Cyber Security

GLOBAL COURSEWARE

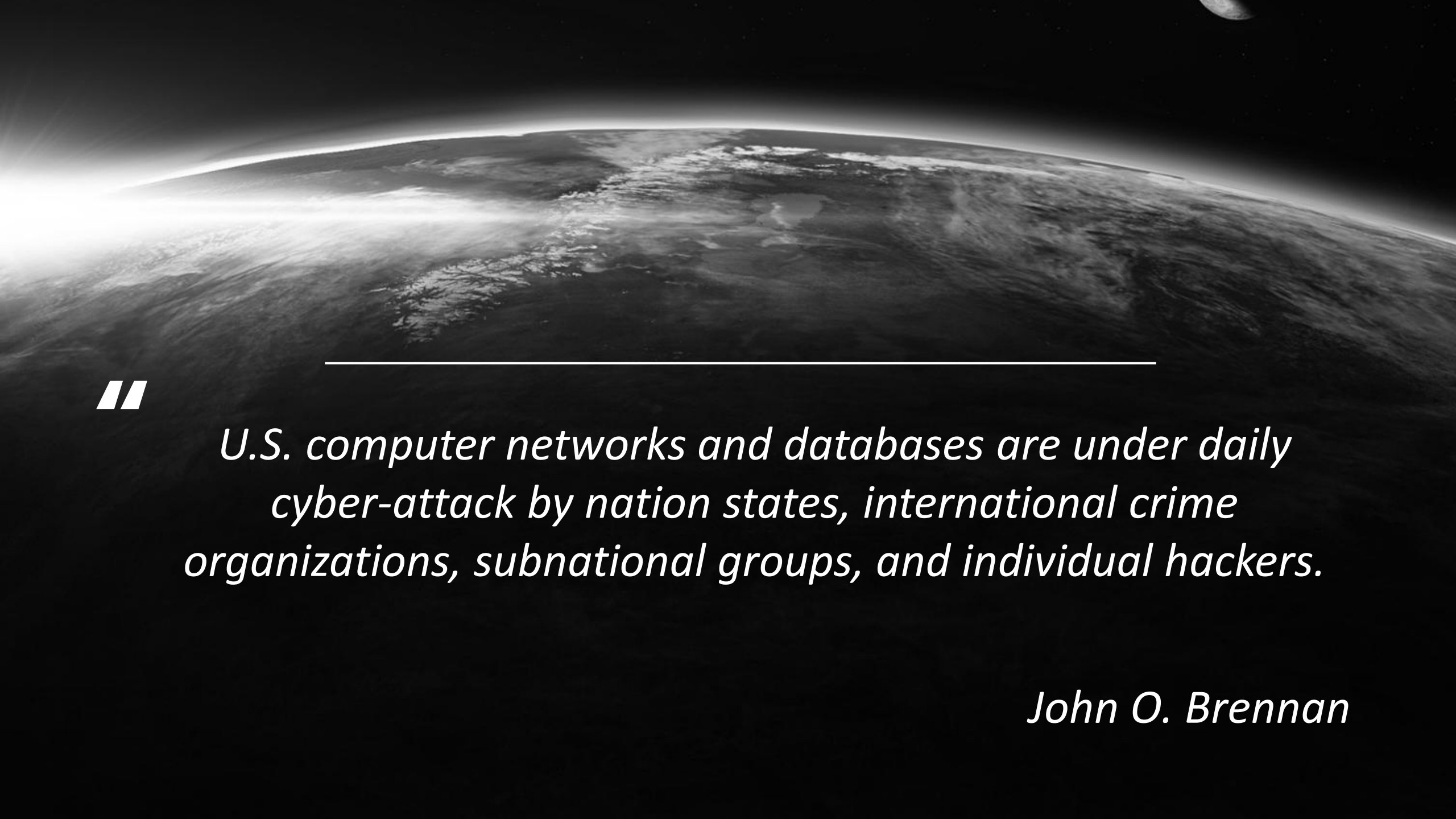
MODULE ONE

Getting Started

Every organization is responsible for ensuring cyber security. The ability to protect its information systems from impairment, or even theft, is essential to success. Implementing effective security measures will not only offer liability protection; it will also increase efficiency and productivity.

Workshop Objectives

- Understand different types of malware and security breaches
- Know the types of cyber-attacks to look out for
- Develop effective prevention methods



"U.S. computer networks and databases are under daily cyber-attack by nation states, international crime organizations, subnational groups, and individual hackers.

John O. Brennan

MODULE TWO

Cyber Security Fundamentals

Before developing and implementing security measures to prevent cyberattacks, you must understand basic concepts associated with cyber security and what cyberattacks are.

What is Cyberspace?

- Networks
- Devices
- Software
- Applications

What is Cyber Security?

The implementation of methods to prevent attacks on a company’s information systems.

Why is Cyber Security Important?

- Credit card and bank details
- Trade secrets
- Intellectual property

What is a Hacker?

- Grey hats: do it “for the fun of it”.
- Black hats: stealing and/or selling data for monetary gain.

Practical Illustration

- What is Cyberspace?
- What is Cyber Security?
- Why is Cyber Security Important?
- What is a Hacker?

Module Two: Review Questions

1. Cyberspace refers to which of the following?

A. Computer-to-computer activity

B. Individual-to-individual activity

C. Supervisor-to-employee activity

D. Computer-to-physical location activity

Module Two: Review Questions

2. What is an item that is included in cyberspace?

A. Network

B. Software

C. Application

D. All of the above

Module Two: Review Questions

3. Why is cyber security implemented?

A. To speed up the network of a company's computers

B. To avoid the disruption of a company's business

C. To increase the number of clients a company has

D. To lessen the number of employees a company employs

Module Two: Review Questions

4. Cyber security helps control physical access to and prevents danger that may come in from:

A. Hardware

B. Network access

C. Code injection

D. All of the above

Module Two: Review Questions

5. What type of information is NOT secure information that is likely to be compromised in a data security breach?

A. Intellectual property

B. Credit card information

C. The name of a company's CEO

D. Social security numbers

Module Two: Review Questions

6. What is the main purpose of computer sabotage?

A. To disable a company's computers or networks to prevent it from conducting business.

B. To disable a company's computers or networks to prevent it from being able to obtain a business license.

C. To disable a company's computers or networks to prevent it from being able to hire employees.

D. To disable a company's computers or networks to prevent it from being able to give its employees raises.

Module Two: Review Questions

7. Why do “grey hat” hackers typically hack into computers?

A. To steal data for monetary gain

B. For the fun of it

C. To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them

D. To sell data for monetary gain

Module Two: Review Questions

8. Why do “white hat” hackers typically hack into computers?

A. To steal data for monetary gain

B. For the fun of it

C. To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them

D. To sell data for monetary gain

Module Two: Review Questions

9. The method(s) of cyber security that a company uses should be tailored to fit the needs of the _____.

A. Hacker

B. Employees

C. Organization

D. Manager

Module Two: Review Questions

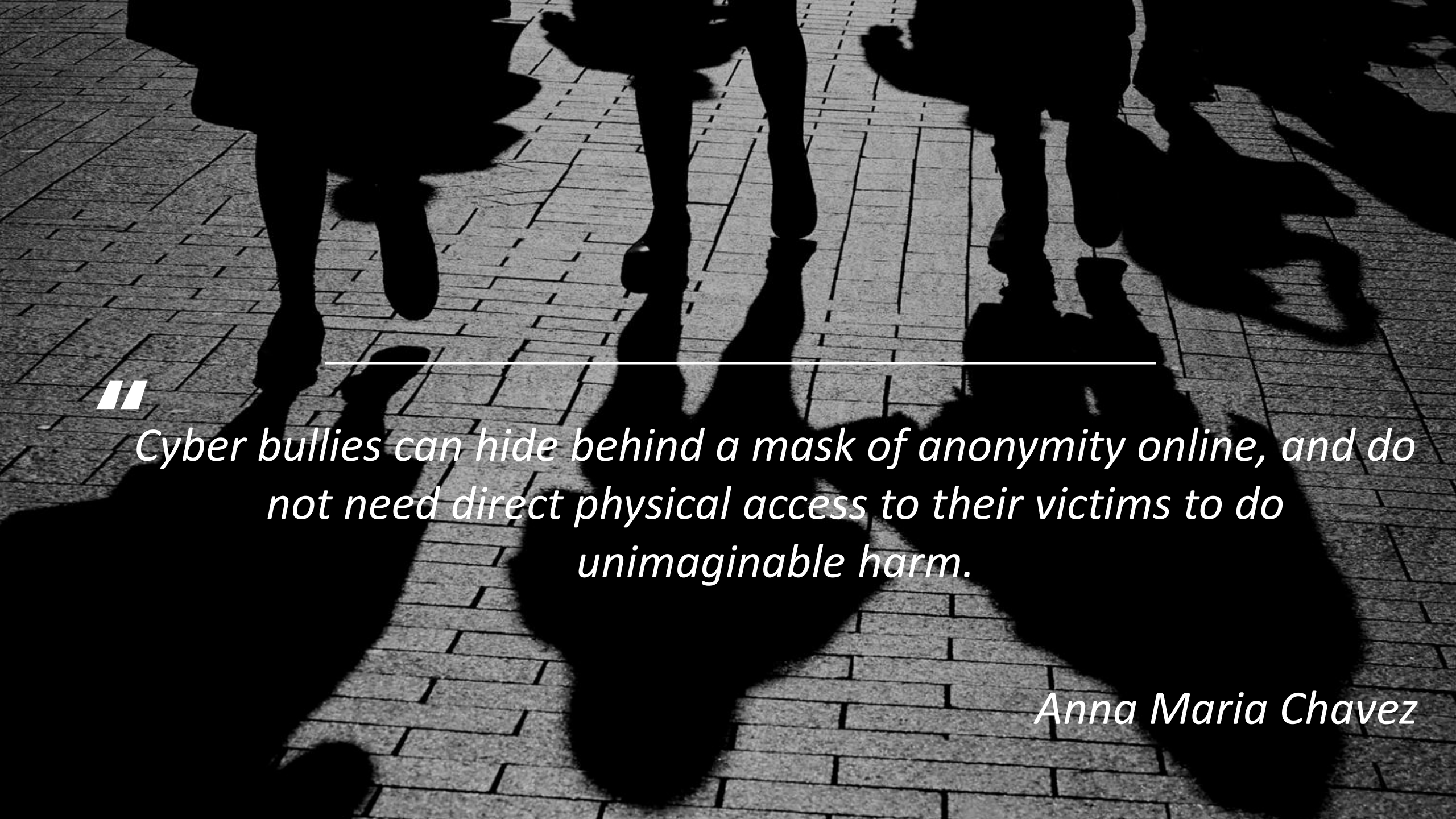
10. _____ is the environment where computer transactions take place.

A. An office

B. Cyberspace

C. A mall

D. None of the above



"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm.

Anna Maria Chavez

MODULE THREE

Types of Malware

Malware, or malicious software, is intrusive software, used to perform actions such as interrupting computer operations and obtaining sensitive information.

Worms

- Bandwidth consumption
- Stopping active anti-malware service
- Immobilizing Safe Mode
- Hindering Windows auto update

Viruses

- Corrupting files
- Computer slowdown
- Taking over basic functions of the operating system

Spyware

- Collecting personal information
- Installing unsolicited software
- Redirecting web browsers

Trojans

- Crashing the computer
- Deleting files
- Corrupting data

Practical Illustration

- Worms
- Viruses
- Spyware
- Trojans

Module Three: Review Questions

1. How do worms work?

A. They are always downloaded as email attachments

B. They are automatically installed on every computer

C. They must attach themselves to existing programs in order to spread

D. They reproduce themselves to infect other computers

Module Three: Review Questions

2. Which of the following does the lesson NOT list as damage that worms can cause?

A. Bandwidth consumption

B. Immobilizing Safe Mode

C. Corrupting files

D. Stopping active anti-malware service

Module Three: Review Questions

3. When can infected files infect other computers?

A. When the file is shared with other computers

B. Whether or not the file is shared with other computers

C. They automatically infect other computers within the same network of the originally infected computer

D. Never

Module Three: Review Questions

4. Which of the following does the lesson NOT list as damage that viruses can cause?

A. Computer slowdown

B. Corrupting files

C. Taking over basic functions of the operating system

D. Bandwidth consumption

Module Three: Review Questions

5. Spyware is commonly used to bombard the user with:

A. Emails without attachments

B. Unsolicited text messages

C. Emails with attachments

D. Pop-up ads

Module Three: Review Questions

6. Which of the following does the lesson NOT list as damage that Spyware can cause?

A. Crashing the computer

B. Collecting personal information

C. Installing unsolicited software

D. Redirecting web browsers

Module Three: Review Questions

7. How do Trojans gain access to computers?

A. By being installed via a disk

B. By misleading the user of its true intention

C. By spreading via legitimate email attachments

D. None of the above

Module Three: Review Questions

8. Which of the following does the lesson NOT list as damage that Trojans can cause?

A. Crashing the computer

B. Deleting files

C. Corrupting data

D. Redirecting web browsers

Module Three: Review Questions

9. ”Malware” is the shortened form of _____.

A. Malignant software

B. Malicious software

C. Maleficent software

D. None of the above

Module Three: Review Questions

10. A computer _____ is an independent malware program that reproduces itself to infect other computers.

A. Virus

B. Worm

C. A and B

D. Neither A nor B

Choosing a hard-to-guess, but easy-to-remember password is important!

Kevin Mitnick

MODULE FOUR

Cyber Security Breaches

Whether the data is released intentionally or unintentionally, the consequences can have long-lasting effects, from harassment to identity theft.

Phishing

Cyber criminals who use phishing scams aim to obtain personal information by appearing to be a legitimate source.

Identity Theft

- Be mindful of phishing websites
- Utilize an Anti-virus / Anti-malware program
- Don’t respond to unsolicited requests

Harassment

- Do not immediately respond
- Tell the cyberbully to stop
- Get the authorities involved

Cyber Stalking

The cyber stalker’s intention is typically to intimidate, or in some way influence, the victim.

Practical Illustration

- Phishing
- Identity Theft
- Harassment
- Cyber Stalking

Module Four: Review Questions

1. How do phishing scam criminals attract their victims?

A. By appearing to be a legitimate source

B. By threatening them

C. A and B

D. Neither A nor B

Module Four: Review Questions

2. What is not one of the ways phishing uses individuals' information?

A. To obtain identifying information such as social security number, for malicious purposes

B. To commit crimes in the person's name

C. To steal banking details for personal gain

D. To keep the person's information safe

Module Four: Review Questions

3. What quote is mentioned in the “Identity Theft” lesson?

A. Identity theft is a serious crime that affects millions of Americans each year

B. I don’t need to worry about identity theft because no one wants to be me

C. An ounce of prevention is worth a pound of cure

D. If we don’t act now to safeguard our privacy, we could all become victims of identity theft

Module Four: Review Questions

4. Of the following, which is not mentioned in the “Identity Theft” lesson as a way to help prevent identity theft?

A. Be mindful of phishing websites

B. Protect your passwords

C. Utilize an Anti-Virus / Anti-Malware program

D. Don’t respond to unsolicited requests for secure information

Module Four: Review Questions

5. What is the first thing to do when you discover you have been a victim of cyber bullying?

A. Respond immediately

B. Compose yourself before responding

C. Call the police

D. Shut down your computer

Module Four: Review Questions

6. What is a characteristic of cyber bullying?

A. Can affect companies as well as individuals

B. Is limited to adults

C. Is limited to teenagers

D. Only affects companies

Module Four: Review Questions

7. What does the lesson mention on how cyberstalking is punishable?

A. Monetary penalties only

B. Monetary penalties and jail time

C. Restraining order and monetary penalties

D. Restraining order and jail time

Module Four: Review Questions

8. What is not mentioned in the “Cyberstalking” lesson as an anti-stalking tip?

A. Log out of programs before stepping away from your desk

B. Do not leave on your computer through the night

C. Protect passwords

D. Keep security software updated

Module Four: Review Questions

9. Receiving an email that says, “We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity”, is MOST likely characteristic of what?

A. Cyber bullying

B. Cyber stalking

C. Harassment

D. Phishing

Module Four: Review Questions

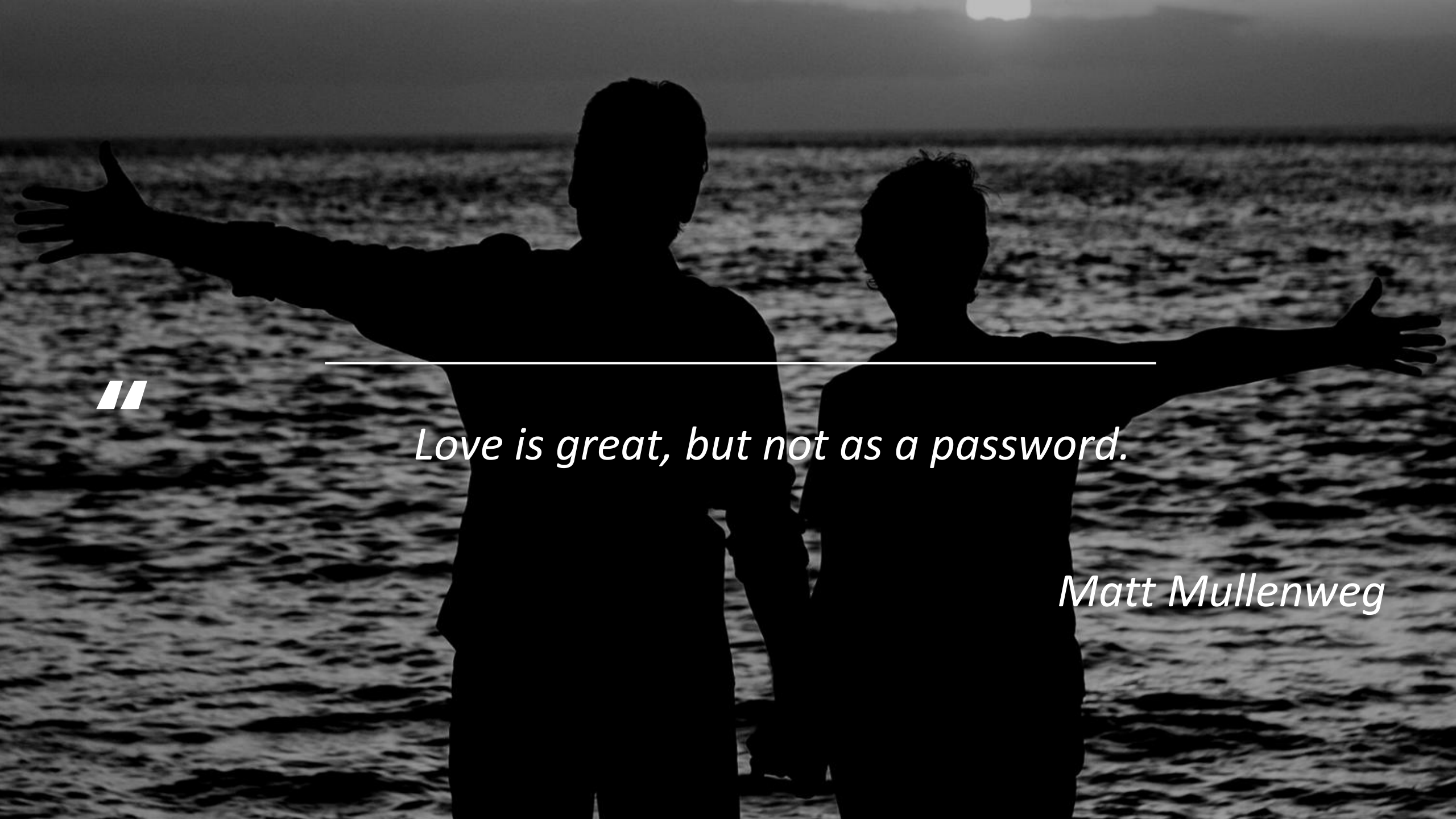
10. Cyber _____ can be intentional or unintentional.

A. Bullying

B. Stalking

C. Security breaches

D. Phishing



Love is great, but not as a password.

Matt Mullenweg

MODULE FIVE

Types of Cyber Attacks

Cyber attacks are orchestrated by individuals or groups to destroy the information systems, networks, etc. of others.

Passwords Attacks

- Include upper- and lower-case letters, numbers, and symbols
- Craft a password that is long
- Regularly update your password

Denial of Service Attacks

- Network performs slowly
- A specific website is inaccessible
- No websites are accessible

Passive Attack

A passive attack is conducted to simply find the vulnerabilities of a system, but not change any data at that time.

Penetration Testing

- Determine the bearing an attack will have on a company
- Assess the company's network risk management capabilities

Practical Illustration

- Password Attacks
- Denial of Service Attacks
- Passive Attack
- Penetration Testing

Module Five: Review Questions

1. You should create a password that is:

A. Easy for you to remember and easy for others to figure out

B. Difficult for you to remember but easy for others to figure out

C. Easy for you to remember but difficult for others to figure out

D. Difficult for you to remember and difficult for others to figure out

Module Five: Review Questions

2. What should your password include?

A. Upper- and lower-case letters

B. Upper- and lower-case letters, numbers, and symbols

C. Numbers and symbols

D. Upper case letters, numbers, and symbols

Module Five: Review Questions

3. What is a denial-of-service attack?

A. An attack that prevents unintended users from being able to access a network

B. An attack that prevents users from being able to access a network in the early morning hours only

C. An attack that prevents users from being able to access a network in the late-night hours only

D. An attack that prevents intended users from being able to access a network

Module Five: Review Questions

4. Which of the following is not mentioned in the “Denial of Service Attack” lesson as damage that denial of service attacks can cause?

A. Network performs slowly

B. A particular website is inaccessible

C. Receiving a large amount of spam emails

D. None of the above

Module Five: Review Questions

5. What is the purpose of a passive attack?

A. To find network vulnerabilities and immediately change data

B. To warn the network user of an impending active attack

C. To find network vulnerabilities but not change data at the time

D. To warn the network user of vulnerabilities so the user can fix them

Module Five: Review Questions

6. In the lesson, passive attacks are likened to:

A. Eavesdropping

B. Murder

C. Downloading

D. Overloading

Module Five: Review Questions

7. What is penetration testing used for?

A. In a controlled environment, to find vulnerabilities in the network, but not exploit them

B. In a controlled environment, to find vulnerabilities in the network and exploit those vulnerabilities to see what impact an actual attack would have

C. In an uncontrolled environment, to find vulnerabilities in the network and exploit those vulnerabilities to see what impact an actual attack would have

D. In an uncontrolled environment, to find vulnerabilities in the network, but not exploit them

Module Five: Review Questions

8. Which of these is discussed in the “Penetration Testing” lesson as a reason that companies implement such testing?

A. Establish the likelihood of a specific attack occurring

B. Detect high risk vulnerabilities that can result from a grouping of low-risk vulnerabilities that take place in a particular pattern

C. Determine the bearing an attack will have on a company

D. All of the above

Module Five: Review Questions

9. _____ are orchestrated by individuals or groups to destroy the information systems, networks, etc. of others.

A. Cyber attacks

B. Personal attacks

C. A and B

D. None of the above

Module Five: Review Questions

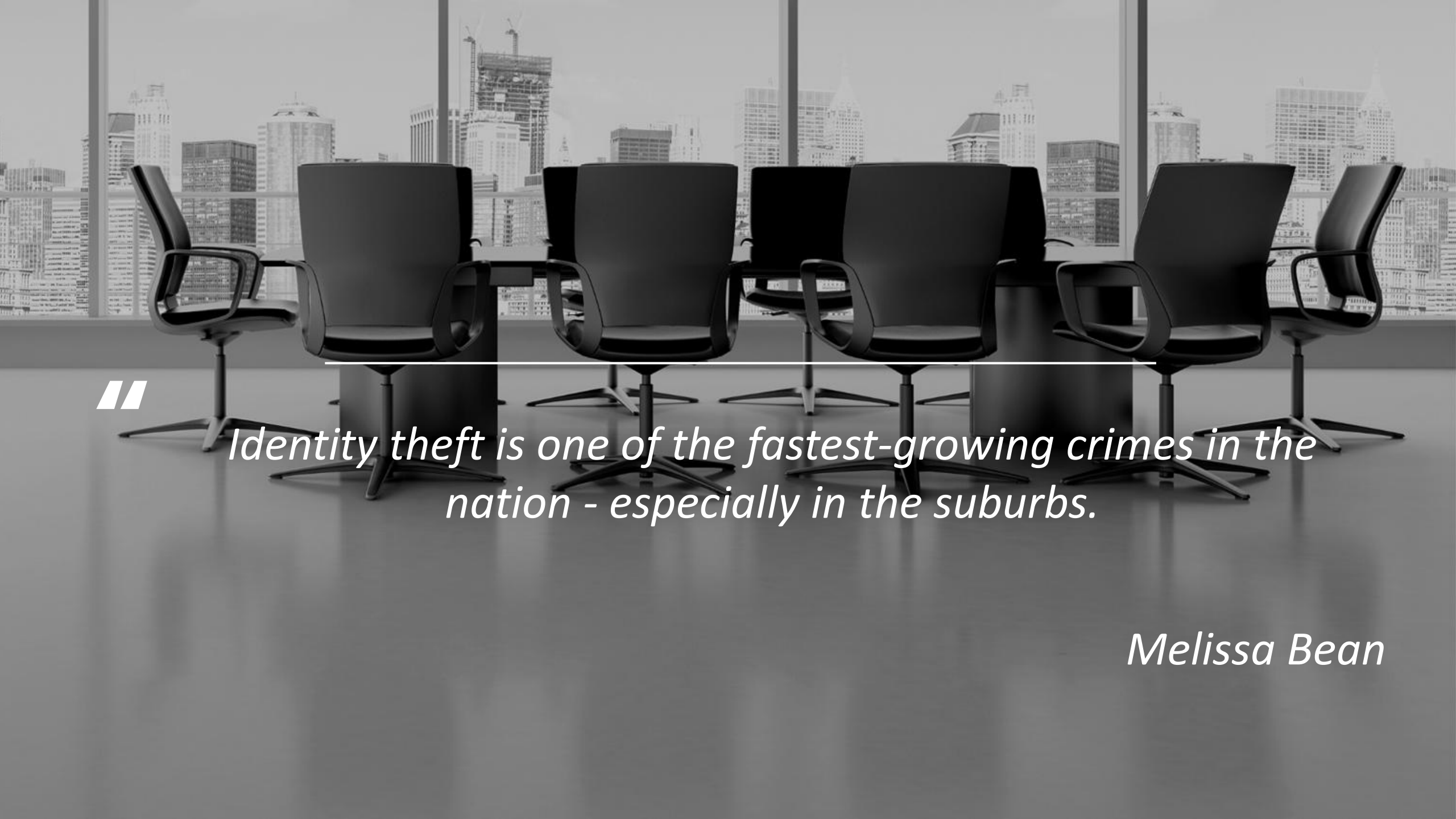
10. Receiving a large amount of spam mail and being locked out of the system after putting in the correct password, but not given access are characteristic of which of the following?

A. Password attack

B. Denial of service

C. Denial of service and password attack

D. None of the above



"Identity theft is one of the fastest-growing crimes in the nation - especially in the suburbs.

Melissa Bean

MODULE SIX

Prevention Tips

It may not be possible to completely avoid falling victim to cybercrime.

Having a tool kit of prevention methods could help your organization minimize the risk of cyber crimes.

Craft a Strong Password

Avoid using common words or consecutive characters to make up your password (e.g., Do not use “password” as your password. Do not use a password such as Office111).

Two- Step Verification

- Token
- Key
- Password
- Pin
- Fingerprint
- Voice recognition

Download Attachments With Care

It’s important to always download email attachments with care, even if the email appears to be from a credible source.

Question Legitimacy of Websites

Opening some sites could lead to damage, such as slowing down the speed of your computer or the loss of files or even stolen identity.

Practical Illustration

- Craft a Strong Password
- Two-Step Verification
- Download Attachments with Care
- Question Legitimacy of Websites

Module Six: Review Questions

1. What is the best way to store a password?

A. On a sticky note, on your desk

B. In your memory

C. In your phone

D. In a notebook located in an unlocked desk

Module Six: Review Questions

2. When is it best to use one password for all of your accounts?

A. If you have no more than two accounts

B. If you have no more than three accounts

C. Never

D. If you have no more than four accounts

Module Six: Review Questions

3. In the “Two-Step Verification” lesson, which of these is mentioned as something that may be used for authentication purposes?

A. Token

B. Key

C. Password

D. All of the above

Module Six: Review Questions

4. The “Two-Step Verification” lesson states that which of these can be used to confirm an individual’s identity?

A. PIN

B. Fingerprint

C. Voice recognition

D. All of the above

Module Six: Review Questions

5. What is true of an email attachment with an extension of .doc?

A. It could be a Trojan

B. It should never be downloaded

C. It will always be a legitimate attachment

D. It should only be downloaded if it is sent from a co-worker

Module Six: Review Questions

6. What is a way to protect yourself when it comes to opening attachments?

A. Regularly update software patches

B. Go with your gut

C. Save and scan the true sender of the attachment

D. All of the above

Module Six: Review Questions

7. Opening a website that appears to be legitimate but is a spoof can do all of the following, except:

A. Slow down the speed of your computer

B. Cause a loss of files

C. Increase the speed of your computer

D. Cause a stolen identity

Module Six: Review Questions

8. Which of these is not mentioned as a precautionary measure to avoid opening a spoof website?

A. Type the complete URL in the browser

B. Question the intention of the sender of an unsolicited request to visit a website

C. Ensure your Anti-Virus / Anti-Spyware is up-to-date

D. Visit the website from at least two different computers to make sure it is legitimate

Module Six: Review Questions

9. What can help your organization minimize risk?

A. Research the federal law

B. Research state laws

C. Having a tool kit of prevention methods

D. None of the above

Module Six: Review Questions

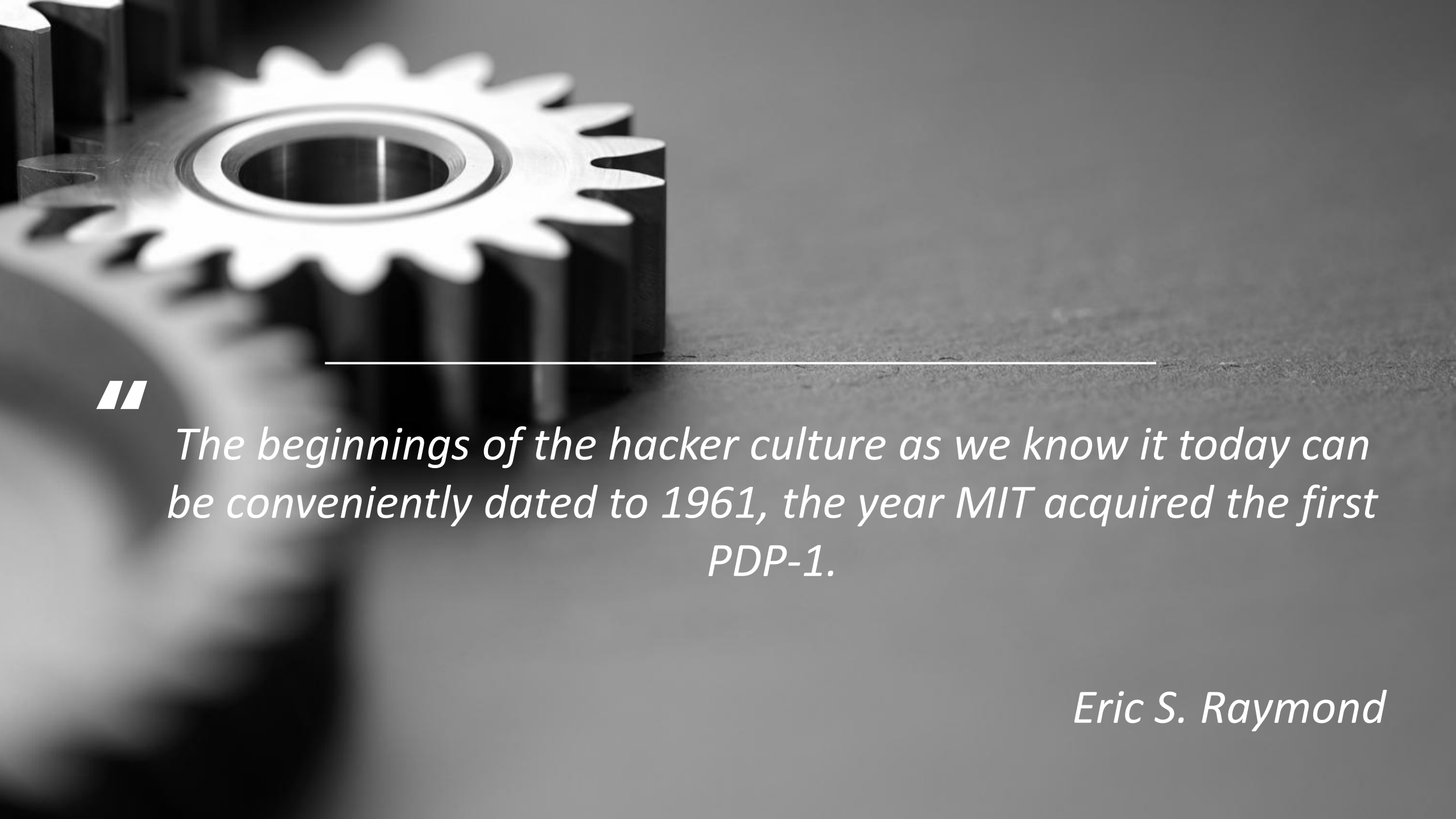
10. One of the easiest steps to keeping your data safe is to craft solid login _____.

A. Credentials

B. Identification

C. Name

D. Password



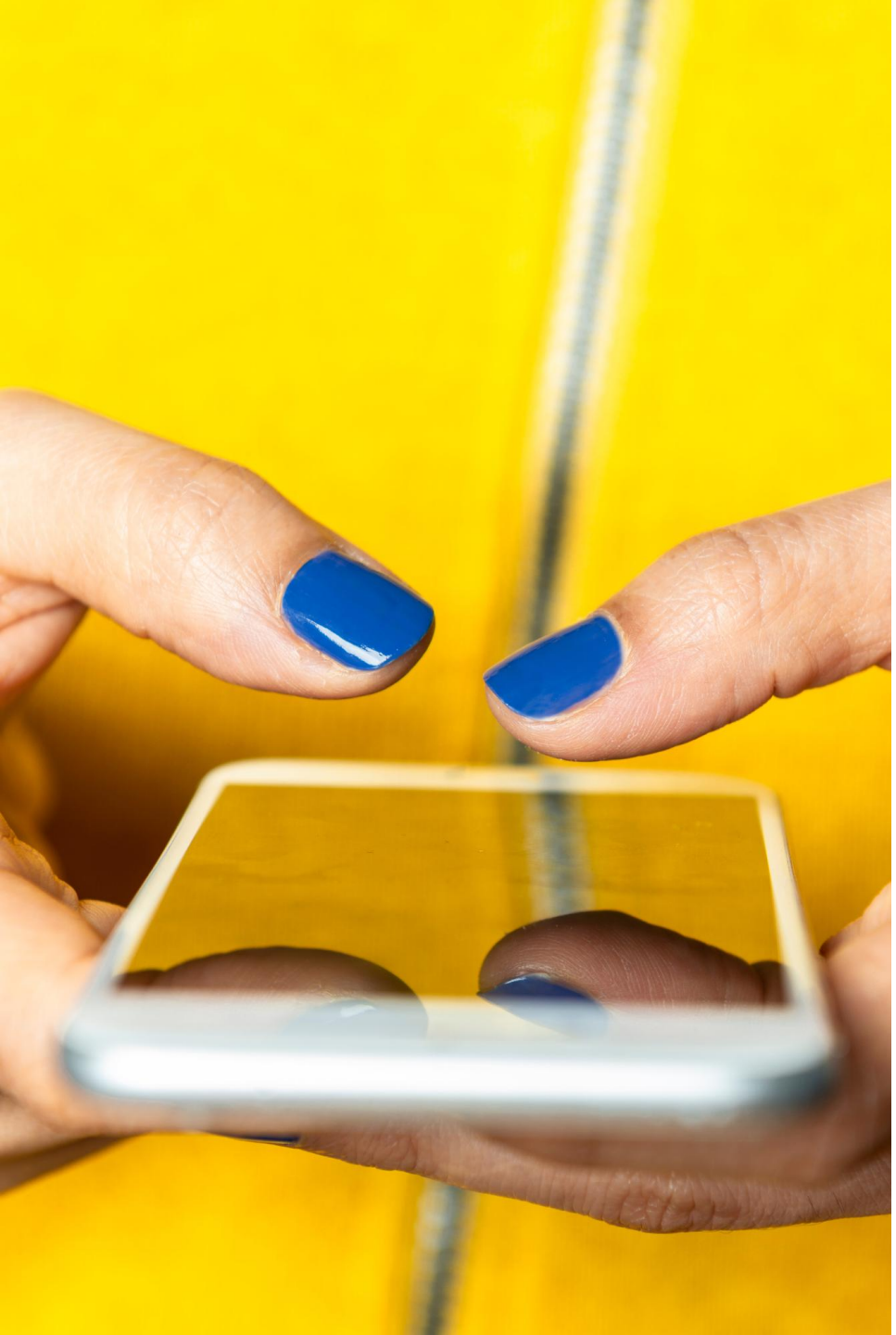
"The beginnings of the hacker culture as we know it today can be conveniently dated to 1961, the year MIT acquired the first PDP-1.

Eric S. Raymond

MODULE SEVEN

Mobile Protection

It is just as important to protect your Smartphone as it is your computer. With phones having many of the same capabilities as computers, they are open to many of the same vulnerabilities that computers face.



No Credit Card Numbers

As easy as it is for you to access these numbers, it is easy for someone who means harm to access them.

Place Lock on Phone

Avoid using common words or consecutive characters to make up your password.

Don’t Save Passwords

- Treat them as you would other important documents by locking them in a safe or drawer that requires a key
- Invest in a password manager service

No Personalized Contacts Listed

Someone who doesn’t have permission to touch your phone may decide to go through your contact list.

Practical Illustration

- No Credit Card Numbers
- Place Lock on Phone
- Don’t Save Passwords
- No Personalized Contacts Listed

Module Seven: Review Questions

1. Credit card numbers:

A. Should only be stored in your phone if you have less than three credit cards

B. Should only be stored in your phone if you have less than two credit cards

C. Should always be stored in your phone

D. Should not be stored in your phone, if possible

Module Seven: Review Questions

2. What is a way to safeguard credit card information that you must store on your phone?

A. Encryption

B. Tokenization

C. A and B

D. Neither A nor B

Module Seven: Review Questions

3. When setting up a lock on your phone that can be opened with a password:

A. Use a password that is the same as all of your other passwords

B. Use a password that is different from all of your other passwords

C. Use a password that has no more than five characters

D. Use a password that has no more than three characters

Module Seven: Review Questions

4. To create a strong password, it should have:

A. Letters and numbers

B. Numbers and symbols

C. Letters, numbers, and symbols

D. Letters and symbols

Module Seven: Review Questions

5. What should be your back-up method if you cannot remember your password?

A. Write down and place in a secure location

B. Save it on your phone

C. Write it down and leave it with a person you trust

D. Any of the above

Module Seven: Review Questions

6. The “Don’t Save Passwords” lesson states that passwords should be secured where?

A. In a co-worker’s files

B. On the main screen of your phone

C. In a closet

D. In a safe

Module Seven: Review Questions

7. What is the name of the person in the contact list?

A. Bill Johnson

B. John Taylor

C. Jim Smith

D. Bob Jones

Module Seven: Review Questions

8. What was the job title of the person in the contact list?

A. Quality representative

B. Manager

C. Account manager

D. Client relations representative

Module Seven: Review Questions

9. What should you NOT save on your phone?

A. Credit card information

B. Passwords for social media accounts

C. Your boss' birthday

D. The address to a client's office

Module Seven: Review Questions

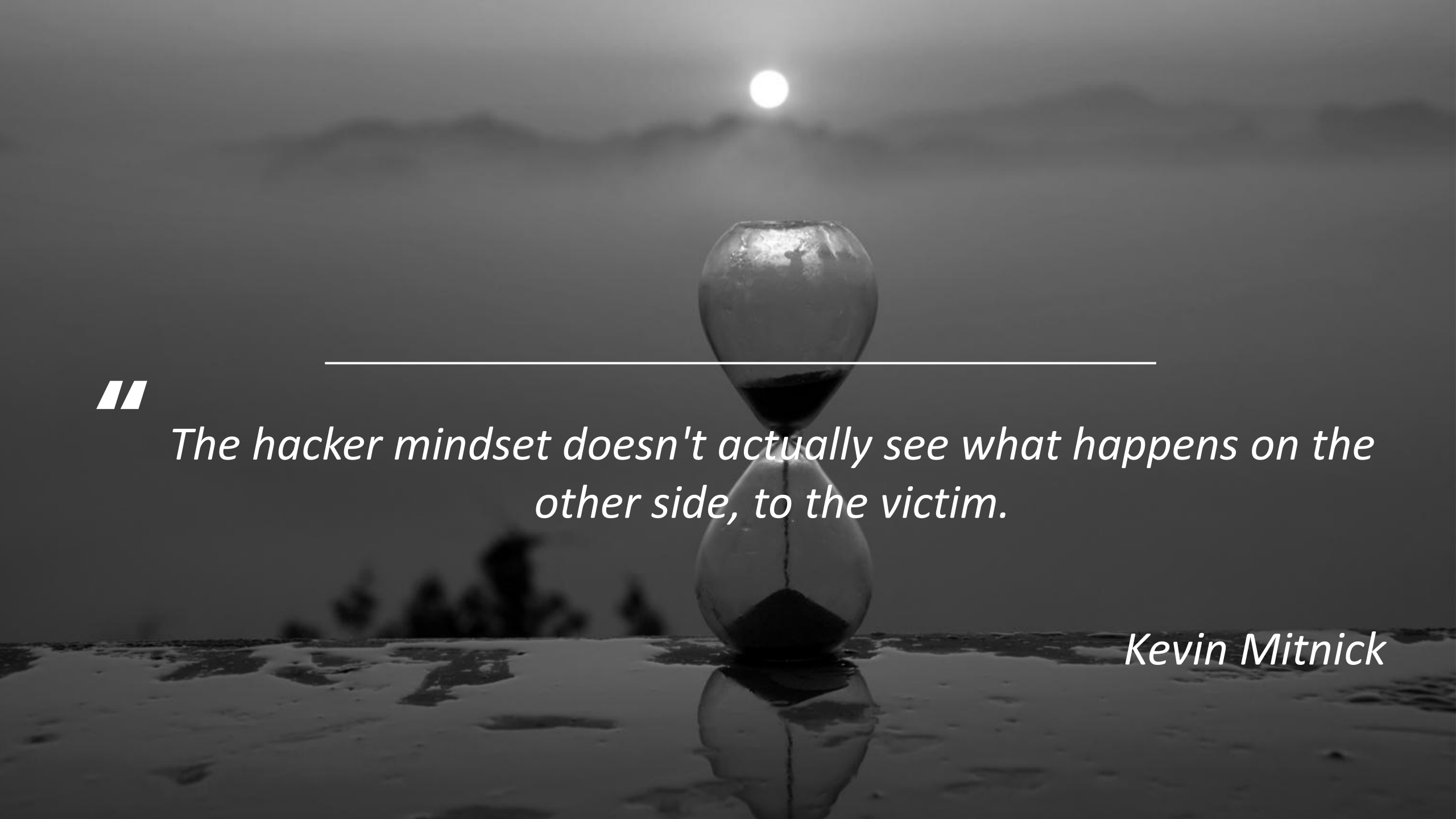
10. How can you protect your phone privacy?

A. Recharge phone every three hours

B. Only use phone after 2:00 p.m.

C. Save passwords on phone

D. Lock phone when not in use



"The hacker mindset doesn't actually see what happens on the other side, to the victim.

Kevin Mitnick

MODULE EIGHT

Social Network Security

Many people forget that with social networking, revealing too much information about oneself could still lead to dangerous situations, such as social engineering attacks.

Don’t Reveal Location

Use your creativity to make a fake location or input a city/state different from where you are actually located.

Keep Birthdate Hidden

If you absolutely must list your birthdate, do not include the year.

Have Private Profile

- Facebook
- Instagram
- Twitter
- Google+
- LinkedIn
- Pinterest

Don’t Link Accounts

Linking social media accounts makes it easier for thieves to find you.

Practical Illustration

- Don’t Reveal Location
- Keep Birthdate Hidden
- Have Private Profile
- Don’t Link Accounts

Module Eight: Review Questions

1. What is the MOST effective thing to do if a social media site requires you to put in your address?

A. Put in your actual location

B. Put in a fake address

C. Contact customer service and complain

D. Refuse to open an account

Module Eight: Review Questions

2. Which of these is NOT mentioned in the “Don’t Reveal Location” lesson of potential things that can happen as a result of inputting your real location?

A. Burglary

B. Harassment

C. Stalking

D. Stolen identity

Module Eight: Review Questions

3. If your birthday is visible on your account, what part of it should you not include?

A. Month

B. Day

C. Year

D. Day of the week you were born

Module Eight: Review Questions

4. The first sentence of the “Keep Birthdate Hidden” lesson says, “Giving away your birthday seems like a _____ act...”

A. Harmless

B. Wise

C. Foolish

D. Noble

Module Eight: Review Questions

5. Which of these is NOT mentioned in “Have Private Profile” as one of the common social media platforms used?

A. Facebook

B. YouTube

C. Instagram

D. Twitter

Module Eight: Review Questions

6. Of the following, which is NOT listed in “Have Private Profile” as a common social media website?

A. Google+

B. LinkedIn

C. Flickr

D. Pinterest

Module Eight: Review Questions

7. You should:

A. Always link your business and personal accounts

B. Never link your business and personal accounts

C. Only link your business and personal accounts if you have only one of each

D. Only link your business and personal accounts if you have less than three of each

Module Eight: Review Questions

8. Which of these is NOT listed as a reason to not link your social media accounts?

A. Decreased risk of identity theft

B. Automated posting

C. Same messages across different platforms

D. Increased risk of identity theft

Module Eight: Review Questions

9. This seems like an issue of _____, but many need to be reminded that revealing your location to strangers is never a good idea.

A. Legal

B. Common sense

C. Illegal

D. None of the above

Module Eight: Review Questions

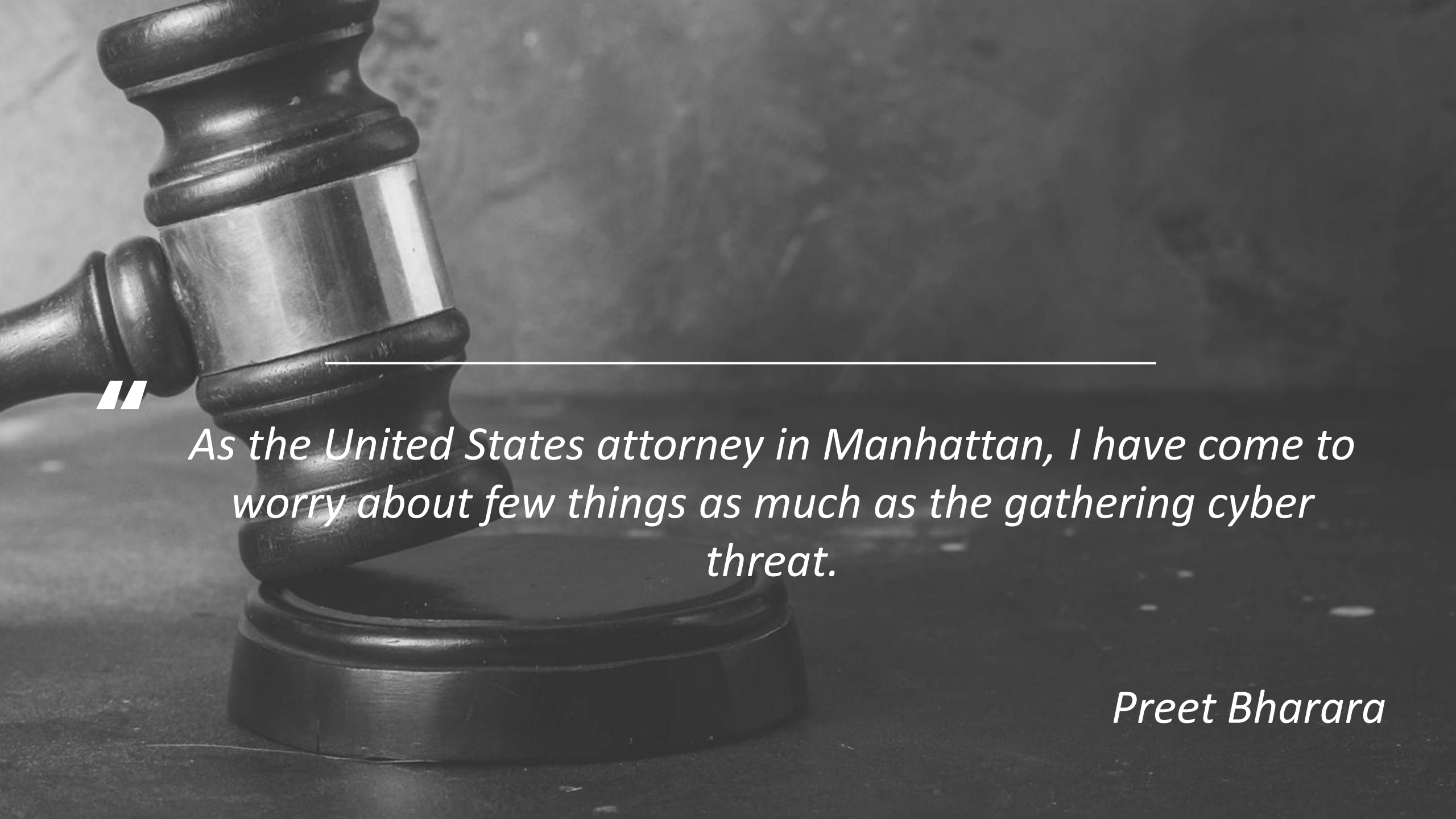
10. The Internet is a _____ source.

A. Private

B. Public

C. Personal

D. Practical



"As the United States attorney in Manhattan, I have come to worry about few things as much as the gathering cyber threat.

Preet Bharara

MODULE NINE

Prevention Software

While you may not be able to completely avoid these risks, there are many ways to lessen your exposure to threats, vulnerabilities, and attacks.

Firewalls

Firewalls use pre-set security rules to keep track of, and regulate, the incoming and outgoing traffic of your network system.

Virtual Private Networks

- Internet Protocol Security
- Layer 2 Tunneling Protocol
- Point-to-Point Tunneling Protocol

Anti-Virus & Anti-Spyware

- McAfee
- Kaspersky
- Bitdefender
- Norton

Routine Updates

- High priority
- Suggested
- Drivers

Practical Illustration

- Firewalls
- Virtual Private Networks
- Anti-Virus & Anti-Spyware
- Routine Updates

Module Nine: Review Questions

1. Which of the following are two types of firewalls?

A. Network and host-based

B. Anti-Virus and Anti-Spyware

C. Network and Internet

D. Host-based and Intranet

Module Nine: Review Questions

2. What are firewalls designed to do?

A. Keep track of but not regulate incoming and outgoing traffic of your network system

B. Keep track of incoming traffic of your network system

C. Keep track of and regulate incoming and outgoing traffic of your network system

D. Keep track of outgoing traffic of your network system

Module Nine: Review Questions

3. An example of using a VPN is a company that gives its employees access to its Intranet while not inside of the office. What type of VPN is this?

A. Site-to-site

B. Remote access

C. Public access

D. On-site access

Module Nine: Review Questions

4. Of the following, which is an actual VPN protocol?

A. Internet Protocol Security

B. Layer 2 Tunneling

C. Point-to-Point Tunneling

D. All of the above

Module Nine: Review Questions

5. What are threats that Anti-Virus software protects against?

A. Trojans

B. Viruses

C. Browser hijackers

D. All of the above

Module Nine: Review Questions

6. Which of these companies offers Anti-Virus and Anti-Spyware software?

A. McAfee

B. Norton

C. Kaspersky

D. All of the above

Module Nine: Review Questions

7. Which of these is typically the MOST complicated update to install?

A. High priority

B. Suggested

C. Drivers

D. None of the above

Module Nine: Review Questions

8. How often do operating systems release updates?

A. Regularly

B. Once every year

C. Once every two years

D. Once every three years

Module Nine: Review Questions

9. What is a potential danger when using the internet?

A. Takeover of your computer system

B. Identity theft

C. A and B

D. None of the above

Module Nine: Review Questions

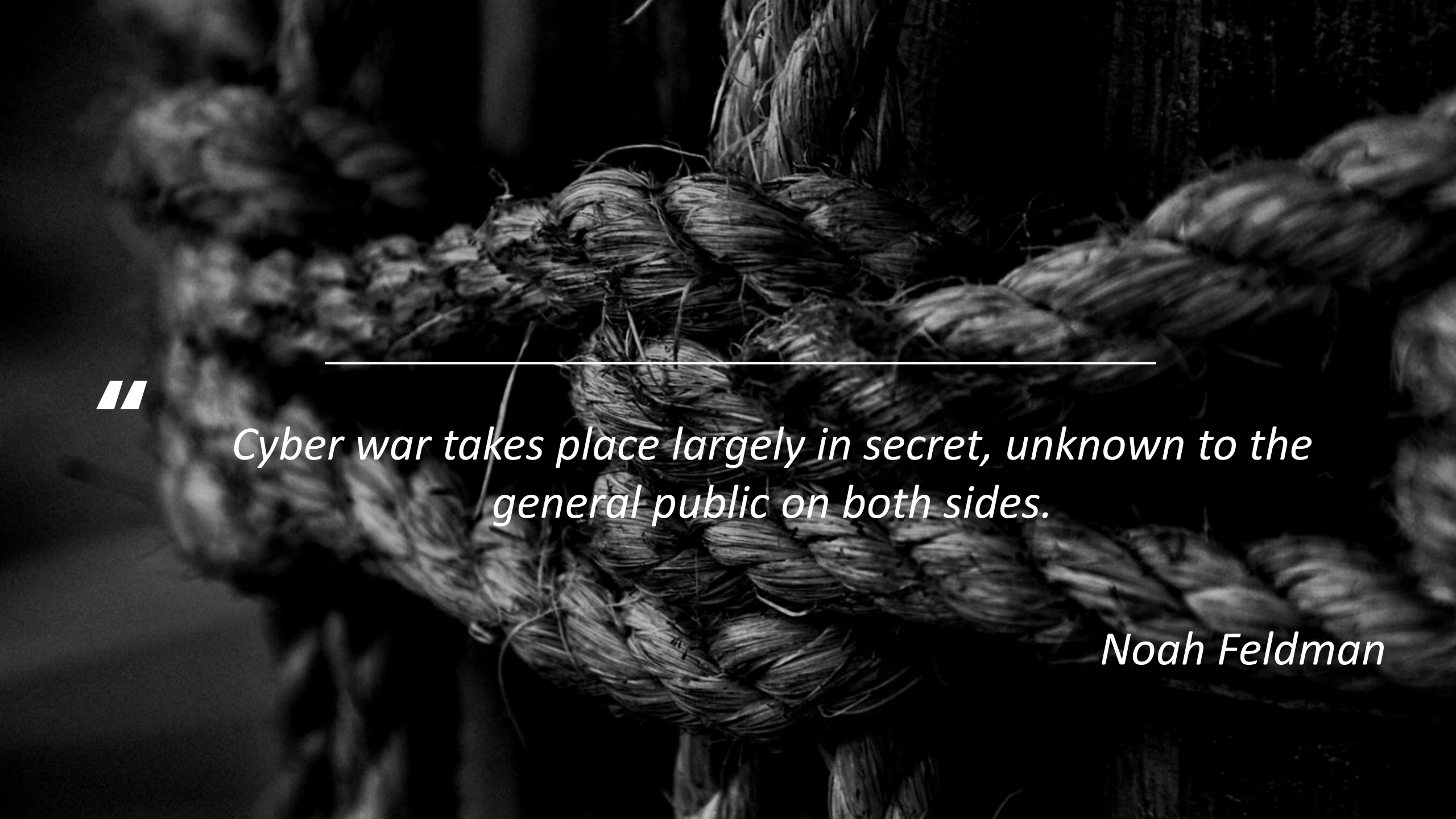
10. Firewalls use pre-set security rules to keep track of, and regulate, the incoming and outgoing traffic of your _____.

A. Social media

B. Network system

C. LinkedIn account

D. Amazon purchases



Cyber war takes place largely in secret, unknown to the general public on both sides.

Noah Feldman

MODULE TEN

Critical Cyber Threats

Critical cyber threats are those that if carried out, could have a debilitating effect on an organization, or even a country.

Critical Cyber Threats

- Dams
- Finance
- Healthcare
- Government facilities

Cyber Terrorism

Cyber terrorism is cyber threats/attacks on a large scale.

Cyber Warfare

Cyber warfare is a means of war against another state or country to damage that other state/country's information networks.

Cyber Espionage

The purpose of cyber espionage is to obtain the secrets of another, without their permission.

Practical Illustration

- Critical Cyber Threats
- Cyber Terrorism
- Cyber Warfare
- Cyber Espionage

Module Ten: Review Questions

1. According to the “Critical Cyber Threats” lesson, which of these is mentioned as a critical infrastructure?

A. Energy

B. Defense

C. Transportation

D. All of the above

Module Ten: Review Questions

2. Which of the following is NOT listed in “Critical Cyber Threats” as a type of critical infrastructure?

A. Food and agriculture

B. Emergency services

C. Communications

D. None of the above

Module Ten: Review Questions

3. In the white supremacist example of Cyber terrorism, what state's ISP was temporarily disabled?

A. Oregon

B. Massachusetts

C. Alabama

D. New Mexico

Module Ten: Review Questions

4. In the Institute for Global Communications Cyber terrorism example, protesters from what country bombarded the institute with thousands of bogus e-mails?

A. Spain

B. France

C. Nigeria

D. China

Module Ten: Review Questions

5. In the Cyber warfare examples, in 1998, the United States hacked into what country's air defense system?

A. North Korea

B. Russia

C. Serbia

D. Germany

Module Ten: Review Questions

6. A cyber spy network called _____ accessed confidential information belonging to both governmental and private organizations.

A. GhostNet

B. Internet Spy

C. CyberNet

D. Ghost Town

Module Ten: Review Questions

7. In one of the examples in the “Cyber espionage” lesson, an unnamed government official told the Wall Street Journal that cyber spies from which countries had broken into computer systems?

A. Israel and Italy

B. Japan and India

C. Poland and Scotland

D. China and Russia

Module Ten: Review Questions

8. Canadian researchers revealed that a cyber-spy network based in what country had broken into diplomatic computer systems involving 103 different countries?

A. China

B. Ireland

C. Turkey

D. Iraq

Module Ten: Review Questions

9. Critical cyber threats are those that if carried out, could have a debilitating effect on an organization, or even _____.

A. A personal account

B. A country

C. A and B

D. None of the above

Module Ten: Review Questions

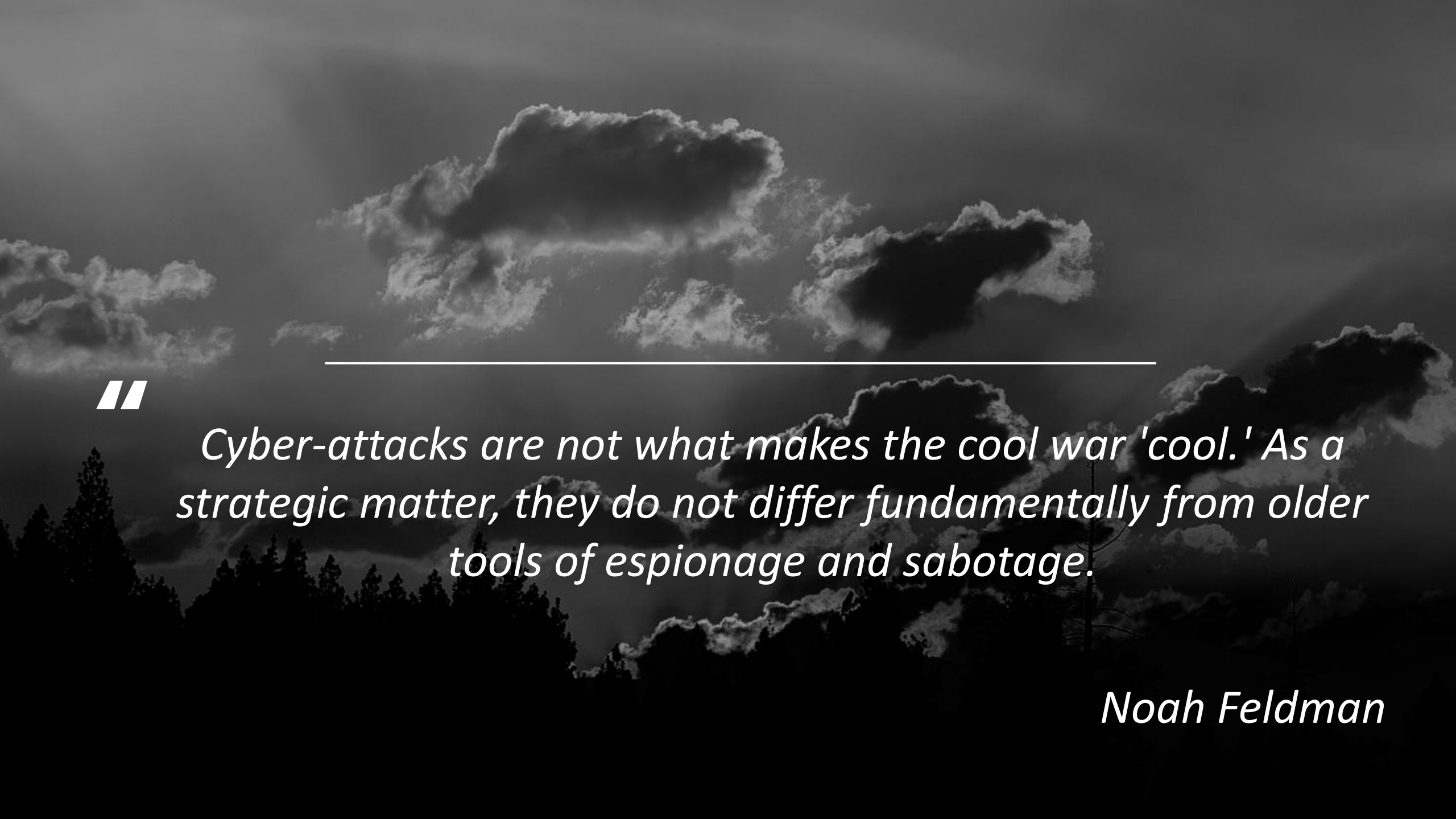
10. _____ are not designed to temporarily disable an organization, but completely destroy it.

A. Viruses

B. Cyber threats

C. A and B

D. None of the above



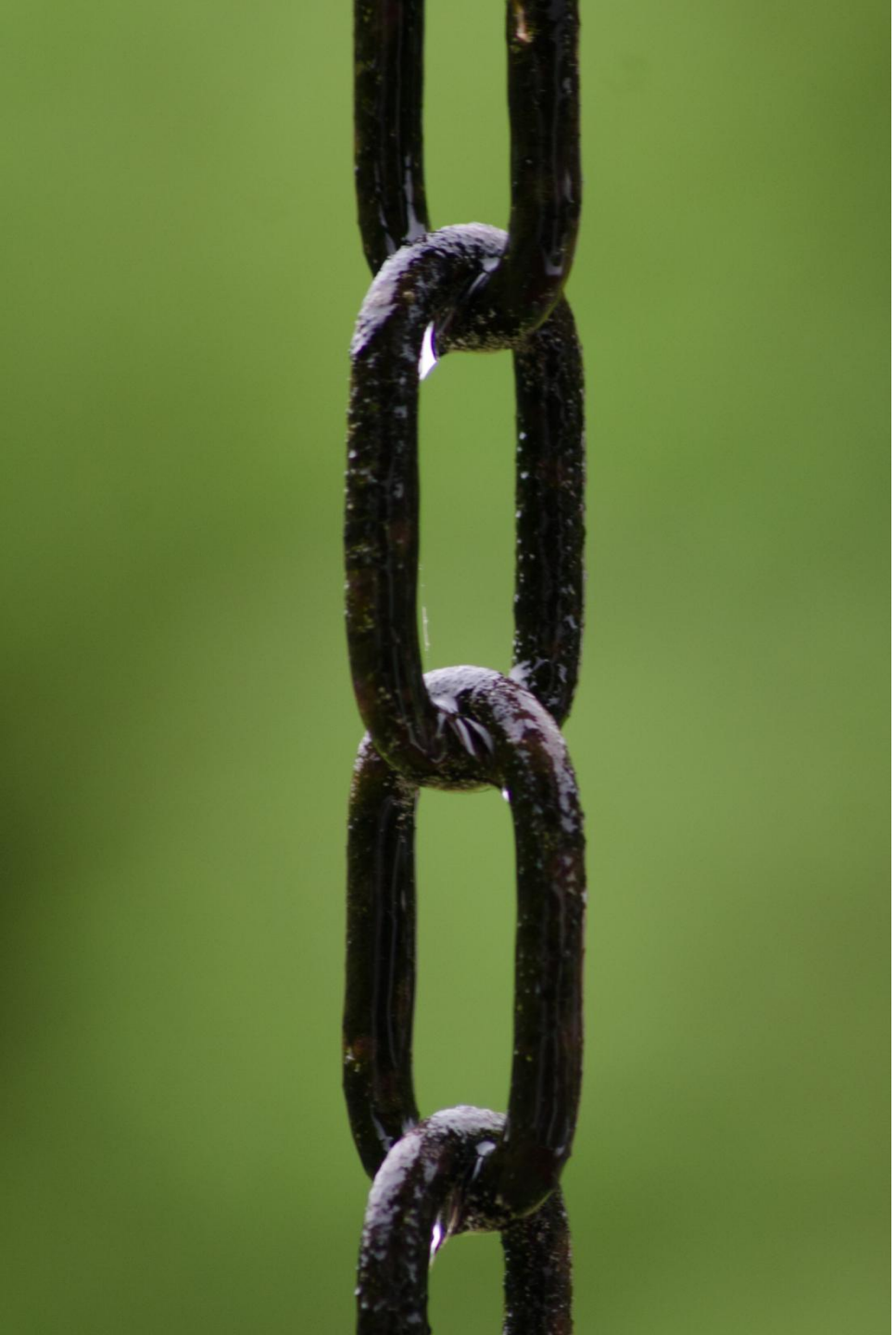
"Cyber-attacks are not what makes the cool war 'cool.' As a strategic matter, they do not differ fundamentally from older tools of espionage and sabotage.

Noah Feldman

MODULE ELEVEN

Defense Against Hackers

“The best defense is a good offense”. Rather than reacting to attacks once they’ve occurred, a wise strategy is to prepare proactive measures, so that if the time comes, you can completely bypass the attack, or lessen the blow of it.



Cryptography

- International Data Encryption Method (IDEA)
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

Digital Forensics

Computer systems have become a tool for committing various crimes.

Intrusion Detection

- Dakota Alert, Inc.
- Juniper Networks
- Linear, LLC
- PureTech Systems, Inc.
- Telguard

Legal Recourse

- Obtaining National Security Information
- Accessing a Computer and Obtaining Information
- Trespassing in a Government Computer

Practical Illustration

- Cryptography
- Digital Forensics
- Intrusion Detection
- Legal Recourse

Module Eleven: Review Questions

1. What is cryptography?

A. Secret method of hearing

B. Secret method of speaking

C. Secret method of writing

D. Secret method of seeing

Module Eleven: Review Questions

2. Which of these is NOT an encryption method mentioned in the “Cryptography” lesson?

A. IDEA

B. YAR

C. AES

D. DES

Module Eleven: Review Questions

3. The “Digital Forensics” lesson says that who collects and analyzes the data?

A. Company CEO

B. Independent forensics specialists

C. Company employees

D. Law enforcement

Module Eleven: Review Questions

4. In the Sharon Lopatka example in “Digital Forensics” lesson, who was found to be the person who murdered her?

A. Robert Glass

B. Lisa Billingsley

C. John Smith

D. Renee Porter

Module Eleven: Review Questions

5. What is NOT a question that the “Intrusion Detection” lesson states that one must ask before investing in an IDS?

A. What does our business need in an IDS?

B. Does state law allow our business to have an IDS?

C. Can we afford an IDS?

D. Will our network support the IDS system?

Module Eleven: Review Questions

6. Which of these companies is mentioned as a manufacturer of IDSs?

A. Dakota Alert, Inc.

B. Juniper Networks

C. Linear, LLC

D. All of the above

Module Eleven: Review Questions

7. The majority of computer hacking crimes are punishable under:

A. Computer Fraud and Abuse Act

B. Civil Rights Act

C. National Security Act

D. Workforce Investment Act

Module Eleven: Review Questions

8. The “Legal Recourse” lesson states there are penalties for committing the following offenses involving computer:

A. Trafficking in Passwords

B. Accessing a Computer to Defraud & Obtain Value

C. Recklessly Damaging by Intentional Access

D. All of the above

Module Eleven: Review Questions

9. What method of defense can help deter hackers?

A. VPN

B. Anti-Virus software

C. Encryption

D. Anti-Spyware software

Module Eleven: Review Questions

10. What do intrusion detection systems do?

A. Notify the intruder that they will be arrested

B. Notify the company of suspicious activity

C. Notify the company that an intrusion report has been sent to the federal government

D. Notify the intruder that the company is aware of their presence and will be fining them

MODULE TWELVE

Wrapping Up

Although this workshop is coming to a close, we hope that your journey to understanding Cyber Security is just beginning.

Words From the Wise

Everybody should want to make sure that we have the cyber tools necessary to investigate cyber-crimes, and to be prepared to defend against them and to bring people to justice who commit it.

- Janet Reno

Somebody could send you an office document or a PDF file, and as soon as you open it, it's a booby trap and the hacker has complete control of your computer.

- Matt Gentile

People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical.

- Frank Abagnale