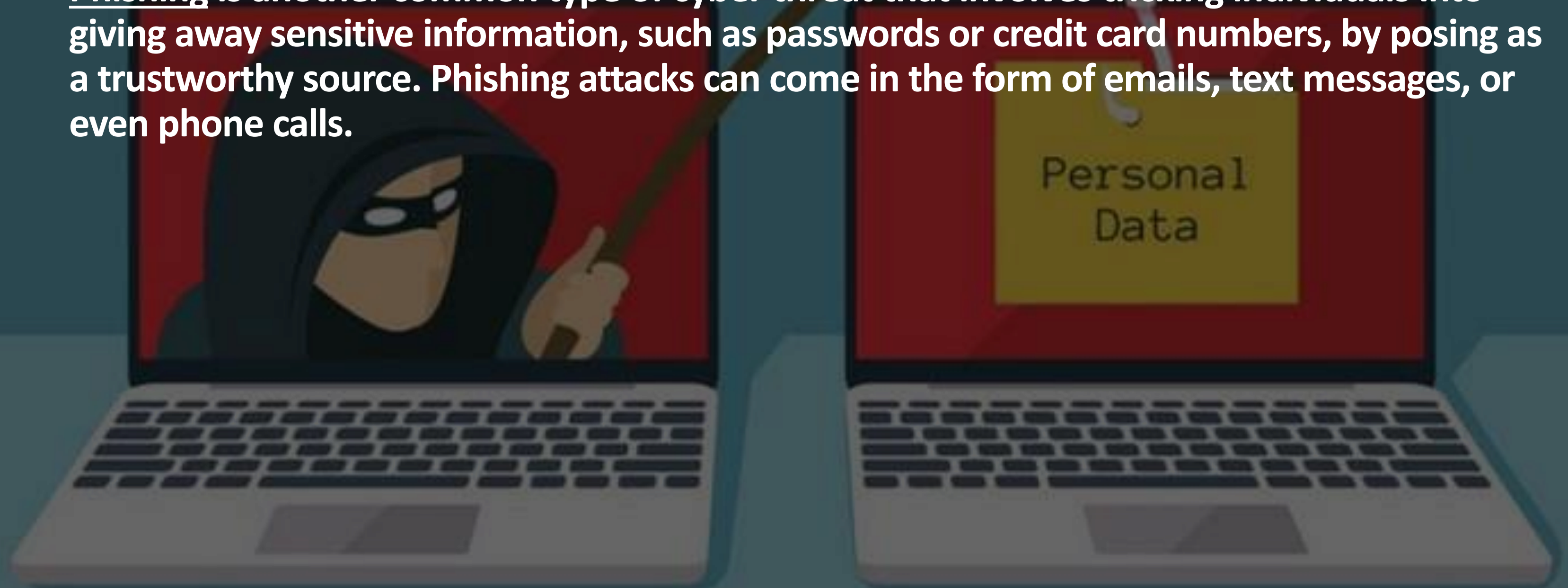
# Why Is Cybersecurity Important?

Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing measures to ensure the confidentiality, integrity, and availability of information. The increasing reliance on technology and the interconnectedness of devices have made individuals, organizations, and governments vulnerable to various cyber threats.

# Types Of Cyber Threats And Attacks

---

- Phishing is another common type of cyber threat that involves tricking individuals into giving away sensitive information, such as passwords or credit card numbers, by posing as a trustworthy source. Phishing attacks can come in the form of emails, text messages, or even phone calls.





# Types Of Cyber Threats And Attacks cont.

- **Broken Access Control** refers to a vulnerability that occurs when a system fails to properly enforce restrictions on user access. It allows unauthorized individuals to gain access to sensitive information or perform actions beyond their authorized privileges. This weakness can result in data breaches, unauthorized modifications, and other security breaches.
- **Malware** is a type of cyber threat that can infect your computer or device with harmful software designed to steal personal information or cause damage to your system. Malware can come in many forms, including viruses, worms, and Trojans.

# Types Of Cyber Threats And Attacks cont.

- Ransomware is a particularly malicious type of cyber threat that can lock you out of your own files or systems until a ransom is paid. This can be devastating for individuals and businesses alike, as it can result in the loss of important data or even financial ruin.

- It's important to be aware of these and other types of cyber threats in order to take steps to protect yourself and your devices from harm.





# RANSOMWARE

## BEHIND THE SCENES

By the time victims see the ransom note, it's already too late—ransomware has already encrypted files before they know it's there.

Here's what happens between infection and the ransom demand.



## Summary:

---

- **Cybersecurity is the practice of protecting electronic devices, networks, and sensitive information from unauthorized access, theft, or damage. The consequences of cyber attacks can be devastating, making cybersecurity a critical concern. Types of cyber threats include broken access control, malware, phishing, and ransomware, all of which can result in data breaches, financial losses, or other harm. Understanding these threats and taking proactive measures to safeguard against them is essential in today's interconnected digital world**

# Section 2: Understanding Common Cyber Threats

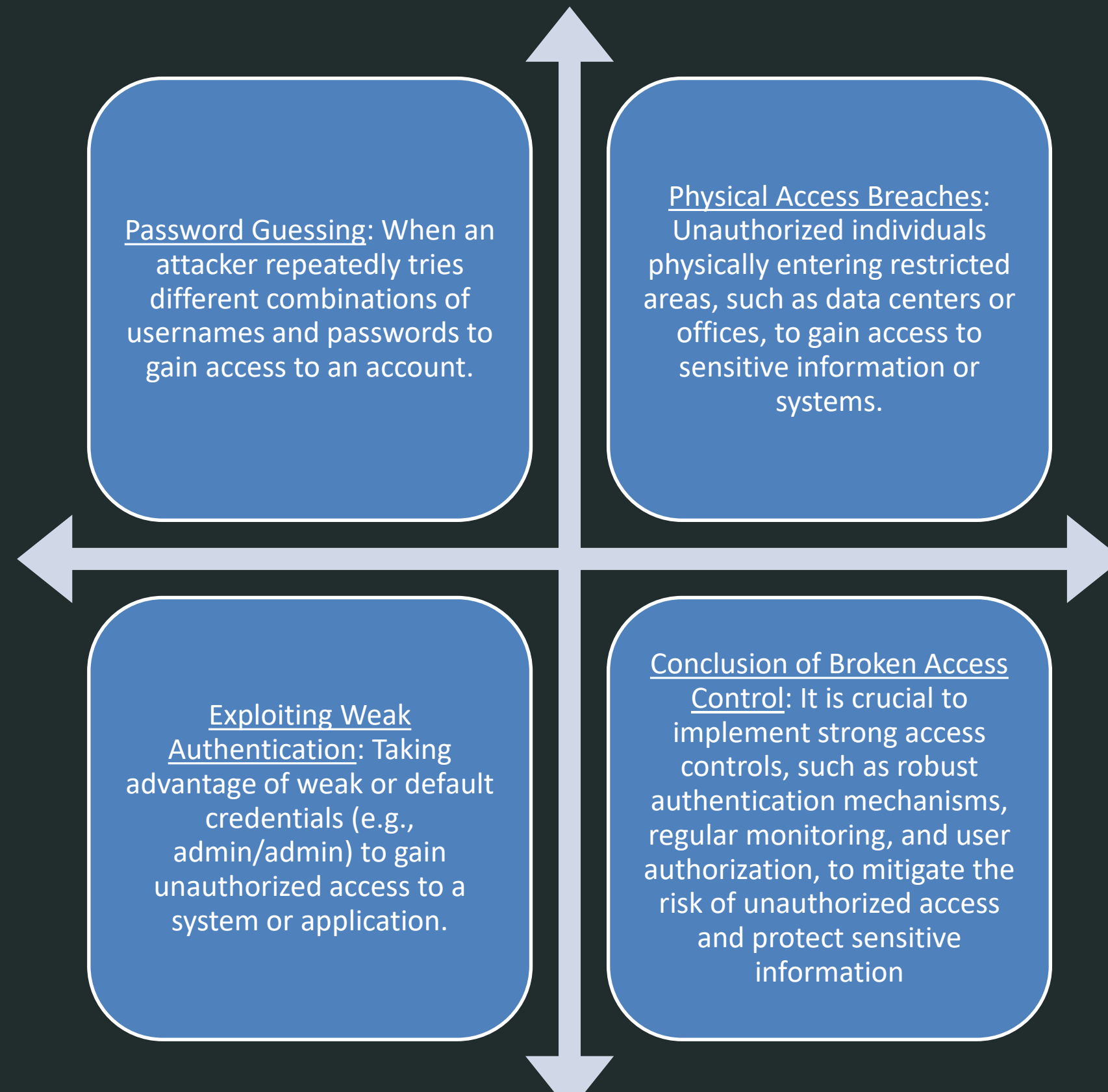
---

# Broken Access Control: Unauthorized access and credential theft

- Unauthorized access refers to the act of gaining entry or obtaining information without proper authorization or permission. It occurs when an individual bypasses or circumvents security measures to gain access to resources, systems, or data they are not supposed to have access to. Unauthorized access can lead to data breaches, privacy violations, and compromise the integrity of systems.



# Broken Access Control: Unauthorized access and credential theft





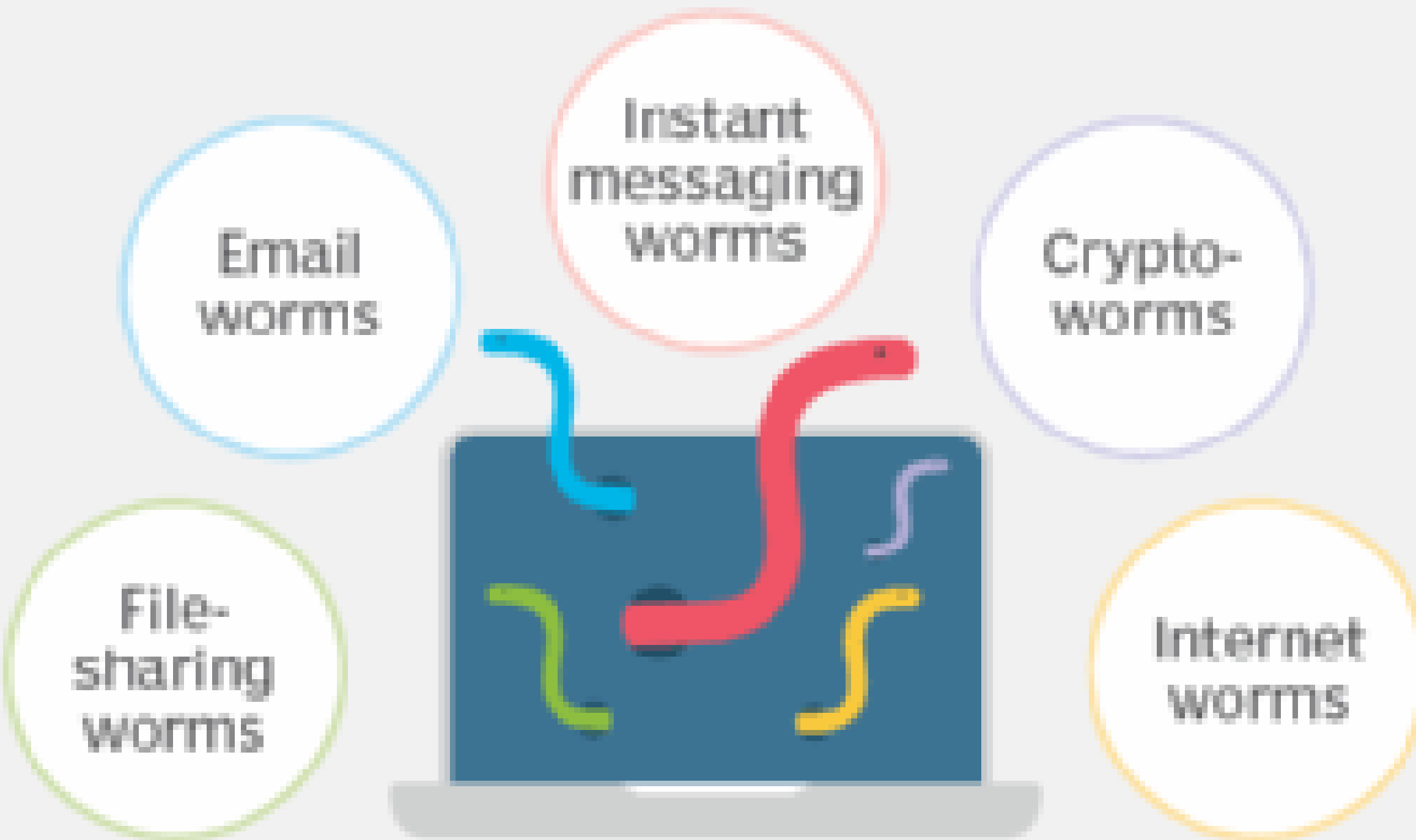
# Malware: Viruses and worms

---

- Viruses and worms are different types of malware that pose a threat to computer systems and networks. While they are all malicious software, each has its own distinct characteristics and methods of operation.
- Viruses: Viruses are self-replicating programs that infect other files or systems by attaching themselves to them. They spread by executing the infected files and can cause a range of harmful effects, such as data corruption, system instability, or unauthorized access.
  - Example: The "ILOVEYOU" virus, which emerged in 2000, spread via email and infected millions of systems worldwide. It disguised itself as a love letter and when opened, it executed the malicious code and propagated itself to the user's contacts, causing widespread damage.



# Types of computer worms



WORMS SUPPLIAL/GETTY IMAGES, ADRIE RECHONNET/ALL RIGHTS RESERVED.

- 
- **Worms:** Worms are standalone programs that self-replicate and spread across computer networks without the need for user interaction or the attachment to other files. They exploit vulnerabilities in network protocols or operating systems to infect and compromise connected devices.
  - **Example:** The "Conficker" worm, discovered in 2008, exploited a vulnerability in Microsoft Windows systems. It rapidly spread across networks by exploiting weak passwords and unpatched systems, infecting millions of computers worldwide.

**Conclusion to Malware: It is important to have up-to-date antivirus/anti-malware software. regularly apply security patches. exercise caution when downloading or executing files. and practice safe browsing habits to protect against viruses and worms. Additionally, maintaining backups of important data can help mitigate the impact of malware infections.**


# Phishing Attacks: Identifying And Avoiding Email And Phone Scams

---


- **Identifying and avoiding email and phone scams involves recognizing and taking necessary precautions against fraudulent attempts to deceive and manipulate users into revealing sensitive information like Personal Identifiable Information (PII) or financial details and/or performing harmful actions such as downloading malicious attachments. These scams often impersonate trusted entities or individuals and employ social engineering techniques to trick victims. By being vigilant and implementing security measures, users can protect themselves from falling victim to phishing attacks.**

# Email Scam

**Identifying** - Look out for suspicious email characteristics such as poor grammar, spelling errors, generic greetings, or email addresses that don't match the official sender. Phishing emails often employ urgency, fear, or enticing offers to prompt immediate action.



**Avoiding** - Do not click on suspicious links or download attachments from unknown senders. Verify the legitimacy of emails by independently contacting the organization or individual through trusted channels. Be cautious when providing personal or financial information online.



**Example** - A phishing email claims to be from a well-known bank, stating that the recipient's account has been compromised and urges them to click on a link to update their login credentials. The email has grammatical errors, uses a generic greeting, and the sender's email address doesn't match the bank's official domain.

# Mobile Scams (Ex: WhatsApp)

**Identifying** - Be cautious of messages from unknown numbers or contacts, especially if they contain unusual requests, strange attachments, or suspicious links. Pay attention to messages that create a sense of urgency, ask for personal information, or promise rewards or prizes.



**Avoiding** - Do not click on links or download files from unfamiliar sources, even if they come from seemingly trustworthy contacts. Double-check with the sender through a different communication channel to verify the authenticity of the message. Enable security features like two-step verification in WhatsApp settings.



**Example** - A WhatsApp message from an unknown number claims to be a friend in urgent need of financial assistance. The message includes a link to a website where the recipient is asked to provide their credit card details to send the money quickly. The urgent nature of the request and the request for sensitive financial information are red flags.



# Conclusion to Phishing Attacks

- By staying alert to these signs and exercising caution when dealing with unsolicited messages, individuals can effectively identify and avoid falling victim to email and WhatsApp scams. Remember, it's always better to err on the side of caution and verify the legitimacy of requests before taking any action.

# Social Engineering

- Manipulating and deceiving individuals through personal interactions to trick them into revealing their login credentials
- **Manipulating human behavior for malicious purposes. It involves exploiting psychological and social aspects to deceive individuals into disclosing sensitive information, granting unauthorized access, or performing actions that benefit the attacker. By leveraging trust, authority, or emotions, social engineering attacks bypass technical security measures and rely on human vulnerabilities.**

## Social Engineering Explained

Also known as human hacking, social engineering is the manipulation of someone to divulge confidential information that can be used for fraudulent purposes.



The social engineer gathers information about their victims.



The social engineer poses as a legitimate person and builds trust with their victims.



The social engineer gathers information about their victims.



The social engineer poses as a legitimate person and builds trust with their victims.

- Example: A common form of social engineering is a "Tech Support Scam." In this scenario, an attacker impersonates a technical support representative from a reputable company and contacts a victim via phone or email. The attacker convinces the victim that their computer is infected with malware or experiencing technical issues. To resolve the problem, the victim is asked to provide remote access to their computer or download malicious software under the guise of a legitimate tool. Once the attacker gains control, they can steal personal information, install malware, or extort money from the victim.

# Conclusion To Social Engineering

---

- **It is essential to remain cautious and skeptical of unsolicited communication, especially when it involves sensitive information or requests for actions that seem unusual or suspicious. Verify the authenticity of requests independently, be wary of sharing personal information or credentials, and report any suspected social engineering attempts to relevant authorities or the organization being impersonated. Education and awareness play a critical role in mitigating the risks associated with social engineering attacks.**

# Password Attacks: Brute-Force And Password Hygiene

Brute Force Attack - A brute force attack is an automated method where an attacker systematically tries all possible combinations of characters until the correct password is found. It relies on the assumption that eventually, the correct combination will be discovered through sheer trial and error.



Password Hygiene - Password hygiene refers to following good practices to create strong and secure passwords. It involves using complex and unique passwords for each account, regularly changing passwords, and avoiding common and easily guessable choices.



**Conclusion to Password Attacks:** Implementing strong, unique passwords and regularly changing them can significantly reduce the risk of successful brute force attacks. Additionally, enabling multi-factor authentication and using password managers can enhance password security by adding an extra layer of protection and simplifying the management of complex passwords.

---

# Summary

---

- In the session on understanding common cyber threats, we explored broken access control, password attacks, malware, phishing attacks, and social engineering. Broken access control involves unauthorized access and credential theft, while password attacks exploit weak authentication methods. Malware includes viruses and worms that can harm systems. Phishing attacks target individuals through email and WhatsApp scams. Social engineering manipulates human behavior for malicious purposes, and password attacks like brute force and password hygiene play a role in protecting against unauthorized access. By understanding these threats, individuals can take proactive measures to enhance their cybersecurity.

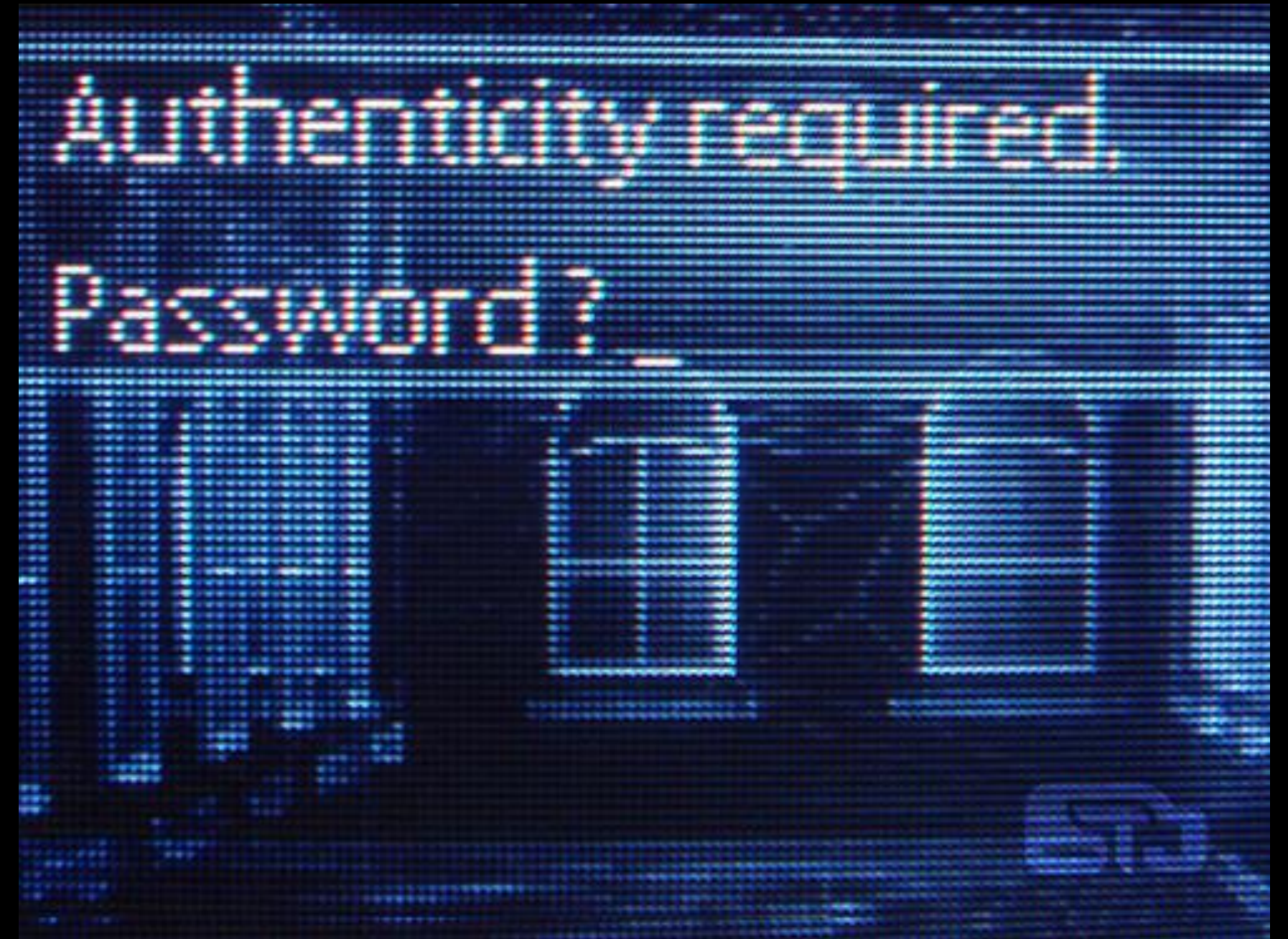
The background of the slide is a dark blue, textured pattern of circuit board traces. In the center, there is a metallic padlock with a circular hole in its body. The text is overlaid on this image.

# Section 3: Secure Online Behavior

---

# Secure Online Behavior

- One of the most important aspects of cybersecurity is practicing good online habits. By using strong passwords, avoiding suspicious links, and keeping your software up to date, you can greatly reduce your risk of falling victim to cyber attacks.
  - Creating strong and unique passwords
    - Strong and unique passwords provide a crucial defense against unauthorized access to personal accounts and sensitive information. They significantly reduce the likelihood of successful brute force attacks as complex passwords are difficult to guess or crack. By using strong and unique passwords, individuals can enhance the security of their online presence and protect themselves against potential data breaches and identity theft.
  - Two-factor authentication:
    - Enhancing security with an extra layer of protection - Two-factor authentication (2FA) provides an additional layer of security by requiring users to provide two forms of verification to access their accounts. This extra step adds an extra level of protection against unauthorized access, even if the password is compromised. By combining something the user knows (password) with something they have (such as a unique code sent to their mobile device), 2FA significantly reduces the risk of unauthorized access and enhances overall account security.







**Enhancing security with an extra layer of protection means making something more safe and secure by adding another step to it. Just like how you have a lock on your diary to keep it safe, we can add a special lock to our online accounts. This special lock is called Two-factor authentication (2FA).**




**Normally, when we log in to our accounts, we just need to put in a password. But with 2FA, we need to do two things to prove that we are the real owners of the account. It's like having two locks instead of one.**

- **The first thing we do is put in our password, which is something we know and only we should know. But that's not enough to keep our account really safe.**
- **The second thing we do is provide another proof that we are the right person. This can be a special code that is sent to our mobile phone. So, not only do we have to know the password, but we also need to have our phone with us to get the special code. It's like having a special key that only we have.**
- **By doing these two steps, it becomes much harder for someone else to get into our account, even if they somehow find out our password. It's like having double protection! This makes our account much safer and helps us keep our information private."**



# Safe Browsing Practices

- **Identifying malicious websites and using secure connections (HTTPS) - By recognizing and avoiding malicious websites, individuals can protect themselves from phishing attacks, malware infections, and potential data breaches. Additionally, using secure connections through HTTPS ensures that the data transmitted between the user's device and the website is encrypted, enhancing privacy and safeguarding sensitive information from unauthorized access or interception.**



# Social media privacy:

- **Protecting personal information online - Social media privacy is vital for safeguarding personal information online. By actively managing privacy settings, users can control who has access to their posts, photos, and personal details. This reduces the risk of unauthorized individuals exploiting or misusing personal information, protecting against potential privacy violations, identity theft, and targeted advertising.**

# Summary

- **In Module 3 on secure online behavior, we covered several key aspects of cybersecurity. Creating strong and unique passwords was highlighted as a crucial defense against unauthorized access and data breaches. Two-factor authentication was discussed as an effective way to enhance security by requiring users to provide an additional form of verification. Safe browsing practices, such as identifying malicious websites and using secure connections (HTTPS), were emphasized to protect against phishing attacks and ensure data privacy. Lastly, the importance of social media privacy was emphasized in safeguarding personal information and mitigating risks of privacy violations and identity theft. By practicing these habits, individuals can greatly reduce their risk of falling victim to cyber attacks and protect their online presence.**



# Section 4 Securing Your Devices

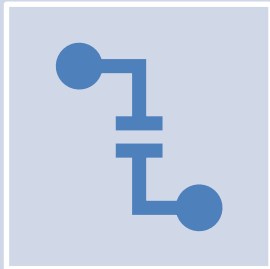
# Securing Your Devices

## Keeping software and operating systems up to date

Keeping software and operating systems up to date is crucial for cybersecurity as it ensures that the latest security patches and fixes are installed, minimizing vulnerabilities that can be exploited by hackers and protecting your devices from potential threats.

## Installing and using antivirus/anti-malware software

Installing and using antivirus/anti-malware software is crucial for securing your devices as it helps detect, prevent, and remove malicious software, protecting your sensitive information and ensuring the overall integrity and performance of your system.



## **Firewall basics: Protecting against unauthorized network access**

Firewall basics are crucial for protecting against unauthorized network access by acting as a barrier between your device and the internet, monitoring and controlling incoming and outgoing traffic to prevent potential threats from infiltrating your system.



## **Encrypting sensitive data: Understanding encryption and its importance**

Encrypting sensitive data is crucial because it transforms information into a secure and unreadable format, ensuring that even if it is intercepted or accessed without authorization, it remains protected and unintelligible to unauthorized individuals or hackers.



# Summary

- **Keeping software and operating systems up to date is essential for cybersecurity, as it installs the latest security patches and fixes, reducing vulnerabilities. Antivirus/anti-malware software is crucial in detecting and removing malicious software, safeguarding sensitive information and system integrity. Firewalls act as a protective barrier, monitoring and controlling network traffic to prevent unauthorized access. Encrypting sensitive data ensures its security and makes it unreadable to unauthorized individuals, even if intercepted.**



# Section 5: Essential Tips for a Secure Online Presence

---

## Secure Wi-Fi practices: Securing your home network

- Secure Wi-Fi practices, such as securing your home network, are crucial for maintaining a safe online presence as they prevent unauthorized access to your personal information and protect against potential cyber threats.
- For example, if your home Wi-Fi network is left unsecured, hackers in proximity can easily gain access to your network, potentially intercepting sensitive data or launching attacks on connected devices.



## Backing up your data: Importance and methods

- Backing up your data is crucial because it ensures that you have copies of your important files and information in case of data loss, such as hardware failure, malware, or accidental deletion.
- For example, imagine losing all your important documents, photos, and work files due to a computer crash with no backup, resulting in significant loss and potential disruption to your personal or professional life.

## Being cautious with downloads and email attachments

Being cautious with downloads and email attachments is crucial for maintaining a secure online presence as they can often contain malware or malicious code that can compromise the security of your device and personal information.

- For example, opening a suspicious email attachment can lead to the installation of ransomware, which encrypts your files and demands a ransom for their release.

## Regularly reviewing and adjusting privacy settings on online accounts

Regularly reviewing and adjusting privacy settings on online accounts is essential to maintain control over personal information and protect against unauthorized access.

- For example, by regularly checking and adjusting the privacy settings on social media accounts, users can limit the visibility of their posts and personal details to their desired audience, reducing the risk of potential privacy breaches.

# Summary

- **Secure Wi-Fi practices, such as securing your home network, are essential for maintaining a safe online presence, preventing unauthorized access and potential cyber threats. Backing up your data is crucial to avoid losing important files and information due to hardware failure, malware, or accidental deletion. Being cautious with downloads and email attachments is vital as they can contain malware that compromises device security. Regularly reviewing and adjusting privacy settings on online accounts helps maintain control over personal information and protects against unauthorized access**



# Resources

Additional Resources For Further Learning

- **Here are some online websites that students and participants of the course can visit to learn more about cybersecurity:**
  - **Cybrary (<https://www.cybrary.it/>):** Cybrary offers a wide range of free cybersecurity courses, including beginner-friendly material. It covers various topics such as network security, ethical hacking, and incident response.
  - **Open Security Training (<https://www.opensecuritytraining.info/>):** Open Security Training provides free and open-source security training materials, including videos and slides from various security conferences and workshops. It covers a broad range of cybersecurity topics, including software vulnerabilities, network security, and reverse engineering.
  - **National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog (<https://niccs.us-cert.gov/training/search>):** The NICCS Training Catalog is a comprehensive database of cybersecurity training resources provided by government agencies, academic institutions, and private organizations. It allows users to search for courses based on their interests and skill levels.

- **SANS Institute (<https://www.sans.org/>):** SANS Institute offers a mix of free and paid training resources. They provide webcasts, whitepapers, and newsletters on various cybersecurity topics. Their blog is also a valuable source of information for staying updated on the latest security trends.
- **OWASP (<https://owasp.org/>):** The Open Web Application Security Project (OWASP) is a nonprofit organization that focuses on web application security. Their website offers a wealth of resources, including articles, guides, tools, and community-driven projects aimed at helping individuals understand and address web application security challenges.
- **Khan Academy - Computing (<https://www.khanacademy.org/computing>):** Khan Academy's Computing section covers computer science and programming topics, including cybersecurity fundamentals. It provides interactive lessons, quizzes, and coding exercises suitable for beginners.



- **Carnegie Mellon University's Software Engineering Institute**  
(<https://www.sei.cmu.edu/>): The SEI website offers resources and publications on various aspects of cybersecurity, including best practices, frameworks, and research papers. They cover topics such as secure coding, incident response, and secure software development.
- **The Cybersecurity and Infrastructure Security Agency (CISA)**  
(<https://www.cisa.gov/>): CISA's website provides a wealth of information on cybersecurity best practices, resources, and guidance. They offer training materials, alerts, and advisories to help individuals and organizations protect themselves against cyber threats.

**Remember, cybersecurity is a rapidly evolving field, so it's important to explore multiple sources and stay updated with the latest trends and best practices. These websites provide a solid foundation for learning, but always exercise caution and verify the credibility of the information you come across.**

# Course Test

A 25-question test on cybersecurity for beginners



# Section 1: Multiple Choice

Select one answer for each question

# 1. What Is Cybersecurity?

- a) Protecting physical assets from damage
- b) Protecting electronic devices, networks, and sensitive information from unauthorized access, theft, or damage
- c) Protecting personal reputation on social media platforms
- d) Protecting physical health from cyber threats

# 1. What Is Cybersecurity?

- a) Protecting physical assets from damage
- b) Protecting electronic devices, networks, and sensitive information from unauthorized access, theft, or damage**
- c) Protecting personal reputation on social media platforms
- d) Protecting physical health from cyber threats

**2. Which of the following is NOT a potential consequence of a cyber attack?**

**a) Financial losses**

**b) Reputational damage**

**c) Physical harm**

**d) Improved network performance**

**2. Which of the following is NOT a potential consequence of a cyber attack?**

**a) Financial losses**

**b) Reputational damage**

**c) Physical harm**

**d) Improved network performance**



### **3. Which of the following best defines broken access control?**

- a) Unauthorized access to a computer system**
- b) Unauthorized entry into restricted areas**
- c) Failure to enforce restrictions on user access**
- d) Manipulating individuals through personal interactions**

### 3. Which of the following best defines broken access control?

- a) Unauthorized access to a computer system
- b) Unauthorized entry into restricted areas
- c) Failure to enforce restrictions on user access**
- d) Manipulating individuals through personal interactions

## **4. What is phishing?**

- a) Infecting a computer with harmful software**
- b) Gaining unauthorized access to a system or application**
- c) Manipulating individuals through personal interactions**
- d) Tricking individuals into revealing sensitive information by posing as a trustworthy source**

## 4. What is phishing?

- a) Infecting a computer with harmful software
- b) Gaining unauthorized access to a system or application
- c) Manipulating individuals through personal interactions
- d) Tricking individuals into revealing sensitive information by posing as a trustworthy source**

# 5. What is ransomware?

- a) Infecting a computer with harmful software
- b) Gaining unauthorized access to a system or application
- c) Locking files or systems until a ransom is paid**
- d) Manipulating individuals through personal interactions

# Section 2: True or False

Determine whether the statement is true or false.

**6. True or False: Cybersecurity only affects businesses and governments.**

**6. True or False: Cybersecurity does not only affect businesses and governments.**



**7. True or False: Broken access control refers to unauthorized physical access to restricted areas.**

**7. True or False:** Broken access control refers to the act of gaining entry or obtaining information without proper authorization or permission. It occurs when an individual bypasses or circumvents security measures to gain access to resources, systems, or data they are not supposed to have access to. Unauthorized access can lead to data breaches, privacy violations, and compromise the integrity of systems.

**8. True or False: Malware can come in the form of viruses, worms, and trojans.**

8. **True** or False: Malware can come in the form of viruses, worms, and trojans.

**9. True or False: Phishing attacks can occur through emails, text messages, or phone calls.**

9. **True** or False: Phishing attacks can occur through emails, text messages, or phone calls.

**10. True or False: Regularly updating antivirus software is important to protect against malware.**

10. **True** or False: Regularly updating antivirus software is important to protect against malware.



# Section 3: Multiple Selection

Select the best answers for each question

**11. Which of the following are examples of malware? (Select all that apply)**

- a. Viruses**
- b. Worms**
- c. Phishing**
- d. Ransomware**

**11. Which of the following are examples of malware?**

**a. Viruses**

**b. Worms**

**c. Phishing**

**d. Ransomware**

**12. Which of the following are methods used in credential theft? (Select all that apply)**

- a) Password guessing**
- b) Shoulder surfing**
- c) Brute-force attacks**
- d) Social engineering**

**12. Which of the following are methods used in credential theft? (Select all that apply)**

- a) Password guessing**
- b) Shoulder surfing**
- c) Brute-force attacks**
- d) Social engineering**

**13. Which of the following are examples of good password hygiene practices? (Select all that apply)**

**a) Using complex and unique passwords**

**b) Reusing the same password across multiple platforms**

**c) Changing passwords regularly**

**d) Avoiding easily guessable choices**

**13. Which of the following are examples of good password hygiene practices? (Select all that apply)**

**a) Using complex and unique passwords**

**b) Reusing the same password across multiple platforms**

**c) Changing passwords regularly**

**d) Avoiding easily guessable choices**

**14. Which of the following are safe browsing practices? (Select all that apply)**

- a) Clicking on suspicious links**
- b) Downloading files from unfamiliar sources**
- c) Using secure connections (HTTPS)**
- d) Recognizing and avoiding malicious websites**



**14. Which of the following are safe browsing practices? (Select all that apply)**

a) Clicking on suspicious links

b) Downloading files from unfamiliar sources

**c) Using secure connections (HTTPS)**

**d) Recognizing and avoiding malicious websites**

**15. Which of the following are methods for securing your devices? (Select all that apply)**

**a) Keeping software and operating systems up to date**

**b) Installing and using antivirus/anti-malware software**

**c) Disabling firewalls to improve network performance**

**d) Encrypting sensitive data**

**15. Which of the following are methods for securing your devices? (Select all that apply)**

**a) Keeping software and operating systems up to date**

**b) Installing and using antivirus/anti-malware software**

**c) Disabling firewalls to improve network performance**

**d) Encrypting sensitive data**

# Section 4: Fill in the Blanks

**16. Broken access control occurs when a system fails to properly enforce restrictions on access.**

**16. Broken access control occurs when a system fails to properly enforce restrictions on **USER** access.**

**17.            is a type of cyber threat that infects a computer or device with harmful software.**

**17. Malware** is a type of cyber threat that infects a computer or device with harmful software.



**18.            involves tricking individuals into revealing sensitive information by posing as a trustworthy source.**

**18. Phishing** involves tricking individuals into revealing sensitive information by posing as a trustworthy source.

**19. Brute force attack is an automated method where an attacker systematically tries all possible combinations of characters until the correct is found.**

**19. Brute force attack is an automated method where an attacker systematically tries all possible combinations of characters until the correct password is found.**

**20. Secure Wi-Fi practices are crucial for protecting your and sensitive data.**

**20. Secure Wi-Fi practices are crucial for protecting your **network** and sensitive data.**

# Section 5: Matching

Match the following terms with their corresponding definitions

**Firewall**

**a)**

An attack that aims to make a computer or network resource unavailable to its intended users by overwhelming it with a flood of incoming traffic or requests.

**Two-factor authentication (2FA)**

**b)**

A technique used by cyber attackers to manipulate individuals into divulging sensitive information or performing certain actions.

**Social Engineering**

**c)**

A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules

**Denial of Service (DoS)**

**d)**

A security measure that requires users to provide two different types of identification before granting access to a system or account.

**Encryption**

**e)**

The process of converting plaintext data into a form that cannot be easily understood or deciphered by unauthorized parties.



**Firewall**

**Two-factor authentication (2FA)**

**Social Engineering**

**Denial of Service (DoS)**

**Encryption**

**a)**

**b)**

**d)**

**e)**

An attack that aims to make a computer or network resource unavailable to its intended users by overwhelming it with a flood of incoming traffic or requests.

A technique used by cyber attackers to manipulate individuals into divulging sensitive information or performing certain actions.

A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules

A security measure that requires users to provide two different types of identification before granting access to a system or account.

The process of converting plaintext data into a form that cannot be easily understood or deciphered by unauthorized parties.