

Cyberbombs That Sneak into Your Devices

Vathna.lay@cadt.edu.kh

Objectives

After finishing this lesson, you will be able to:

- **Understand the range of cyberattack techniques**
- **Recognize the motivations behind attacks**
- **Develop a sense of potential consequences**



Malware – The Hidden Threat

- Some cyberattacks are designed to cause damage, not directly steal data.
- Type: **viruses, worms, Trojans, ransomware, and spyware.**
- **Malware** can steal passwords, crash your system, extort money, and spy on you.



Viruses: The Self-Replicating Threat

- How Viruses Work
 - Like a biological virus, they need a host to spread.
 - They insert their code into files, programs, or even your operating system.
 - When you open the infected file, the virus runs and spreads
- The Damage
 - Viruses can slow down your computer or make it crash.
 - They can steal your sensitive information.
 - Some are sneaky, while others announce themselves with a bang!



Computer Worms: Network Invaders

- How Viruses Work
 - **Stand-alone malware** – they don't need to piggyback on other files
 - Exploit security holes in your computer and network to spread
 - Multiply like crazy, slowing everything down
- The Danger
 - Even if they don't steal data directly, they clog up your network
 - Can make internet and work tasks painfully slow
 - Can open the door for other, even nastier malware to sneak in!



Trojans: The Digital Deception

- The Trick
 - **Disguised as helpful software or hidden inside something legitimate.**
 - Relies on YOU to accidentally let it in (clicking links, installing apps)
 - Doesn't spread on its own like viruses or worms
- What They Do
 - Once inside, a Trojan can do almost anything the attacker wants.
 - Steal your passwords or bank details.
 - Let other malware sneak onto your system.
 - Even take remote control of your computer.



Ransomware: Your Data Held Hostage

- How Ransomware Works
 - **Encrypts your files so you can't access them.**
 - Demands payment, or threatens to delete your data forever
 - Can even steal your files instead of just encrypting them
- The Danger
 - Often arrives disguised as a virus or Trojan.
 - Attacks are getting smarter, targeting valuable data
 - Stakes are high – businesses and individuals can lose everything



Scareware: When Fear is the Weapon

- The Trick
 - Fake pop-ups scream about 'viruses' on your device.
 - They push useless 'security software' you have to buy
 - Preys on your fear, not actual tech problems.
- Why it Works
 - Even tech-savvy people can get startled in the moment.
 - No one wants their computer to break.
 - Scammers know how to exploit panic.





Spyware: The Silent Watcher

- What Spyware Does
 - Steals your keystrokes, passwords, and personal information.
 - Snaps secret photos or videos with your webcam.
 - Records everything you say near your device
 - Tracks your every move, online and offline.
- The Blurred Line
 - Some spying tools are used by legitimate businesses (tracking cookies)
 - **Even popular apps can collect sensitive data about you.**
 - **The difference is in permission – malware spies without it.**





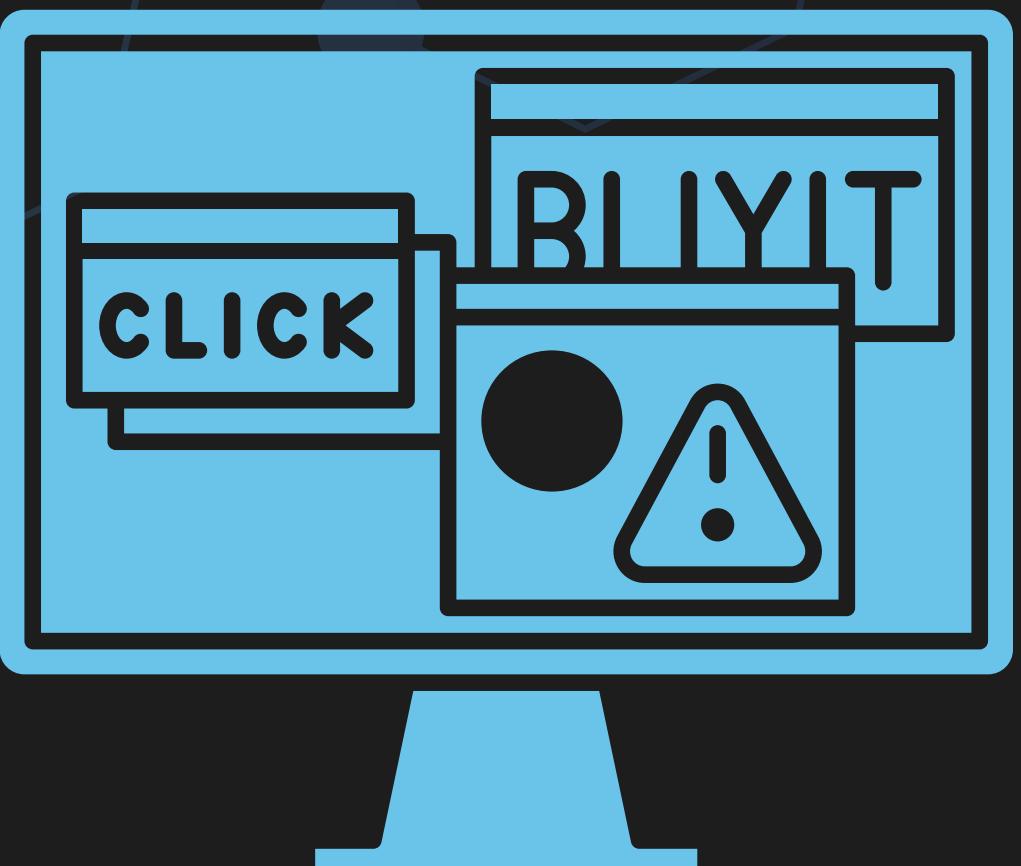
Cryptominers: Stealing Your Power for Profit

- How Cryptominers Work
 - Malware hijacks your computer's processing power.
 - Use to solves complex math problems to create cryptocurrency.
 - Profit goes straight to the attacker, not you.
- Why They're Dangerous
 - Miners skyrocket your electricity bill.
 - Slow down your device to a crawl.
 - **Easy money for criminals, even if you don't earn much**



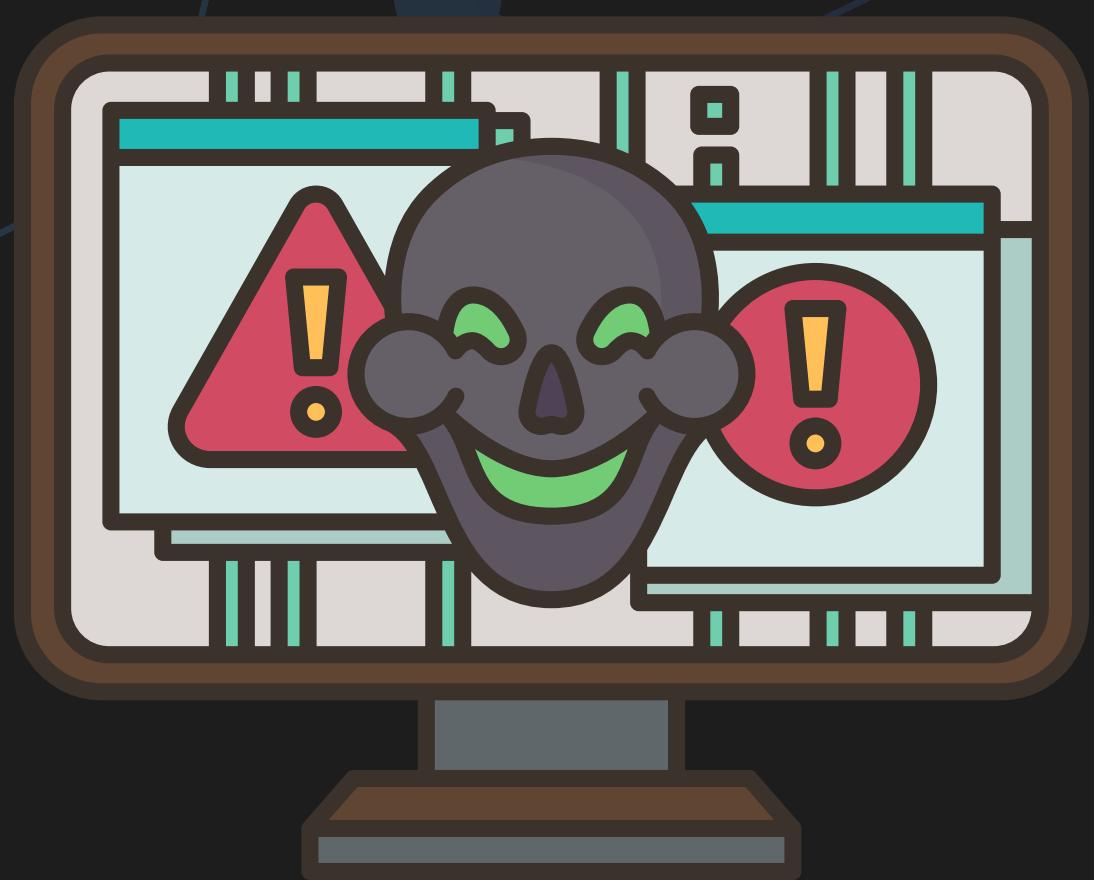
Adware: The Double-Edged Sword

- Adware Can Be Legitimate
 - Often comes bundled with 'free' software.
 - Displays ads, but you know it's there.
 - Developers use it to make money instead of charging you
- When Adware is Malware
 - Sneaks onto your device without permission.
 - Bombards you with pop-ups or hijacks your browser.
 - Can track your activity to personalize the ads.



Blended Malware: The Ultimate Threat

- The Hybrid Attack
 - Combines the worst parts of viruses, worms, Trojans, and more.
 - Can spread quickly, hide cleverly, and inflict maximum damage.
- Why It's Dangerous
 - Difficult to detect with traditional security tools.
 - Often created by experienced, well-funded attackers



Zero-Day Malware: The Invisible Attack

- What Makes It Dangerous
 - Exploits an unknown flaw in software or systems.
 - No patches or defenses exist yet.
 - Devastating attacks made possible.
- The High Price Tag
 - Complex to create, requiring expert knowledge.
 - Often developed by well-funded groups, even governments.
 - A single exploit can cost over \$1 million!





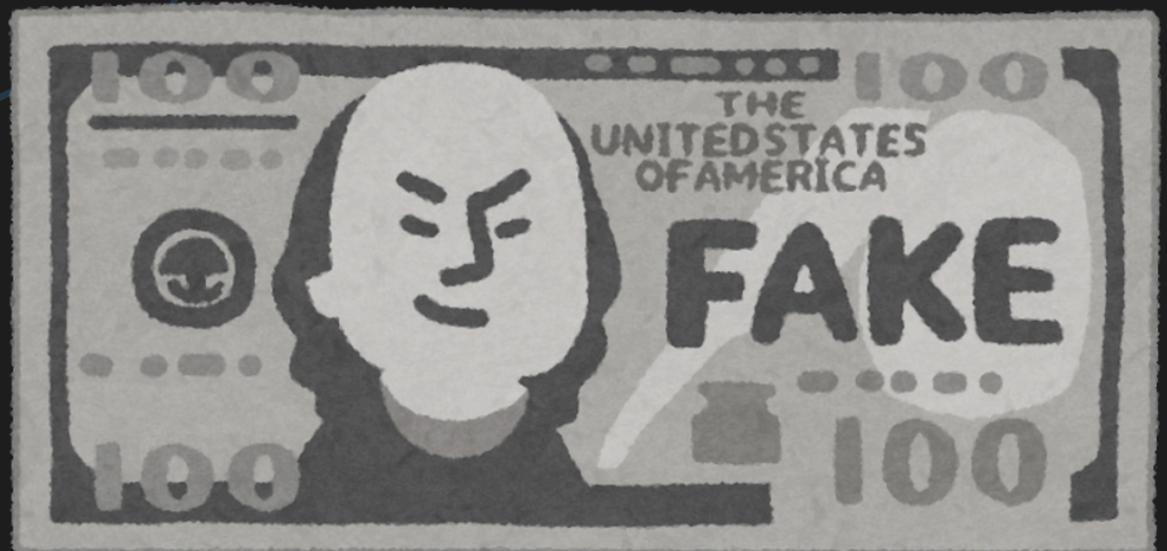
Fake Malware: When Hacking Is Just a Bluff

- The Trick
 - Fake virus alerts or emails demand money.
 - No actual hacking involved, just scare tactics.
 - Preys on fear and confusion.
- Why It Works
 - Panic can override logic, even for tech-savvy people.
 - Scammers know the right buttons to push.
 - Easy money if victims fall for it.



Fake Renewals: When Protection is the Scam

- The Scam
 - Emails or pop-ups claim your security subscription is expiring.
 - Demands urgent payment to renew.
 - Mimics real security companies to trick you.
- How to Spot a Fake
 - Check the sender's email address closely for misspellings.
 - Hover over links WITHOUT clicking to see the real destination.
 - Never renew through an unsolicited email or pop-up.

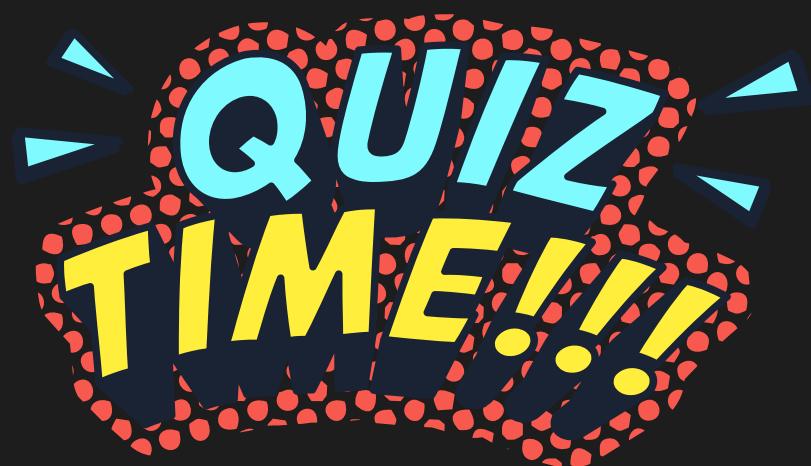




Question

Which of the following is NOT a common type of malware?

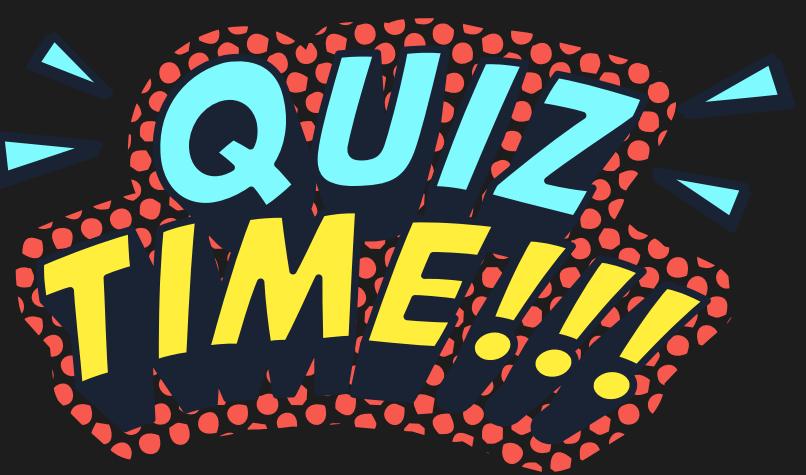
- A. Spyware
- B. Firewall
- C. Ransomware
- D. Trojan



Question

Viruses typically spread by:

- A. Exploiting vulnerabilities in network connections.
- B. Inserting their code into files or programs. ✓
- C. Disguising themselves as helpful software.
- D. Both (a) and (b).

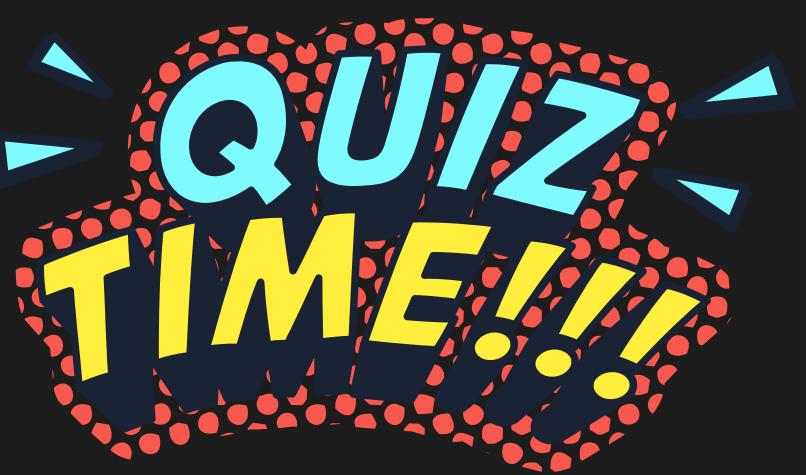




Question

Worms are different from viruses because they can spread

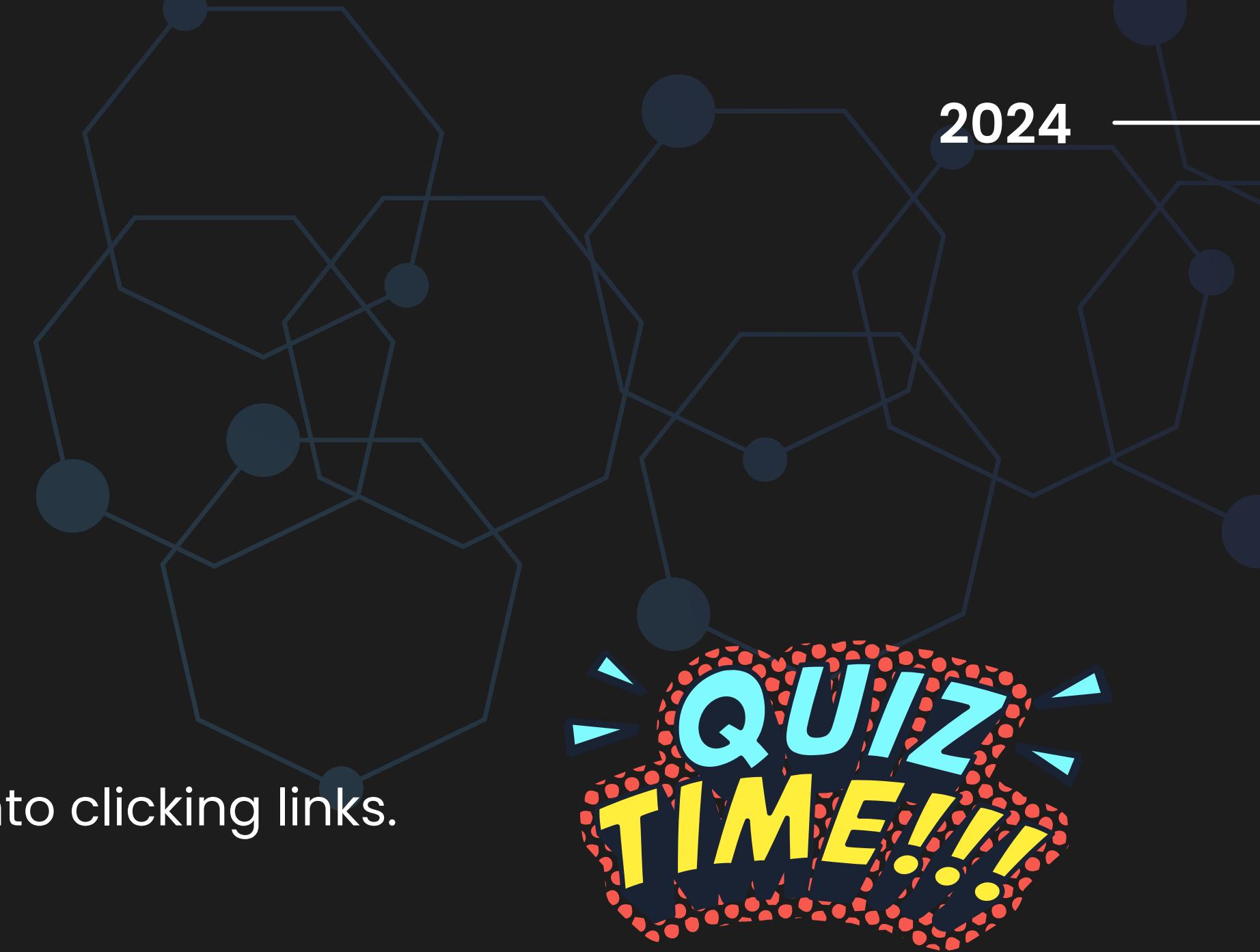
- A Without needing a host file or program.
- B. By stealing your passwords
- C. By encrypting your data.
- D. Only on Windows computers..



Question

Trojans are most commonly spread through:

- A. Network connections.
- B. Social engineering tactics like tricking users into clicking links.**
- C. Hardware malfunctions.
- D. All of the above.

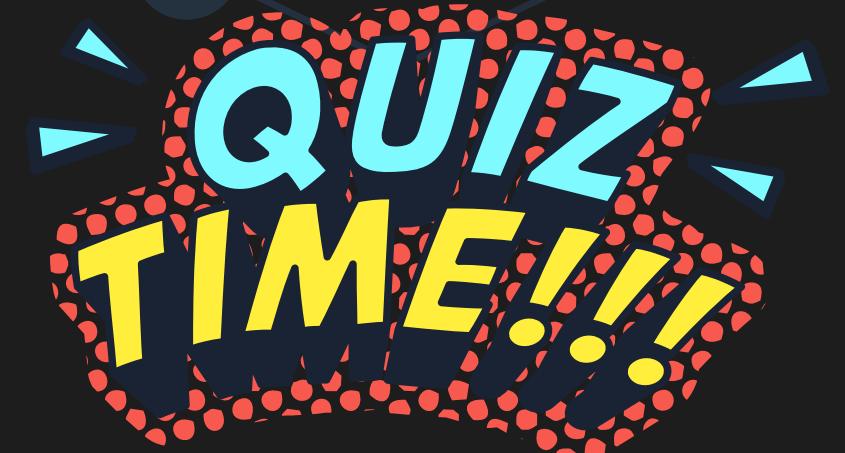


Question

Ransomware encrypts your files and demands a ransom payment

in exchange for:

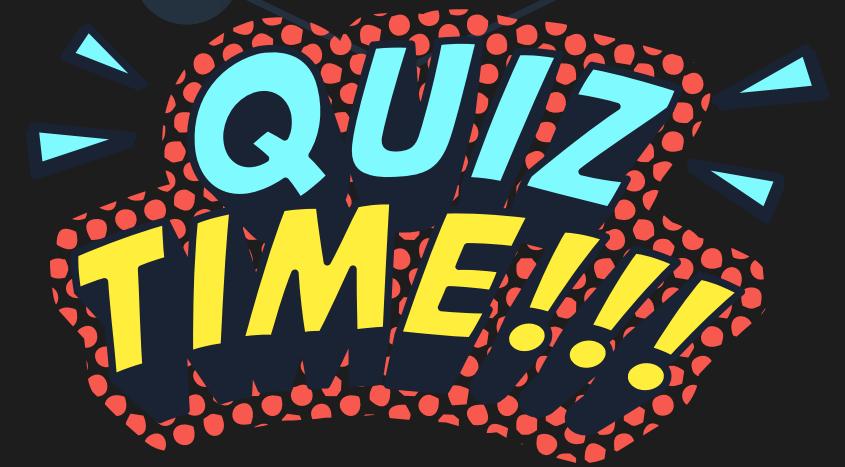
- A. Updating your security software
- B. Installing a new antivirus program.
- C. The decryption key to access your files again.
- D. All of the above.



Question

Scareware attempts to pressure users into buying unnecessary security software by:

- A. infecting their device with a virus.
- B. Displaying fake pop-up warnings about non-existent threats.
- C. Stealing personal information through keylogging
- D. All of the above.

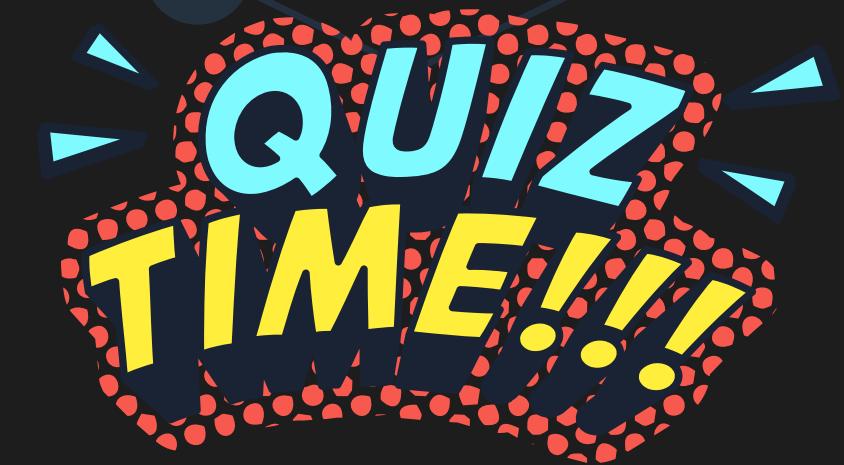


Question

Spyware can steal a variety of information from your device,

including:

- A. Your browsing history.
- B. Your keystrokes as you type.
- C. Recordings from your webcam or microphone.
- D. All of the above.

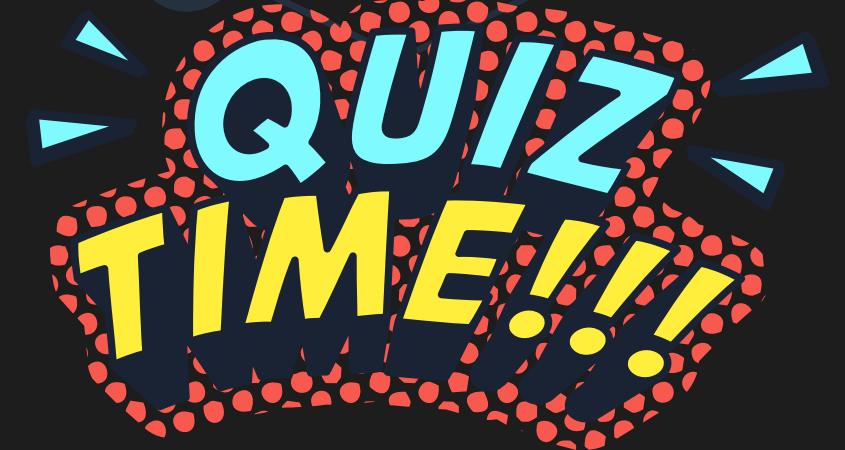




Question

Cryptocurrency miners hijack your computer's processing power to:

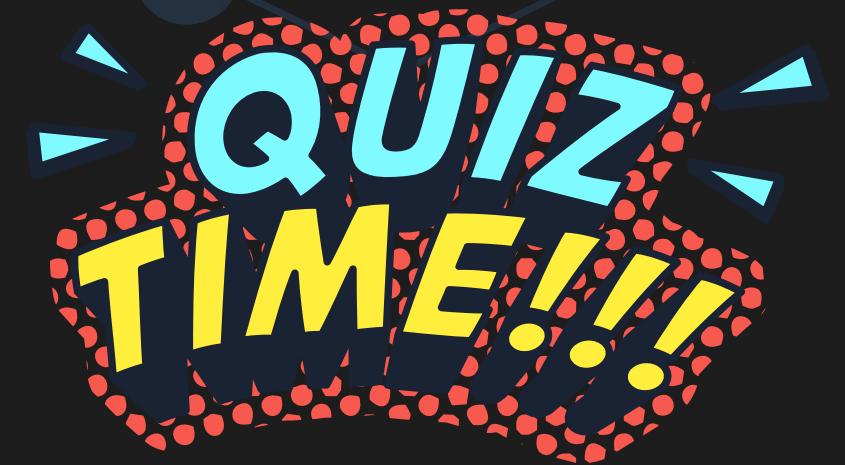
- A. Generate new cryptocurrency for the attacker.
- B. Slow down your device to a crawl.
- C. Both of them
- D. None of them



Question

Adware can be legitimate if:

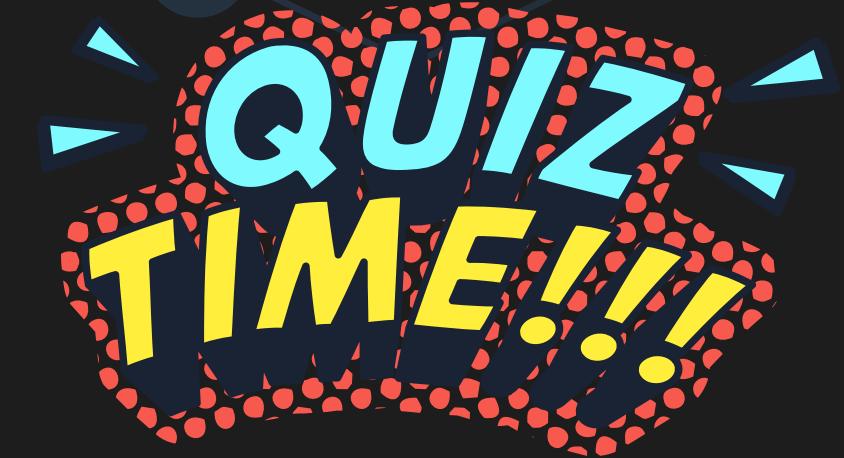
- A. It displays intrusive pop-up ads.
- B. It comes bundled with free software, and you know about it beforehand.
- C. It steals your browsing data
- D. It hides in your device's system files.



Question

Zero-day malware is particularly dangerous because:

- A. It's easy to create and inexpensive.
- B. It exploits unknown vulnerabilities in software or systems.**
- C. It can spread quickly through email attachments.
- D. It targets Apple devices specifically.

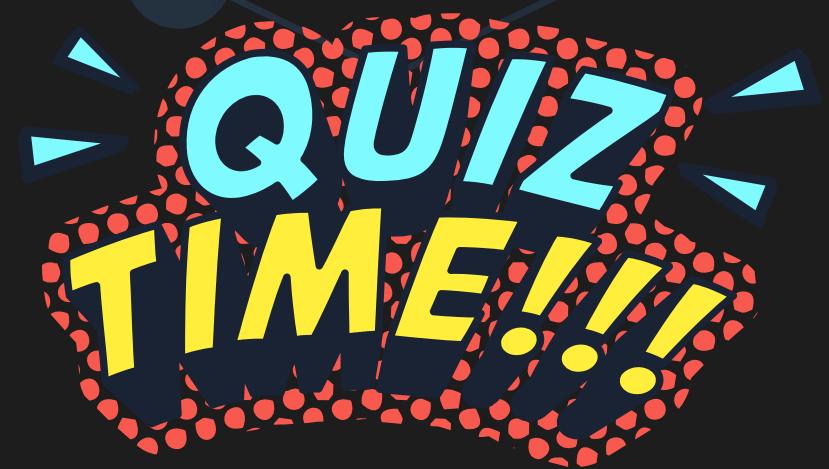




Question

Blended malware attacks are dangerous because they:

- A. Combine features of different malware types for maximum impact.
- B. Only affect outdated systems.
- C. Are created only by inexperienced hackers.
- D. Are easy to detect and defend against.

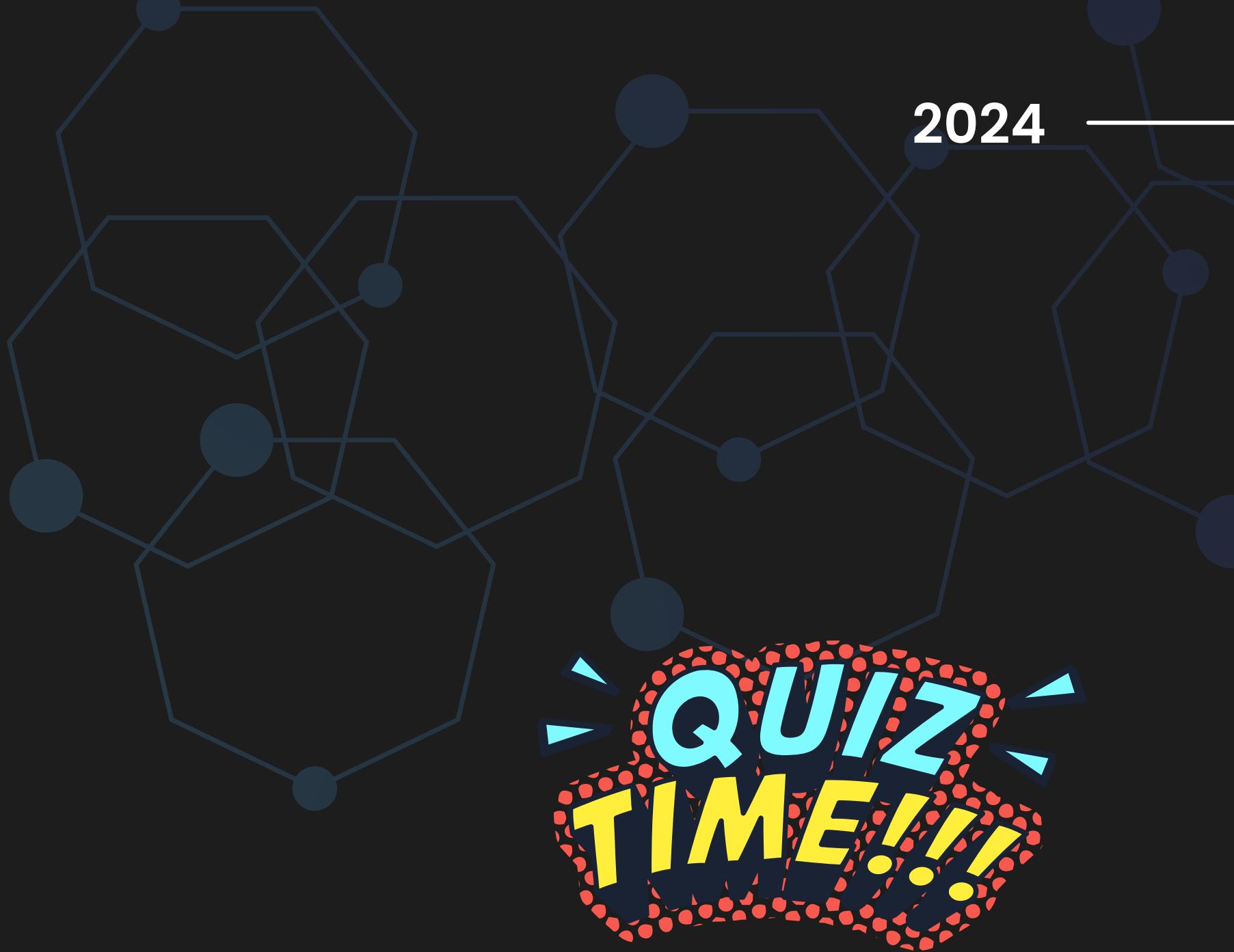




Question

The goal of most malware is to:

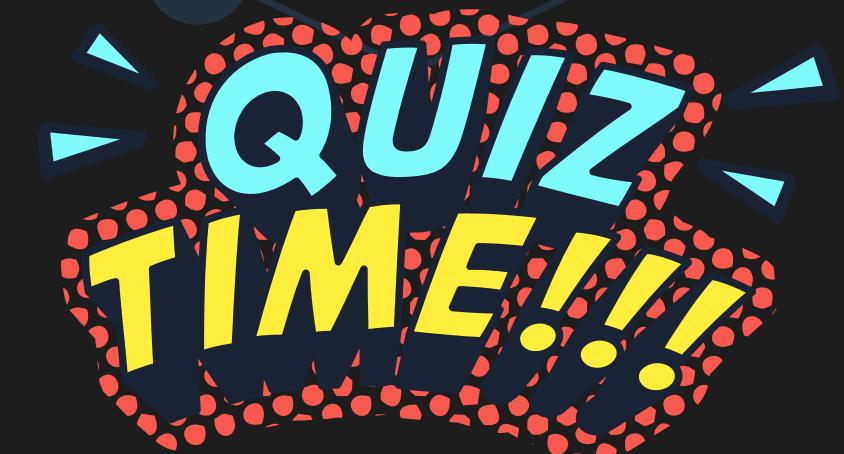
- A. Help secure your computer.
- B. Make the attacker money or cause disruption.**
- C. Test advanced hacking techniques.
- D. Improve the performance of your system.



Question

Which of these is NOT a good defense against malware?

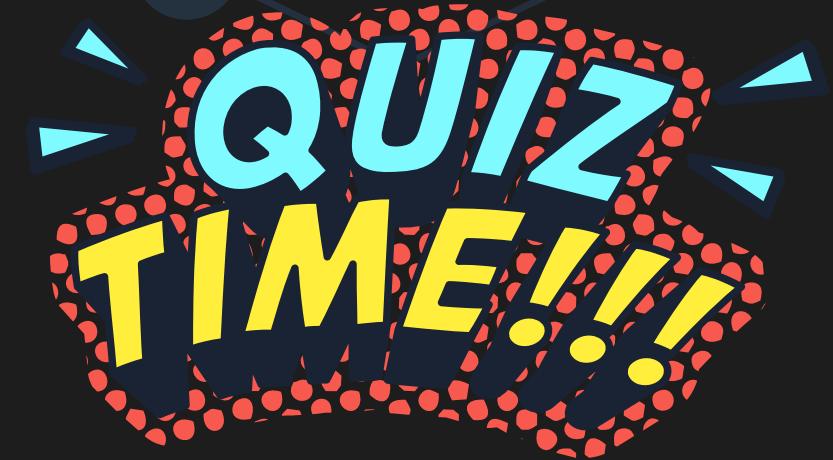
- A. Keep your software and operating system updated.
- B. Install reputable security software.
- C. Avoid opening emails or clicking on links from unknown senders.
- D. Rely on your computer's built-in defenses only.



Question

One way social engineering attacks like fake renewal scams can be successful is by:

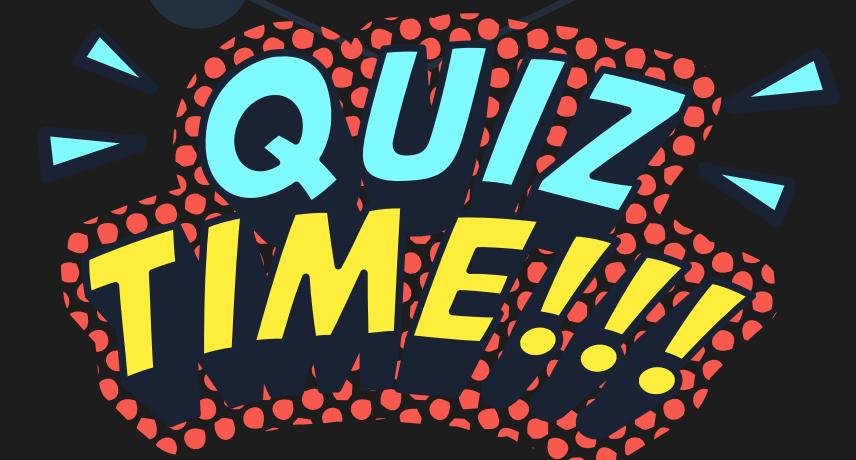
- A. Targeting users when they're already tired or stressed.
- B. Mimicking legitimate companies and messages to lower suspicion.
- C. Both of them
- D. None of them



Question

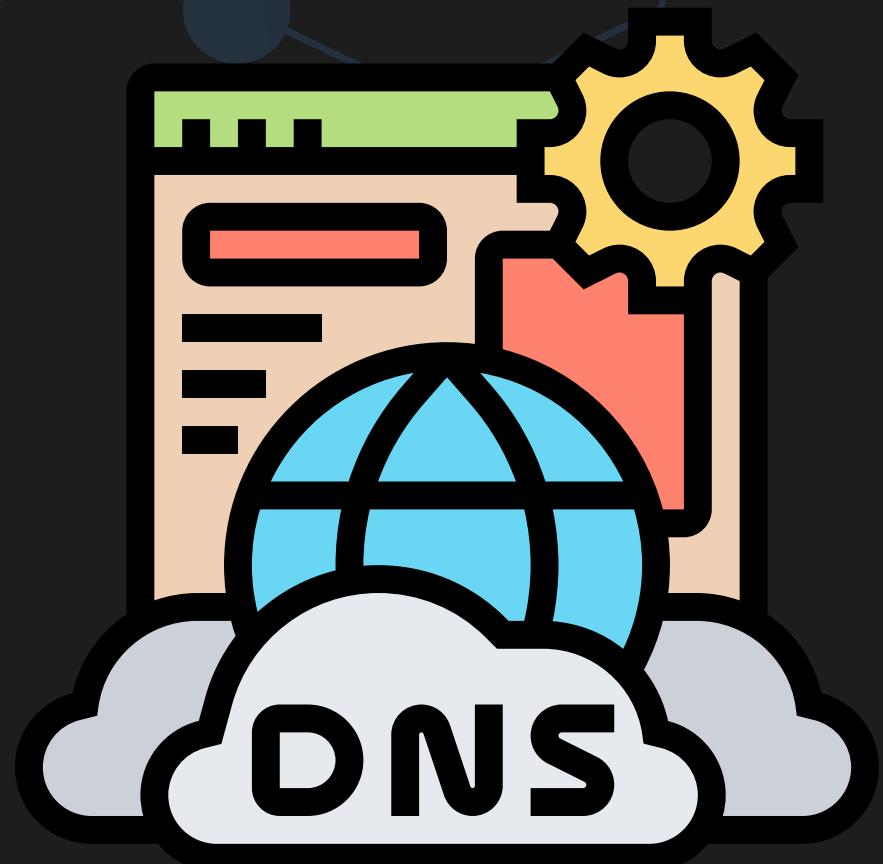
Which of these statements is TRUE about malware?

- A. Macs and other non-Windows devices are immune to malware.
- B. If you're careful, you can avoid all malware infections.
- C. Modern anti-malware software can catch 100% of all threats.
- D. Malware is constantly evolving, requiring vigilance and updated protection.



When the Internet's Map Lies: DNS Poisoning

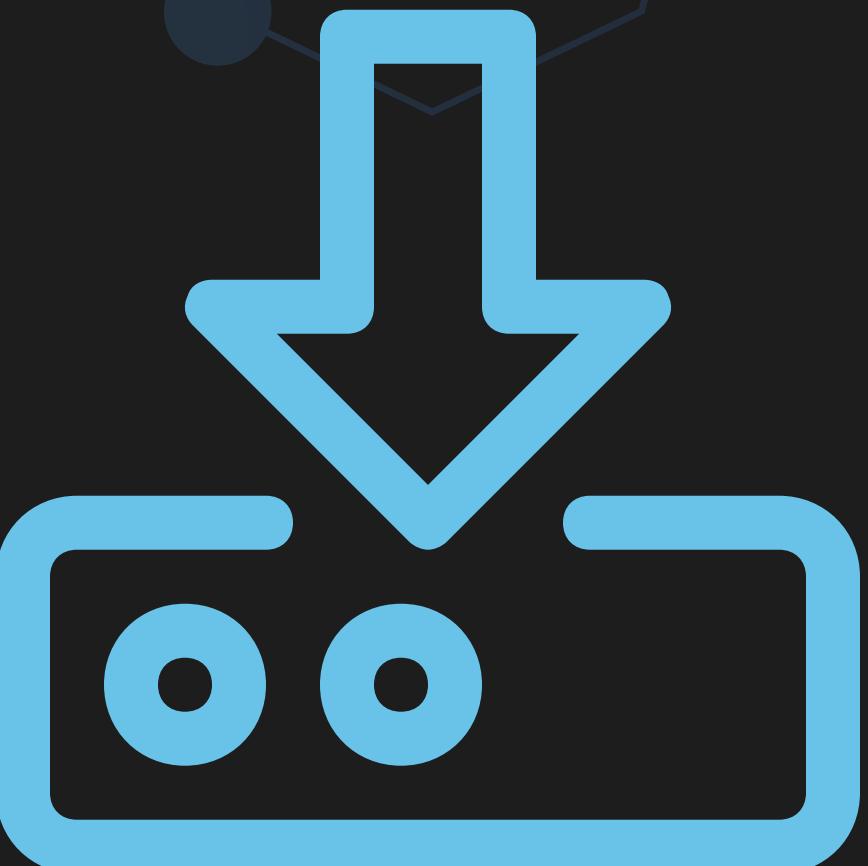
- Your Internet Guide
 - Translates website names (`example.com`) into IP addresses computers understand.
 - Like a giant phonebook for the internet.
- DNS Poisoning
 - Attackers corrupt the 'phonebook', sending you to fake websites.
 - Can steal passwords, even if you typed the address correctly.
 - Your map leads to a trap.





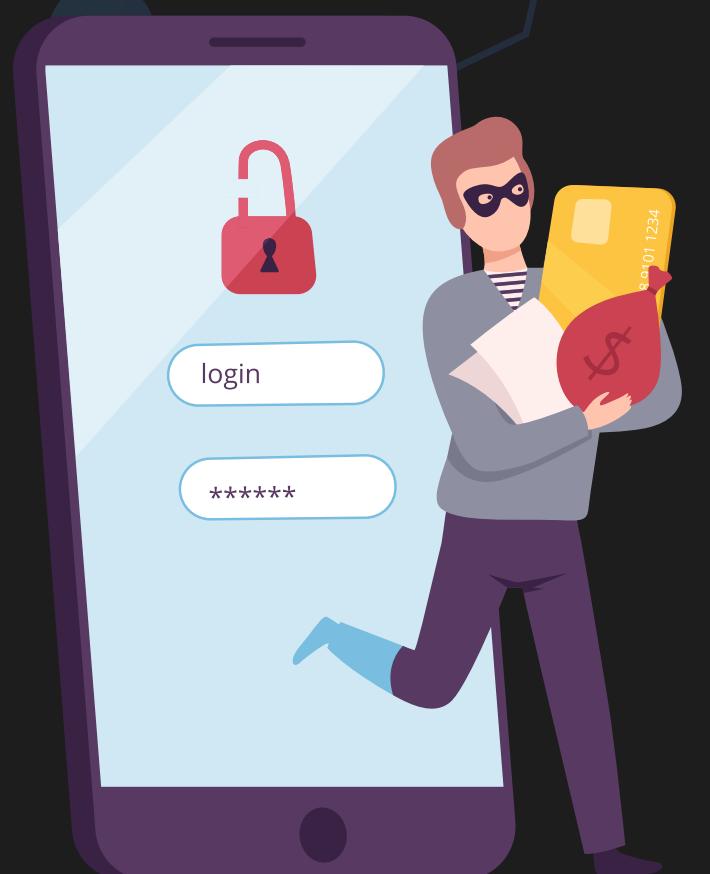
Drive-By Downloads: The Hidden Ride

- What Are They?
 - Malware that sneaks onto your device without your full knowledge.
 - Can be completely automatic (poisoned websites)
 - Or disguised as something helpful (fake 'security patches')
- Why They're Dangerous
 - They play on trust or a sense of urgency.
 - Even cautious users can get tricked by clever disguises.



How Passwords Get Stolen

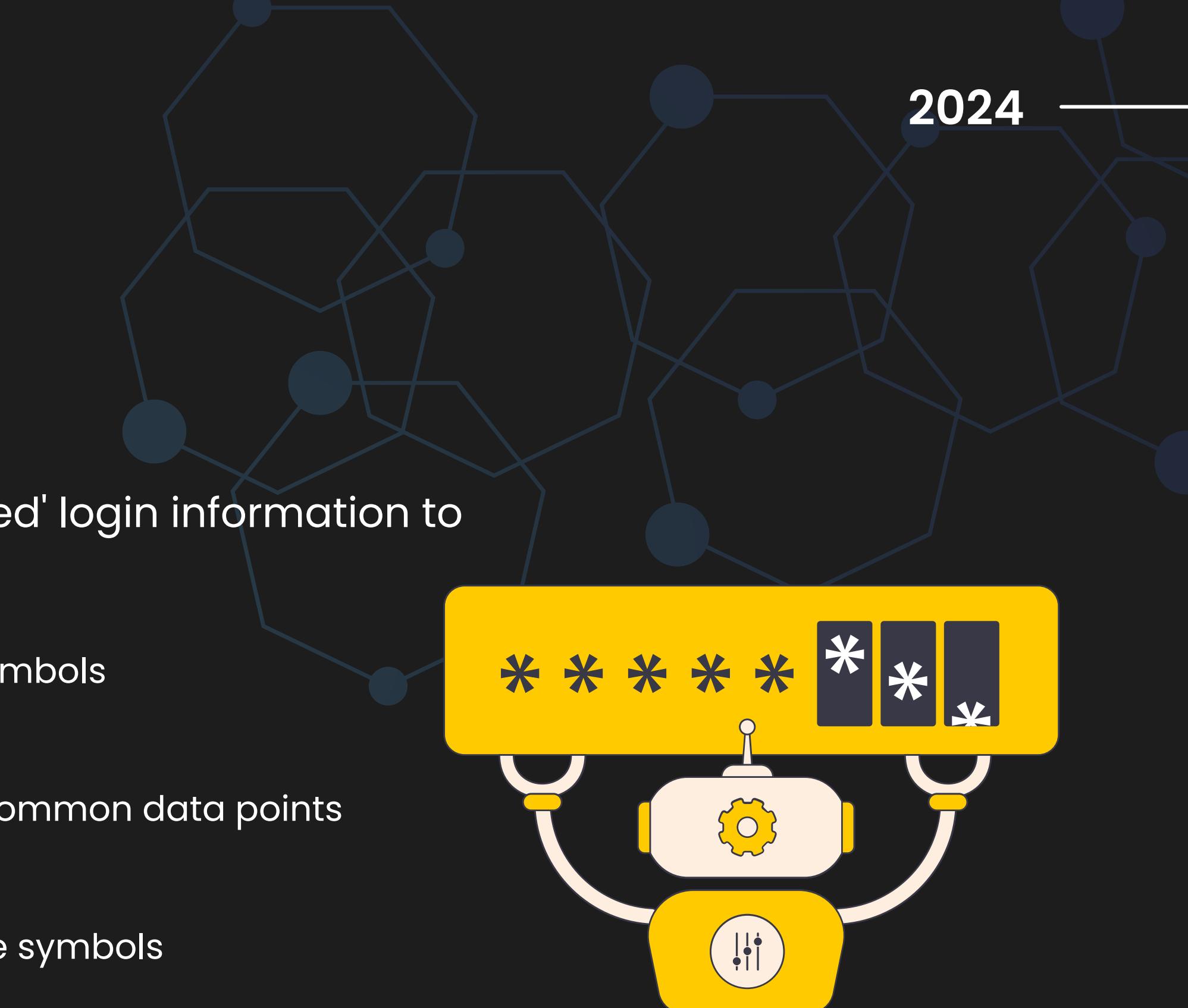
- Passwords are stolen in many ways:
 - Database breaches
 - Social engineering tricks
 - Automated guessing attacks
 - Malware that steals your keystrokes
 - Sniffing on unsecured networks





Credential Attack

- Credential Attacks use stolen or 'guessed' login information to break into systems:
 - Brute Force: A flurry of random character symbols
 - Dictionary Attack: An open dictionary
 - Calculated Attack: A person's silhouette + common data points (birthdate, pet names, etc.)
 - Blended Attack: A combination of the above symbols





When Updates Cause Trouble

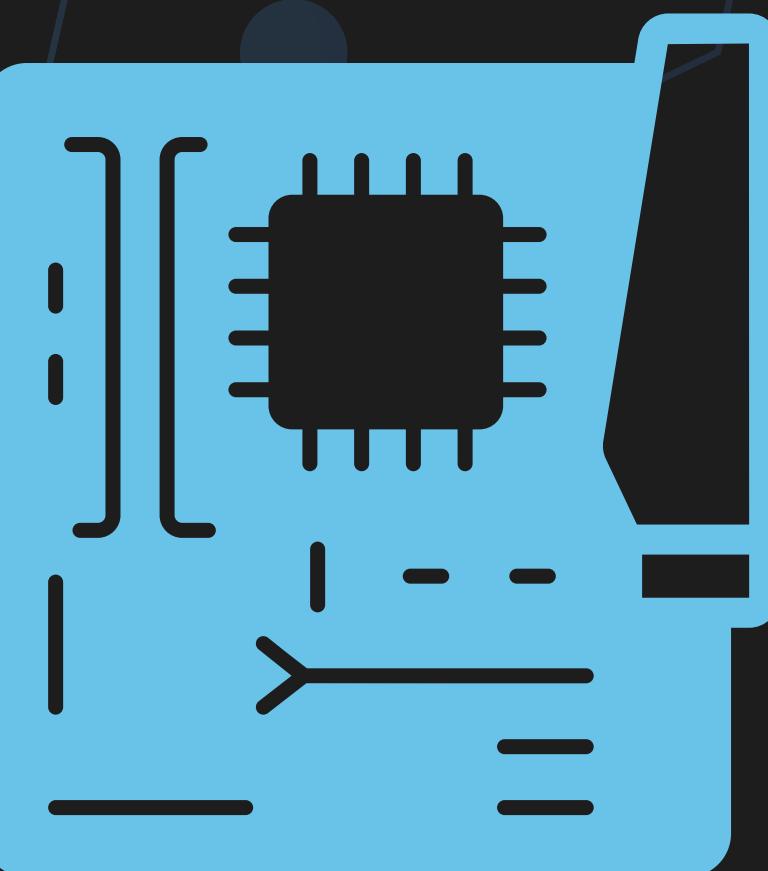
- The Need for Updates
 - Patches fix security flaws and bugs in software
 - Not updating leaves you vulnerable to attack.
- The Maintenance Dilemma
 - Updates sometimes break other programs or cause problems.
 - Delays are common as people troubleshoot compatibility.
 - Security needs often lose out to keeping things working.





Advanced Attacks: Beyond the Buzzword

- What Makes Them Advanced?
 - Often involves expensive research and development.
 - May exploit unknown vulnerabilities (zero-day attacks).
 - Require a high level of technical skill to pull off.
- The Fuzzy Definition
 - No official standard for what 'advanced' truly means.
 - Expert opinions vary.



Opportunistic vs. Targeted Attacks

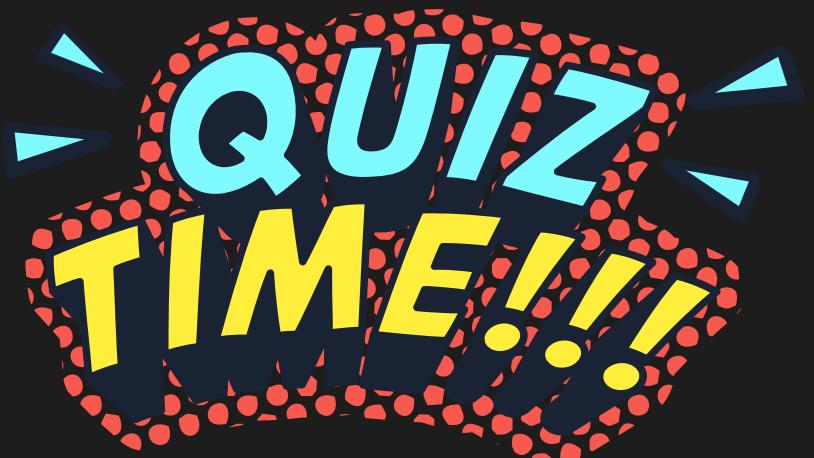
- Opportunistic
 - 'Spray and pray' approach, hoping to exploit many systems.
 - Low skill needed, but lower success rate per target.
- Targeted
 - Focused on a specific victim.
 - Attacks tailored to that system's defenses.
 - High effort, but potentially devastating.



Question

Criminals can steal passwords through various methods. Which is the MOST common way passwords are compromised?

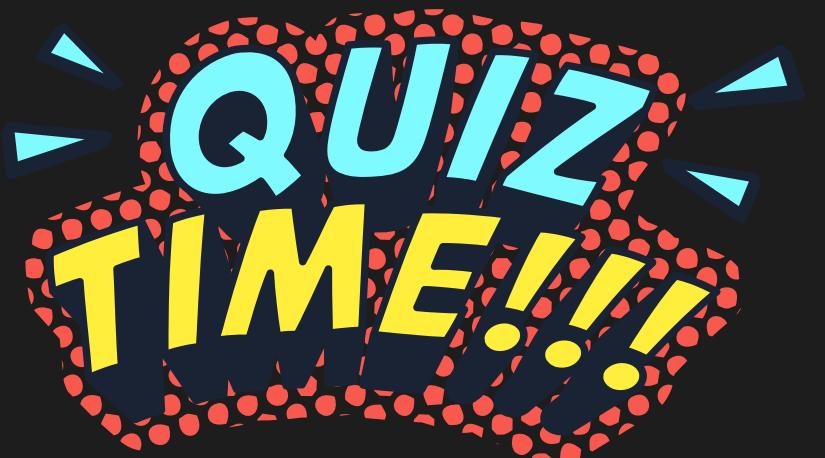
- A. Brute force attacks that try every possible password combination.
- B. Social engineering tricks that manipulate users into giving away passwords
- C. Network sniffing on unsecured Wi-Fi networks
- D. Stealing password databases from online stores (if not properly encrypted)



Question

Malvertising refers to:

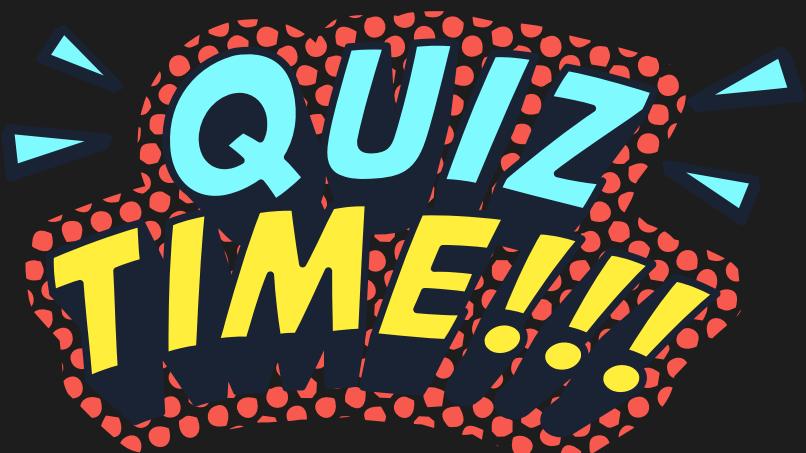
- A. Using legitimate advertising to promote fake security products.
- B. Online ads that contain hidden malware that infects devices.
- C. Spam emails that appear to be from reputable companies.
- D. Phishing attacks that try to trick users into revealing personal information.



Question

Which of these is NOT a way that drive-by downloads can infect your device:

- A. Clicking on a malicious advertisement on a website
- B. Downloading a seemingly helpful software that's malware 
- C. Visiting a compromised website that automatically infects your device
- D. Opening an email attachment containing hidden malware



Question

A common challenge in keeping computer systems secure is:

- A. The high cost of security software.
- B. The lack of user awareness about cyber threats.
- C. The difficulty of balancing security updates with maintaining software compatibility
- D. All of the above

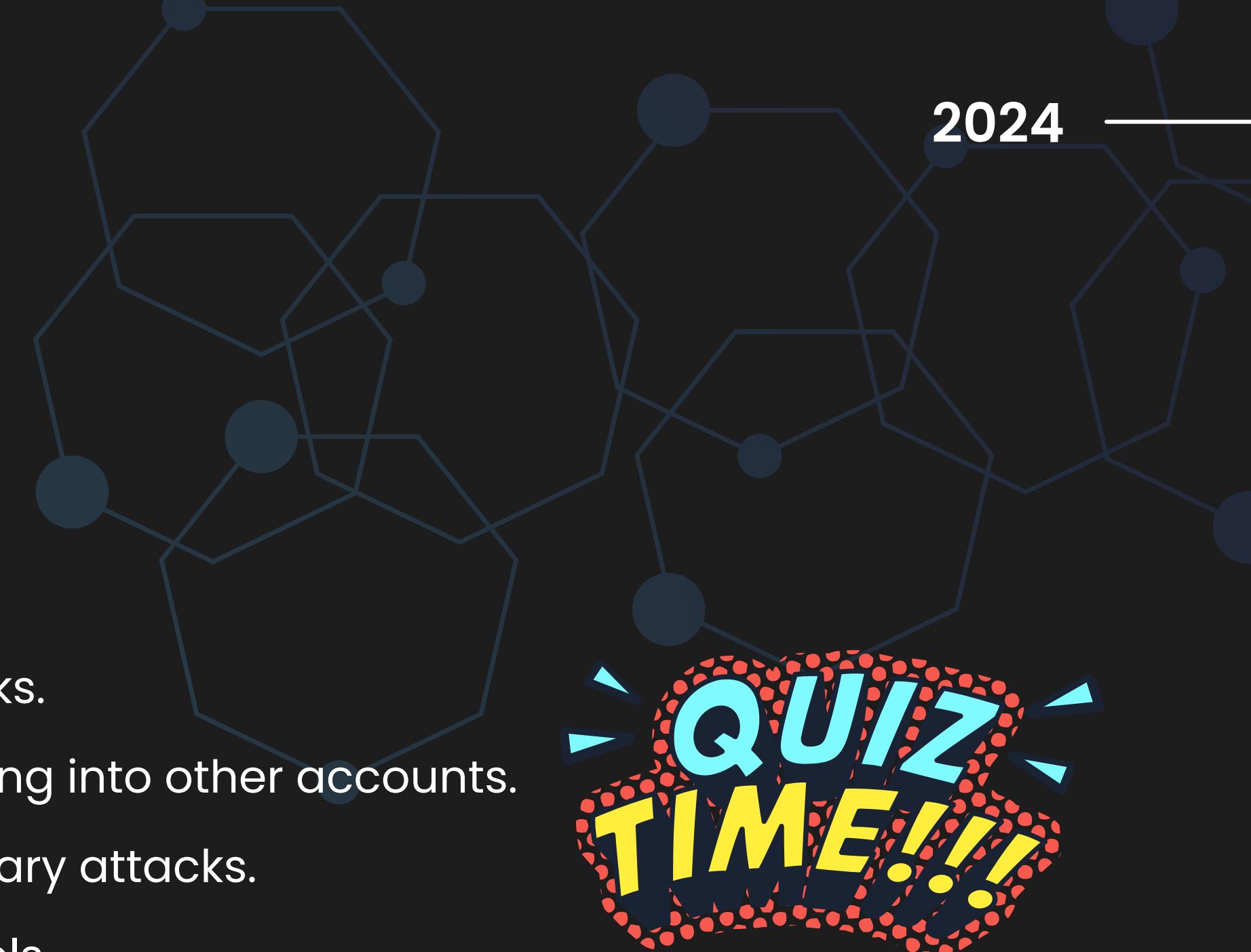




Question

Credential stuffing attacks involve:

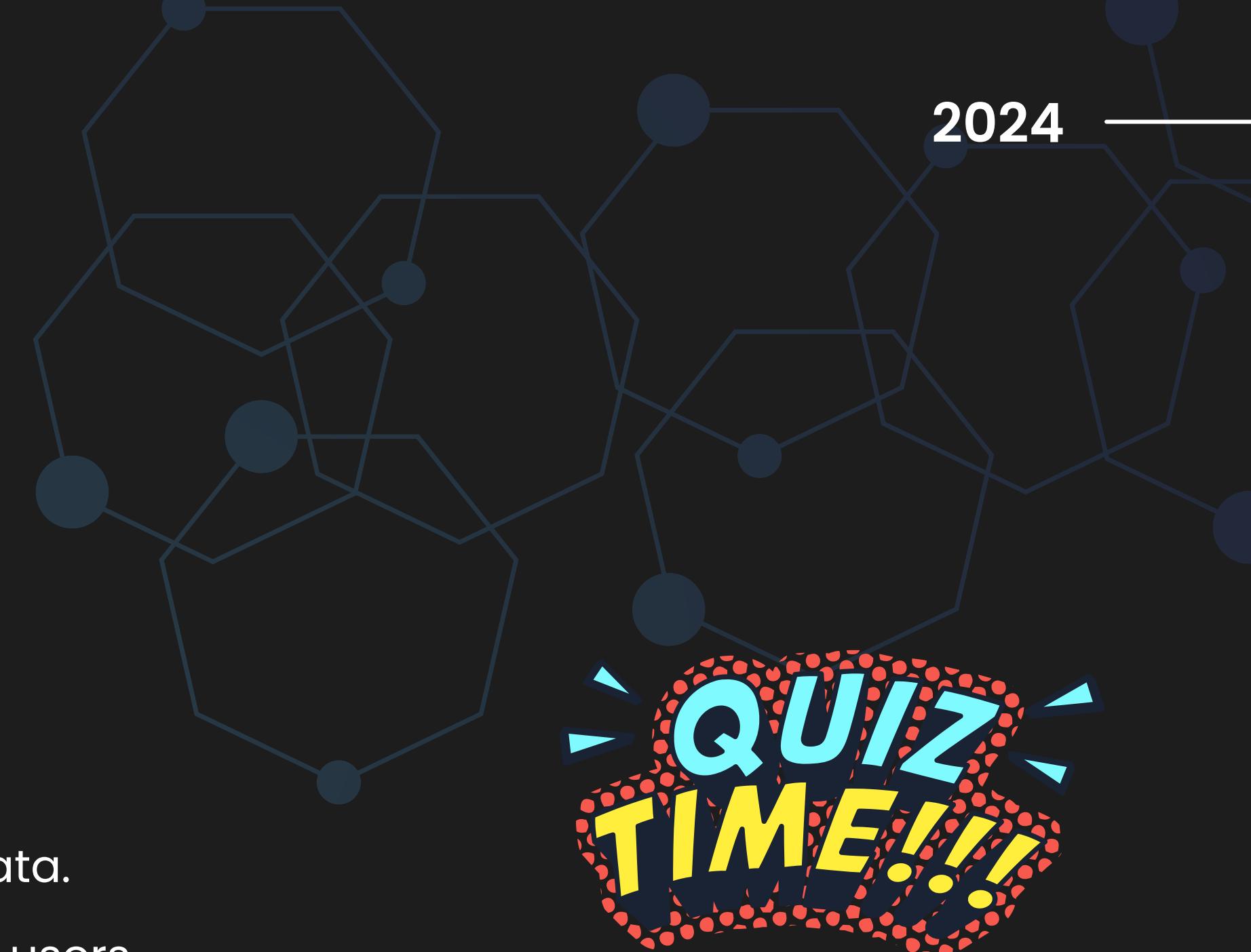
- A. Stealing passwords through social engineering tricks.
- B. Using stolen usernames and passwords to try logging into other accounts.
- C. Guessing passwords through brute force or dictionary attacks.**
- D. Exploiting vulnerabilities in network security protocols.



Question

DNS (Domain Name System) translates:

- A. IP addresses into human-readable website names.
- B. Usernames into passwords for secure logins.
- C. Encryption codes are used to scramble sensitive data.
- D. Website content into different languages for global users.

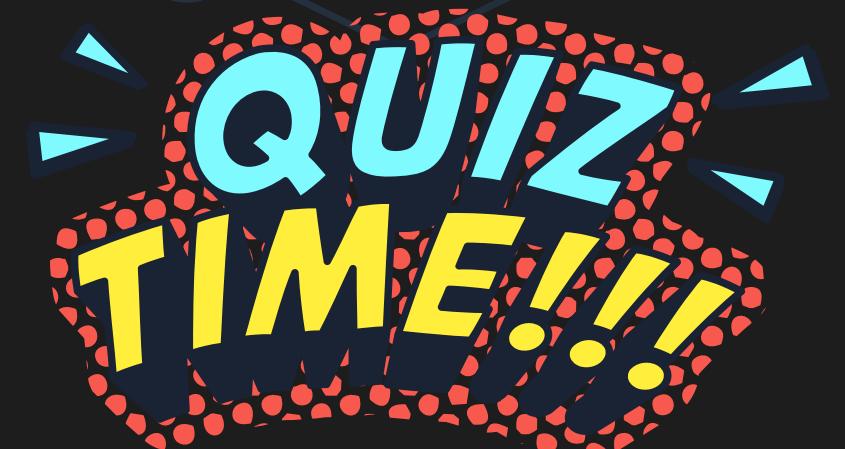




Question

In a DNS poisoning attack, criminals aim to:

- A. Steal your credit card information when you enter it on a website.
- B. Redirect your web traffic to a fake website that impersonates a legitimate one.
- C. Overload a website with traffic to take it down (denial-of-service attack).
- D. Corrupt the data on your computer's hard drive.

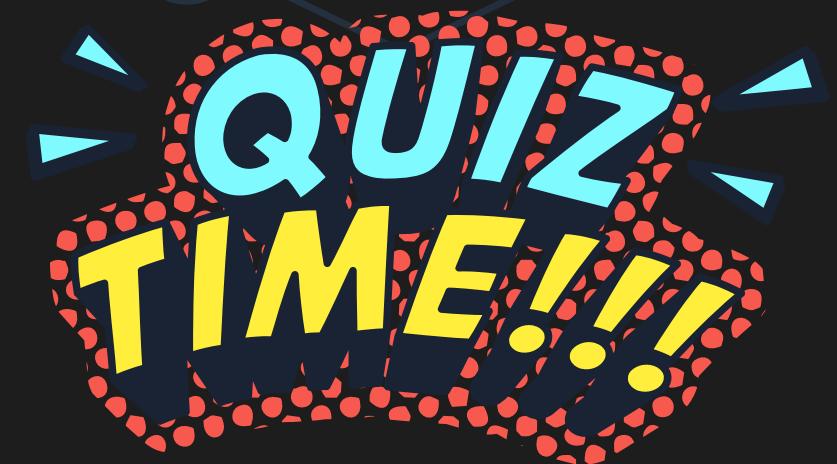




Question

Which of these best describes an opportunistic cyberattack?

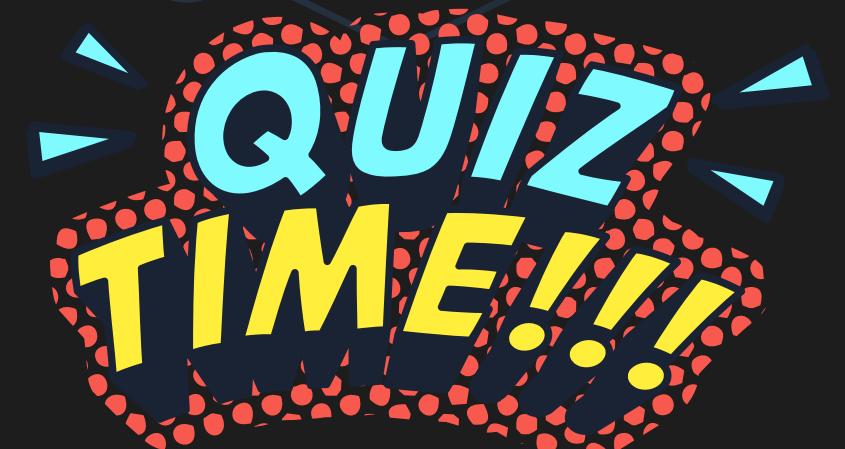
- A. A highly targeted attack that exploits a specific system's vulnerabilities.
- B. A broad attempt to infect as many devices as possible with malware.
- C. A social engineering attack that manipulates users into giving away personal information.
- D. A denial-of-service attack that floods a website with overwhelming traffic.



Question

What is the main benefit for attackers when using malvertising?

- A. They can directly steal money from user accounts.
- B. It allows them to bypass a user's security software.
- C. They can infect a large audience through trusted websites.
- D. Malvertising is a cheap and easy way to launch cyberattacks.



Question

What is a key way to protect yourself from drive-by downloads and other malware threats?

- A. Regularly clear your browsing history and cookies.
- B. Only visit websites you know and trust (avoid suspicious links)
- C. Disable pop-up windows entirely on your web browser.
- D. Update your computer's operating system and software regularly.

