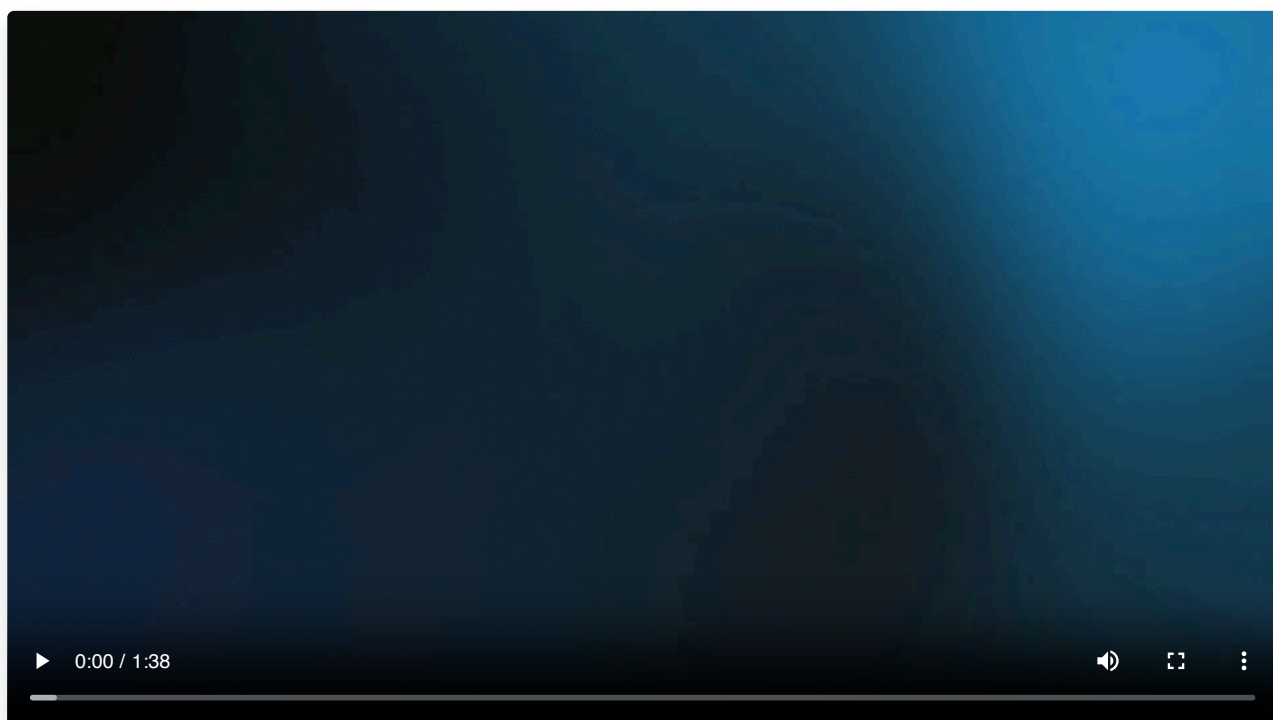


Types of Threat

Textbook

Types of Threat

Learn about the different approaches criminals might take to cause problems with their computers.



Brute Force



[Brute force](#) is when the criminal uses programs designed to figure out passwords or other crucial information through an intense series of trial and error. With the help of computer programs designed to do this efficiently, this approach is highly successful. 2-factor authentication and setting a limit of password attempts greatly reduces the threat of brute-force attempts.

Identity Theft



[Identity theft](#) is when the criminal uses someone else's identity or credentials to give them access to information. This often happens with credit card fraud as the criminal guesses random card numbers and makes big purchases with them. Many banks have systems in place to freeze your card if suspicious activity occurs.

Purchases that were made from a different country, or big purchases that seem different from your usual behavior are often flagged to freeze your account. Depending on your bank, they may give you a call to double check the suspicious behavior. Because of this security measure, you should inform your bank if you plan to travel outside of the country so that your legitimate purchases won't flag your account.

Phishing



[Phishing](#) is when the criminal sends an email or message that seem legitimate in an effort to get information from you. Emails that ask for personal information such as card numbers, bank account information, or personal details should be closely inspected. Common ways to tell if you received a phishing email is that it has interesting offers or eye-catching statements. Another common way to tell is if you have received emails from an unknown or unusual sender, hyperlinks, attachments, or even a sense of urgency to get you to reply.

If you are not sure if an email is legitimate or not, contact your bank or the company in question to double check. Always look for a second opinion to avoid falling for a phishing scam.

Tips to avoid phishing scams:

- **Is anything "off?"** Often they try to look as official as possible. They do this through photoshopping the company images, logos, and names. Look for anything that looks "off" or "not quite right" about the company imagery.
- **Gifts:** Often phishing messages promise gifts. If it sounds too good to be true, it probably is.
- **Call:** If you suspect a message, don't hesitate to call the company directly. Ask them if they've sent out a message like that.
- **Don't Click:** Never visit your bank's website through a link included in a message. These links could lead you to false sources. Type in the website for your bank directly.
- **Safe Websites:** Only enter information into safe websites. Safe websites begin with <https://> The browser should have a little lock symbol next to safe website urls. If there is a link in an email, hover over the URL first because secure websites begin with "HTTPS".
- **Strange Translations:** Because phishing messages come from all over the world, sometimes they are translated poorly. Check for strange grammar or unusual use of words.

- **Be Aware:** Many problems with phishing messages can be easily avoided. Just be cautious and aware and you will make smart choices.
- **Too Good to be True?** If it looks too good to be true, it probably is. Some examples would be an email saying you won a free car or the newest phone! As long as you don't click on any links you should be ok.
- **Change Passwords:** Also remember to change passwords regularly, and never use the same password for multiple accounts.

To prevent phishing attacks you can filter out spam emails from regular ones. Many websites require the users to enter their login info while the user's profile is displayed. That type of system may be open to security attacks.

Follow these suggestions and you will be better equipped to avoid phishing scams.

Smishing

Text message phishing is called [smishing](#), attackers use smishing to catch your attention and trick you into providing your sensitive information. The attackers often pretend to be a government agency, bank, or other companies to make them seem legit. Smishing messages usually ask you to provide usernames and passwords, credit and debit card numbers, PINs, or other private information that scam attackers can use to commit many types of fraud.

Some ways to detect smishing is to keep in mind that most government companies will never call or text you, most companies will send you letters in the mail letting you know that something is wrong with your account, and banks will never ask you through text about your card numbers or pins. Make sure you don't open any links, don't call that number, don't reply, and never give out any private information.

Malware



[Malware](#) is when the criminal creates some sort of software that causes problems. Malware aims to steal, corrupt, or delete important information. This can take many forms and we'll explore a few of them here.

- **Adware:** this is the use of advertising to get access to your computer. This happens when you click on an advertisement. Once you click on it, the malware downloads on your computer and causes problems. The best way to avoid problems from adware is to not click on the ad! But how do you tell which ads are legitimate and which ones are adware? Adware usually appears in the form of a pop up or a window that doesn't close. You can also use some sort of ad blocking software that filters out the majority of these kinds of adware.
- **Bad Bots:** these bits of code called "bots", are designed to repeat a task over and over again, overwhelming a system. The tasks they do are normal, such as submitting a request or creating a log in account. But because it's automated by a computer program, they can duplicate the task so many times that it breaks the system. 2 factor authentication helps prevent this kind of attack as well as using unique passwords for each log in.
- **Ransomware:** the criminal takes your files and encrypts them in a way that they are not usable. Only they have the key to decrypt the files and make them usable again. They then ask for payment to decrypt your files, essentially holding your files ransom. The best way to protect against ransomware is to back up your files often. That way, if your files get held for ransom, you actually already have a copy you can use.
- **Trojans:** these malware attacks disguise themselves as authentic software that you want to download on your computer. But they secretly have an ulterior motive and cause problems on your computer. Or, the trojan software creates an access point for the cyber criminal to get into your files and network. To avoid trojan software, make sure to download software from only reputable sites with a positive reputation.

Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised. Untrustworthy (often free) downloads from freeware or shareware sites can contain malware. Things that sound too good to be true often are.

Keylogging

[Keylogging](#) is usually a subtle form of spyware. Keylogging saves all the characters you type into your device and it is used to steal important information. Keyloggers are activity-monitoring software programs that give hackers access to your personal data. The passwords and debit card numbers you type, the web pages you visit, all happen by logging your keyboard characters. Keylogging is like pressing the keys on a typewriter, every key you press it writes it down.

The software is installed on your computer and records everything you type, which hackers can use. Keylogging is most commonly used with bad intent and is illegal.

But not all types of keylogging is illegal. Most of the time the "Legal" keylogging is used with IT jobs, to troubleshoot issues they may have, and it can also be used at work to make sure you aren't doing something you shouldn't be doing.

To be safer it's better to use virtual keyboards, (like the one on your phone) you can also use a password manager that saves all your passwords so you don't have to type them out. You can also get an Anti-Keylogger which is a software specifically designed to detect keyloggers on a computer, usually comparing all files in the computer against a database of keyloggers, looking for similarities that might indicate the presence of a hidden keylogger, and then alert you.

Security Trade Offs

Sometimes making a computer more secure can also make it less useful. For example, sometimes a firewall can protect a computer from malware, but it also prohibits the user from using certain websites. Perhaps you have run into this at your school or in your home. Another example is two step authentication. Entering a password in two ways definitely makes the account more secure, but it also takes more time and some people find it inconvenient. What other trade offs exist with making a system more secure? Are there any ethical questions associated with making a system more secure?

Critical Thinking Questions

1. **Cyber Threat Methods:** Compare cyber threat methods like brute force attacks, identity theft, phishing, and malware. Discuss protective measures against each.
2. **Security vs. Usability:** Explore trade-offs in computer security, like firewalls limiting website access. Consider ethical implications and societal impacts.

Summary

There are many types of threats that exist in the computer world. Attackers use intense trial and error to guess passwords by brute force. People steal identities to access valuable information. Attackers send emails trying to get people to reply with personal information in a method called phishing. Attackers also create a variety of malware to gain access to places they shouldn't. There's a growing variety of ways people can cause problems in the cyber world. Keeping your computer and softwares updated and using an antivirus software help protect your computer.

AP Standards

IOC-2.A.12

IOC-2.B.7

IOC-2.B.8

IOC-2.B.9

IOC-2.B.10

IOC-2.C.1

IOC-2.C.2

IOC-2.C.5

IOC-2.C.6

IOC-2.C.7

CSTA Standards

2-NI-05

3A-NI-05

3A-NI-06

3A-NI-07

3A-NI-08

3B-NI-04

3B-AP-18

Questions (11)

1. What type of attack is designed to figure out passwords through an intense series of trial and error?

MULTIPLE CHOICE

Choose the correct answer:

- A. Malware
- B. Identity Theft
- C. Phishing
- D. Brute Force

2. Which type of attack uses someone else's identity or credentials to give them access to information?

MULTIPLE CHOICE

Choose the correct answer:

- A. Brute Force
- B. Phishing
- C. Malware
- D. Identity Theft

3. Which type of attack sends an email that seem legitimate in an effort to get information from you?

MULTIPLE CHOICE

Choose the correct answer:

- A. Malware
- B. Phishing
- C. Brute Force
- D. Identity Theft

4. Which type of attack is where the criminal creates some sort of software that causes problems?

MULTIPLE CHOICE

Choose the correct answer:

- A. Malware
- B. Identity Theft
- C. Brute Force
- D. Phishing

5. Which type of malware is disguised as an advertisement?

MULTIPLE CHOICE

Choose the correct answer:

- A. Trojans
- B. Adware
- C. Bad Bots
- D. Ransomware

6. Which type of malware is a piece of code designed to repeat a task over and over again, overwhelming a system?

MULTIPLE CHOICE

Choose the correct answer:

- A. Trojans
- B. Bad Bots
- C. Adware
- D. Ransomware

7. Which type of malware takes your files and encrypts them in a way that they are not usable?

MULTIPLE CHOICE

Choose the correct answer:

- A. Ransomware
- B. Bad Bots
- C. Adware
- D. Trojans

8. Which type of malware attacks disguise themselves as authentic software that you want to download on your computer and then attack?

MULTIPLE CHOICE

Choose the correct answer:

- A. Adware
- B. Ransomware
- C. Trojans
- D. Bad Bots

9. What is keylogging?

MULTIPLE CHOICE

Choose the correct answer:

- A. A software that can track every key typed in a keyboard.
- B. Expanding the memory space on a computer.
- C. The process of saving more passwords.
- D. A computer hardware part that holds the case.

10. What is the difference between phishing and smishing?

MULTIPLE CHOICE

Choose the correct answer:

- A. Phishing is through email and smishing is through text messages (SMS).
- B. Phishing is through text and smishing is through email.
- C. They are the same.
- D. There is no such thing as smishing.

11. What is a good approach to a message that looks like phishing?

MULTIPLE CHOICE

Choose the correct answer:

- A. Reply to the message.
- B. Fill out all the info they ask for.
- C. Press the link they sent.
- D. Do not reply or press any links.

Answer Keys & Solutions

Questions

1. What type of attack is designed to figure out passwords through an intense series of trial and error?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-------------------|-------------|
| A. Malware | ✗ Incorrect |
| B. Identity Theft | ✗ Incorrect |
| C. Phishing | ✗ Incorrect |
| D. Brute Force | ✓ Correct |

Explanation:

Malware is corrupted software, identity theft is stealing your password, phishing is hoping you'll click on something

2. Which type of attack uses someone else's identity or credentials to give them access to information?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-------------------|-------------|
| A. Brute Force | ✗ Incorrect |
| B. Phishing | ✗ Incorrect |
| C. Malware | ✗ Incorrect |
| D. Identity Theft | ✓ Correct |

Explanation:

Malware is corrupted software, brute force is lots of trial and error, phishing is hoping you'll click on something

3. Which type of attack sends an email that seem legitimate in an effort to get information from you?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-------------------|-------------|
| A. Malware | ✗ Incorrect |
| B. Phishing | ✓ Correct |
| C. Brute Force | ✗ Incorrect |
| D. Identity Theft | ✗ Incorrect |

Explanation:

Malware is corrupted software, identity theft is stealing your password, brute force is trial and error

4. Which type of attack is where the criminal creates some sort of software that causes problems?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-------------------|-------------|
| A. Malware | ✓ Correct |
| B. Identity Theft | ✗ Incorrect |
| C. Brute Force | ✗ Incorrect |
| D. Phishing | ✗ Incorrect |

Explanation:

brute force is trial and error guessing, identity theft is stealing your password, phishing is hoping you'll click on something

5. Which type of malware is disguised as an advertisement?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-------------|-------------|
| A. Trojans | ✗ Incorrect |
| B. Adware | ✓ Correct |
| C. Bad Bots | ✗ Incorrect |

D. Ransomware

✗ Incorrect

Explanation:

This kind of threat does anything to get you to click on it.

6. Which type of malware is a piece of code designed to repeat a task over and over again, overwhelming a system?

MULTIPLE CHOICE

Correct Answer:

A. Trojans

✗ Incorrect

B. Bad Bots

✓ Correct

C. Adware

✗ Incorrect

D. Ransomware

✗ Incorrect

Explanation:

These are like tiny programmed robots that are overwhelming to the system.

7. Which type of malware takes your files and encrypts them in a way that they are not usable?

MULTIPLE CHOICE

Correct Answer:

A. Ransomware

✓ Correct

B. Bad Bots

✗ Incorrect

C. Adware

✗ Incorrect

D. Trojans

✗ Incorrect

Explanation:

Often, the criminal then refuses to decrypt them without some sort of payment.

8. Which type of malware attacks disguise themselves as authentic software that you want to download on your computer and then attack?

MULTIPLE CHOICE

Correct Answer:

- | | |
|---------------|-------------|
| A. Adware | ✗ Incorrect |
| B. Ransomware | ✗ Incorrect |
| C. Trojans | ✓ Correct |
| D. Bad Bots | ✗ Incorrect |

Explanation:

This is similar to a battle in ancient Greek times.

9. What is keylogging?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-------------------------------------------------------------|-------------|
| A. A software that can track every key typed in a keyboard. | ✓ Correct |
| B. Expanding the memory space on a computer. | ✗ Incorrect |
| C. The process of saving more passwords. | ✗ Incorrect |
| D. A computer hardware part that holds the case. | ✗ Incorrect |

Explanation:

This is kind of like keeping a log of every single thing you type.

10. What is the difference between phishing and smishing?

MULTIPLE CHOICE

Correct Answer:

- | | |
|---------------------------------------------------------------------------|-------------|
| A. Phishing is through email and smishing is through text messages (SMS). | ✓ Correct |
| B. Phishing is through text and smishing is through email. | ✗ Incorrect |
| C. They are the same. | ✗ Incorrect |
| D. There is no such thing as smishing. | ✗ Incorrect |

Explanation:

Smishing is phishing through texts rather than email.

11. What is a good approach to a message that looks like phishing?

MULTIPLE CHOICE

Correct Answer:

- | | |
|----------------------------------------|-------------|
| A. Reply to the message. | ✗ Incorrect |
| B. Fill out all the info they ask for. | ✗ Incorrect |
| C. Press the link they sent. | ✗ Incorrect |
| D. Do not reply or press any links. | ✓ Correct |