Cyber Security Breach

Vathna.lay@cadt.edu.kh

Identifying a Security breach

- **The Inevitability of Breaches:** Data breach are almost certain to happen, the question is where and when.
- **Your responsibility:** You're responsible for your own systems, so recognizing a breach is crucial
- **Three Common Overt Breaches**
  - **Ransomware**
  - **Defacement**
  - **Claimed Destruction**

Ransomware: The Rising Threat

- **Ransomware:** Encrypts or steals data, demands ransom for restoration
- **The Ultimatum:** Often includes a deadline with threats of permanent data destruction
- **Epidemic:** Increasingly popular among financially motivated cyber attackers.
- **Beware of Fake Smartphone Ransomware:** Verify the threat before taking action.

Defacement

- **Defacement Defined:** Attackers alter your website or online presence to leave their mark
- **Motivations:** mostly hacktivists
- **Recognizing Defacement**
  - Website displaying a “hacked” message.
  - Computer booting up with a similar message.
- **Location of Breach:** Could be your computer or the hosting site.

Claimed destruction

- **Data Destruction:** This can be caused by hackers, technical failures, or human error.
- **The Claim of Responsibility:** Significantly increases the likelihood of a breach.
- **False Claims:** Some parties may falsely claim responsibility to boast their skills.
- **Verifying the Claim:**
  - Specific knowledge of deleted files indicates a higher probability of a breach.
  - Rule out technical failures or human error based on the nature of the missing data.

Detecting Covert Breaches

- **The Hidden Threat**
- **Clues, Not Guarantees**
- **Multiple Symptom or Timing:** Raise suspicion, especially after risky actions
- **Consider the Context:** Operating system updates vs. suspicious emails offering riches.
- **The Importance of Calm:** Panicking hinders problem-solving, focus on minimizing damage.

Signs Your Device Might Be Compromised

- **Slower Performance:** Malware can slow down your device and internet connection.
  - **Rule out other factors:** OS updates, software upgrades...
  - **Check Task Manager/Activity Monitor:** Identify running processes.
- **Task Manager/Activity Monitor Not Running:** Malware can disable these tools
- **Latency Issues:** Delays in data transmission, check network connection and rule out external factors.
- **Communication and Buffering Issues (e.g., Streaming Videos):** Could be a sign of a compromised system or unauthorized connection sharing ("piggybacking").

Signs Your Device Might Be Compromised

- **Changed Settings:** If settings are altered without your knowledge, be cautious.
- **Strange Emails/Texts:** Receiving or sending messages you didn't initiate is a red flag.
- **New Software/Apps:** Unexpected installations could be malicious.
- **Rapid Battery Drain:** Malware running in the background can consume power.
- **Device Overheating:** Increased CPU usage by malware can cause higher temperatures.
- **Altered File Contents:** Unexplained changes to files are suspicious.
- **Missing Files:** Files disappearing without your knowledge could be a sign of a breach.
- **Websites Displaying Differently:** Malware can act as a proxy, affecting how websites appear.

Signs Your Device Might Be Compromised

- **Unexpected Proxy Settings:** If you didn't set up a proxy, someone else might be using it to intercept your data.
- **Apps Stop Working:** Malware or proxy interference can disrupt normal app functionality.
- **Security Programs Disabled:** Malware can disarm your defenses to avoid detection.
- **Increased Network Traffic:** Unexplained traffic spikes could be malware communication.
- **Unusual Open Ports:** Unexpectedly open ports might indicate unauthorized access.
- **Frequent Crashes:** Malware can destabilize your device.
- **Unknown Programs Requesting Access:** Be wary of unfamiliar software seeking internet access.

Signs Your Device Might Be Compromised

- **External Devices Powering On Unexpectedly:** Malware can activate peripherals without your knowledge.
- **Device Acts as if Someone Else is Using It:** Mouse movements, keystrokes, etc.,without your input could indicate remote access.
- **New Default Search Engine:** Changes to your browser settings without your knowledge are suspicious.
- **Device Password Changed:** This is a major red flag and suggests unauthorized access.
- **Pop-ups Appearing:** Unwanted pop-ups, especially outside a browser, could be malware.

Signs Your Device Might Be Compromised

- **New Browser Add-ons:** Unexpected add-ons might be malicious.
- **New Browser Home Page:** If your home page changes without your action, it could be a sign of tampering.
- **Email Blocked by Spam Filters:** This could indicate your email configuration has been altered to relay through a compromised server.
- **Device Trying to Access Blocked Sites:** Attempting to reach restricted websites could indicate malware activity.
- **Unusual Service Disruptions (Phones)**

Signs Your Device Might Be Compromised

- **Changed Language Settings:** Unexpected language changes could be a sign of unauthorized access.
- **Unexplained Activity on Device:** Unfamiliar emails in your sent folder or unexpected downloads are suspicious.
- **Unexplained Online Activity:** Unauthorized social media posts, video rentals, or purchases indicate a potential breach.
- **Sudden Restarts:** Unexplained reboots could be a sign of malware.
- **Signs of Data Breaches/Leaks:** If your data is compromised elsewhere, check your devices

Signs Your Device Might Be Compromised

- **Routed to Wrong Website:** Incorrect routing, especially from specific devices or networks, could indicate a compromise.
- **Hard Drive/SSD Light Constantly On:** Excessive disk activity could be a sign of malware.
- **Other Abnormal Things:** Any unusual behavior not explained by normal usage or updates should raise suspicion.

Question

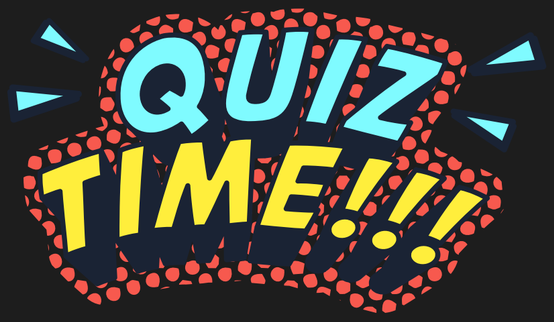
Which of the following is NOT a potential sign of a compromised device?

(A) Slower performance

(B) Unexpected phone charges

(C) Regular operating system updates

(D) New browser home page



Question

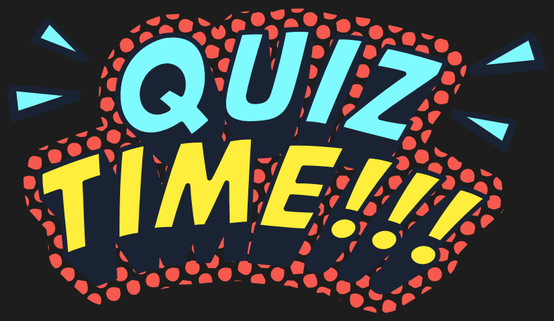
If your smartphone's battery drains much faster than usual, it could indicate:

(A) Normal battery aging

(B) Malware running in the background

(C) High screen brightness

(D) All of the above



Question

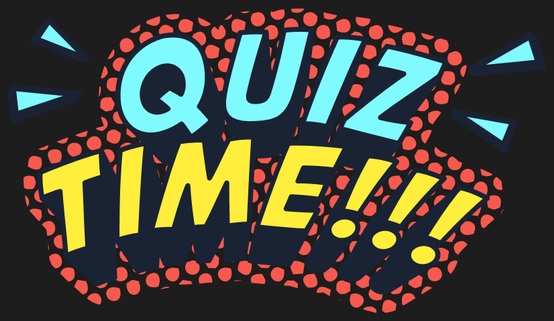
You notice strange emails in your sent folder that you didn't send. This likely means:

(A) Your email provider is having technical difficulties

(B) Your device or email account is compromised

(C) You accidentally sent the emails

(D) Your friends are playing a prank



Question

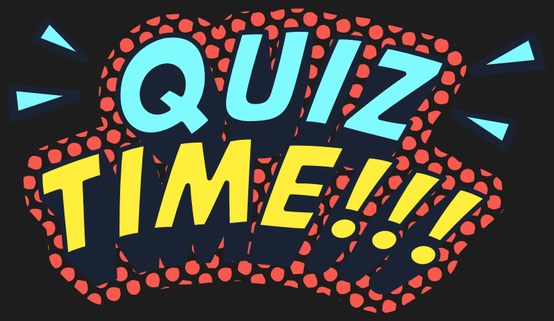
Which of the following could indicate malware is interfering with your internet activity?

(A) Websites appearing different than usual

(B) Being routed to the wrong website even after typing the correct URL

(C) Unexpected proxy settings in your browser

(D) All of the above



Question

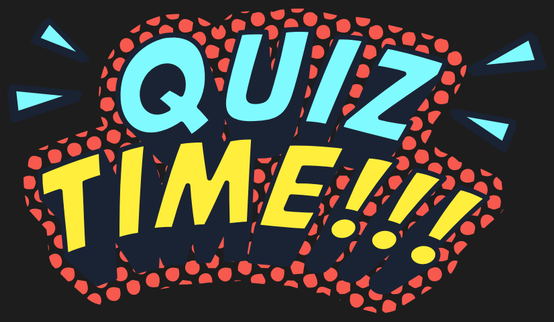
If apps you regularly use suddenly stop working correctly, it could be due to:

(A) A recent operating system update

(B) Malware interfering with their functionality

(C) A bug in the app itself

(D) Any of the above



Question

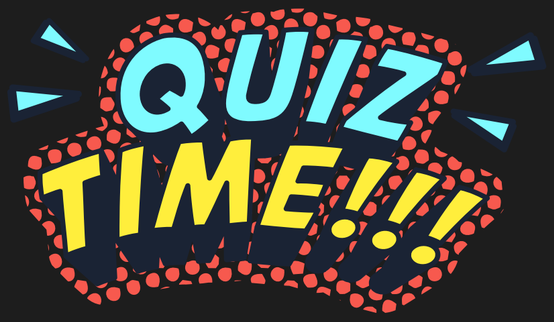
Which of the following is NOT a typical sign of a compromised device?

(A) Increased data usage

(B) Regular software updates from trusted sources

(C) Unexpected pop-up ads

(D) New browser extensions you didn't install



Question

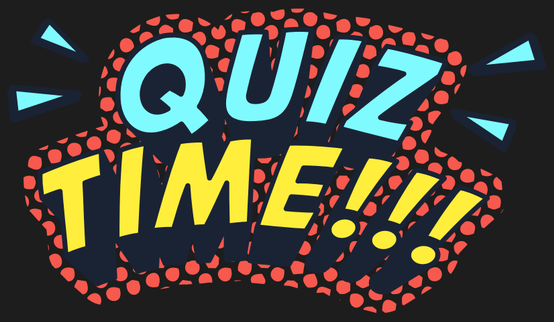
What should you do if you suspect your device is compromised?

(A) Panic and immediately throw away the device

(B) Click on any pop-up ads to see what they do

(C) Stay calm, disconnect from the internet, and run a virus scan

(D) Ignore the issue and hope it goes away



Question

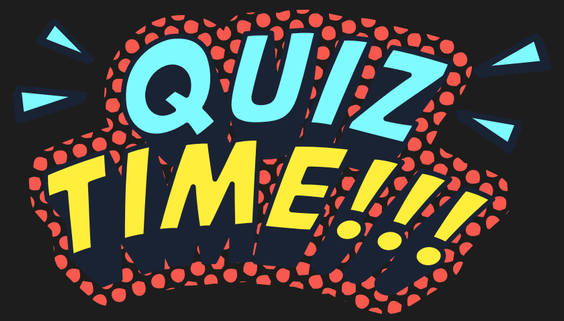
Which of the following scenarios MOST strongly suggests a device has been compromised rather than experiencing a technical glitch?

(A) Your laptop's battery drains slightly faster than usual.

(B) Your smartphone reboots unexpectedly once after a software update.

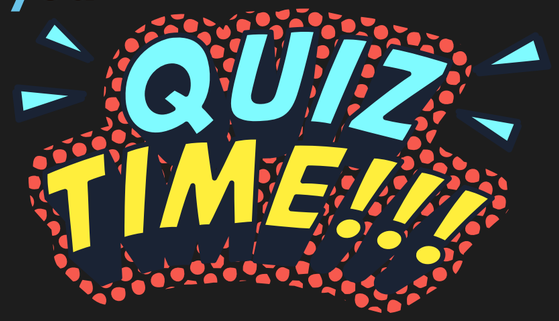
(C) You notice a new, unknown process running in Task Manager with a randomly generated name and high resource usage.

(D) Your internet connection is temporarily slow during peak hours.



Question

You've been receiving complaints that emails seemingly from your account are being marked as spam. Upon checking your sent folder, you find emails you didn't send. What's the MOST likely explanation?



(A) Your email provider is experiencing technical difficulties.

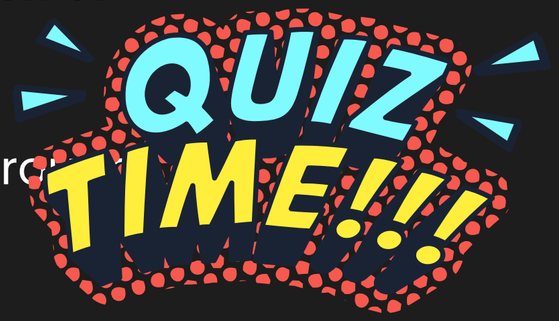
(B) Your email account's password has been compromised.

(C) Your device has been infected with malware that is using your account to send spam.

(D) Both b and c are possible.

Question

Your computer's network traffic monitor shows a significant increase in outgoing data, even when you're not actively using the internet. Which of the following is the LEAST likely explanation?



(A) Your computer is downloading and installing updates in the backgr

(B) Malware is sending data from your computer to a remote server.

(C) A cloud backup service is synchronizing your files.

(D) Your neighbor is stealing your Wi-Fi.

Question

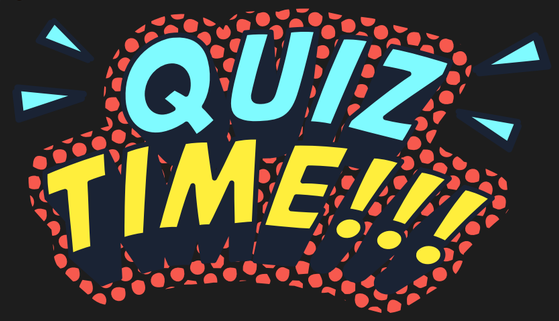
You observe your webcam's LED light turning on briefly even when you're not using it. Which of the following is the MOST concerning possibility?

(A) A software glitch is causing the camera to activate randomly.

(B) The webcam is malfunctioning and needs to be replaced.

(C) Malware is accessing your webcam without your knowledge.

(D) The webcam's settings are incorrectly configured.



Responding to a Security Breach: Preparation is Key

- **The Importance of Preparation:** Proactive prevention is the best defense against breaches.
- **Managing Emotions:** It's normal to feel upset or panicked, but clear thinking is essential.
- **Avoid Rash Actions:** Don't rely on random online advice, especially from questionable websites.
- **Act Quickly:** Stop other activities, save and backup your data, and focus on recovery.
- **Time is of the Essence:** The sooner you act, the better your chances of minimizing damage.

When in Doubt, Bring in a Cybersecurity Pro!

- **Expertise Matters:** Cybersecurity professionals have the experience and skills to handle complex breaches.
- **Just Like Other Emergencies:**
  - Serious illness ➜ Doctor/Hospital
  - Legal Trouble ➜ Lawyer
  - IRS Audit ➜ Accountant
- **Don't Go It Alone:** Professional help can save you time, money, and further damage.

Recovering from a Breach without a Pro’s Help

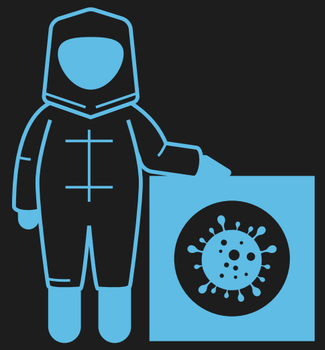
- 1. Figure out what happened (or is happening).
- 2. Contain the attack.
- 3. Terminate and eliminate the attack.

Figure out what happened (or is happening)

- **Gather information**
  - What happened?
  - Which system were effected?
  - what can the attacker do with the stolen data?
  - What data/programs were impacted?
  - Who else might be at risk (including your employer)?
  - Who needs to be notified immediately?
- The Reality of Undetected Attacks:
  - Even businesses with security teams take months to discover breaches.
- Don't Dwell, Act Quickly:
  - Gather essential information, but prioritize taking action to contain the damage.

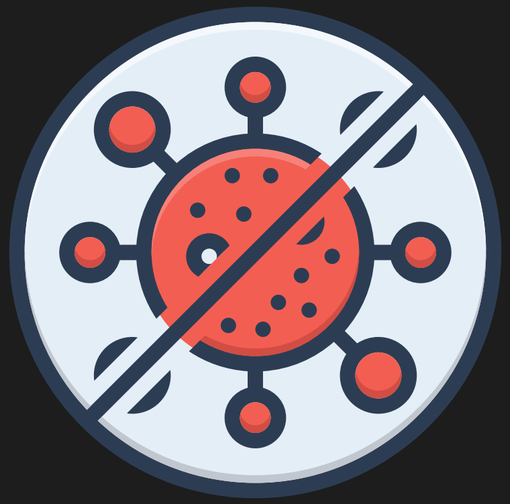
Contain the attack

- **Isolate the Attacker:** Disconnect the compromised device(s) from all communication channels.
- **Termination Methods:**
  - Turn off router: Disconnect the entire network (not always feasible in business settings).
  - Unplug Ethernet cables: Isolate individual devices.
  - Turn off Wi-Fi/Cellular Data: Prevent wireless transmission.
  - Disable Bluetooth/NFC: Block short-range communication.
  - Disconnect USB drives: Prevent malware spread.
  - Revoke attacker's access rights: If applicable, restrict compromised accounts.
- **Prioritize Isolation:** If internet access is needed for cleanup, disconnect all other devices.



Terminate and eliminate the attack.

- **Containment vs. Elimination:**
  - Disconnecting a device is not enough; malware and vulnerabilities remain.
- **The Importance of Cleanup:**
  - Thoroughly remove malware and address security weaknesses.



Back up Your Data

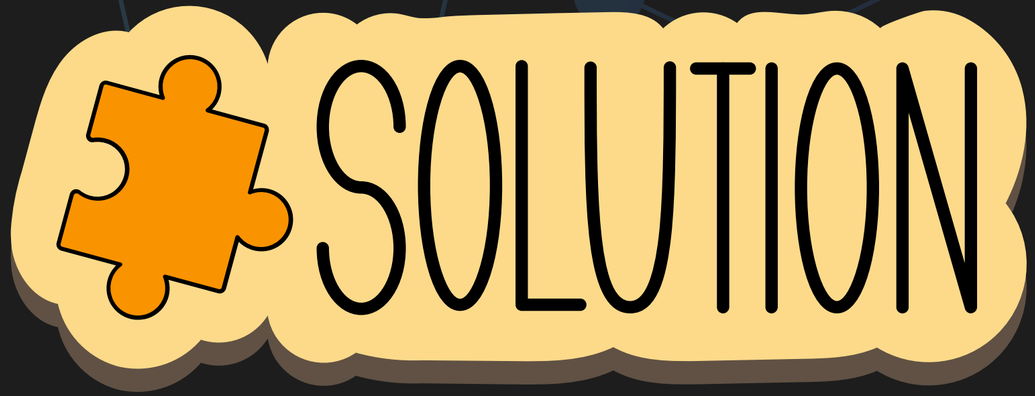
- **Back up:**
  - **Critical Step:** Create a backup on an external drive that you haven't connected to other devices.
  - **Don't Overwrite Existing Backups:** Use separate media for this backup.
- **Delete Junk Files (Optional):**
  - **Benefit**
    - Speeds up security scans
    - May Directly remove some maleware

Run a Full System Scan

- **Importance:** Security software can detect and remove malware.
- **Use Multiple Vendors:** For thoroughness, use security software from different vendors.
- **Update Before Scanning (Mac Safe Boot):** Ensure you have the latest virus definitions.
- **Analyze Security Reports:** Note removed or repaired files, which can help with troubleshooting.
- **Address Non-Critical Issues:** Tracking cookies or adware may not be urgent but can be removed.
- **Run Additional Scanners (If Recommended): F**ollow security software prompts, but only from official sources. Beware of fake pop-up warnings.

Dealing with Stolen Information

- Change password
- Check Account
- Consider Credit Freeze
- Contact Card Issuers
- Keep a log
- Notify other
- Act Quickly, Especially for sensitive data



Type of Stolen Information

- **Not Private, but Helpful for Identity Theft:** Name, address, phone number, public records.
- **Sensitive:** Email addresses, phone numbers, partial card numbers, IDs, birthdays.
- **More Sensitive:** Social Security numbers, passwords, bank accounts, PINs, full card information, security question answers.

Learning for the Future

- **Analyze the Breach:** Understand how and why the attack occurred.
- **Implement Preventive Measures:** Develop policies and procedures to avoid similar incidents in the future.
- **Seek Professional Guidance:** A cybersecurity expert can help you identify vulnerabilities and strengthen your defenses.

Question

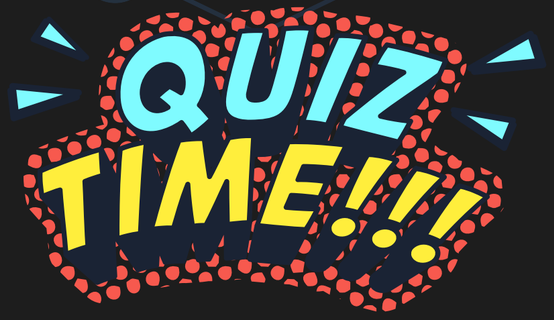
Which of the following actions should be taken FIRST when containing a security breach on a personal device?

A. Delete all temporary files.

B. Disconnect the device from the internet.

C. Reinstall the operating system.

D. Change all your passwords.



Question

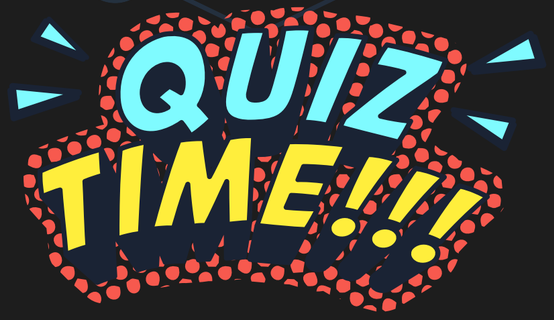
Which type of hacker is often hired by companies to test their security systems?

A. Black hat hacker

B. Gray hat hacker

C. White hat hacker

D. Blue hat hacker



Question

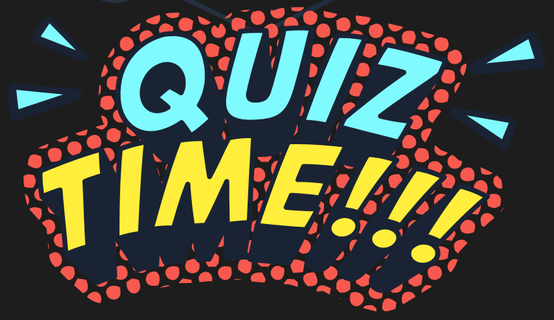
When dealing with a ransomware attack, which of the following is the LEAST recommended course of action?

A. Paying the ransom

B. Disconnecting the affected device from the internet.

C. Reporting the incident to law enforcement

D. Attempting to restore data from backups



Question

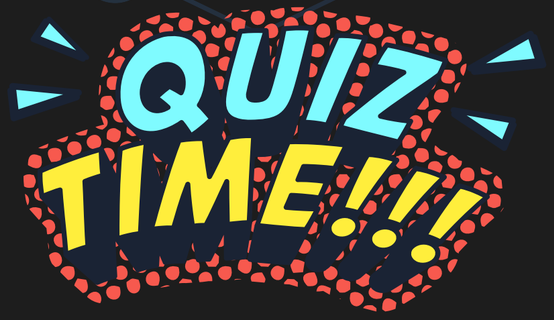
After containing a breach, which of the following is the MOST important next step?

A. Reinstall all software on the affected device

B. Run a full system scan with updated security software

C. Change all your passwords

D. Contact your friends and family to warn them



Question

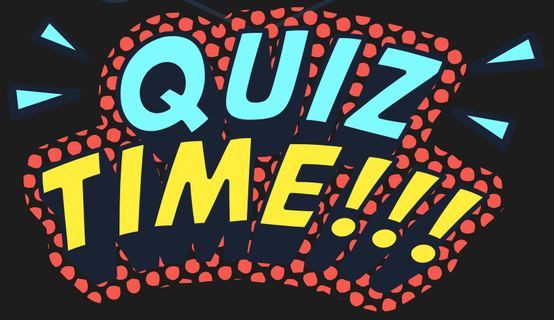
Which of the following statements about seeking professional help during a breach is TRUE?

A. It's only necessary for large corporations and not individuals.

B. It's a sign of weakness and should be avoided.

C. It can save time, money, and prevent further damage.

D. It should only be considered as a last resort.



Question

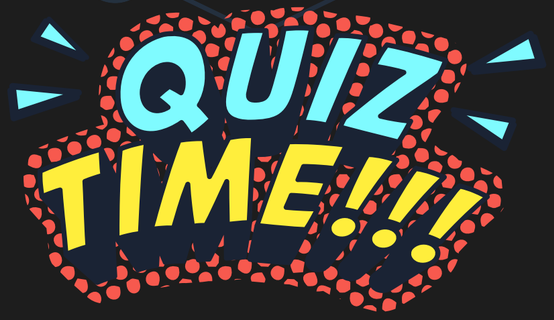
Why is it important to back up your data regularly, especially in the context of security breaches?

A. To ensure you have a copy of your data in case of theft or damage.

B. To speed up the recovery process after a breach

C. To potentially avoid paying a ransom in case of a ransomware attack

D. All of above



Question

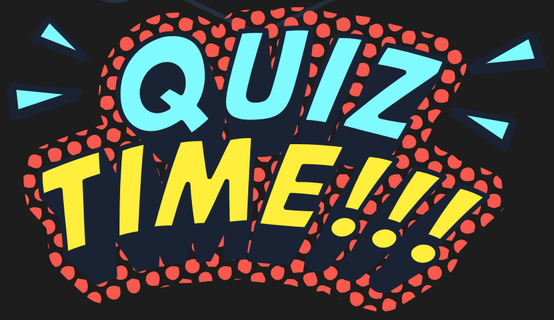
Which of the following is NOT a recommended step after a breach?

A. Analyze how the attack occurred to prevent future incidents.

B. Keep the breach a secret to avoid embarrassment or legal repercussions.

C. Change passwords for any accounts potentially compromised.

D. Contact relevant parties who might be affected by the breach.



Question

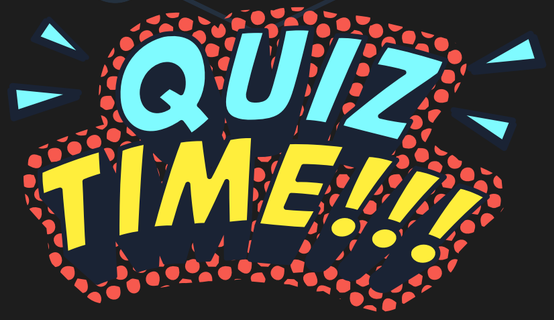
If you suspect your device is compromised but a security scan comes up clean, what should you do?

A. Assume everything is fine and continue using the device as usual.

B. Try running the security scan again after updating the software.

C. Consider using a different security software or seeking professional help

D. Both b and c are valid options.



Question

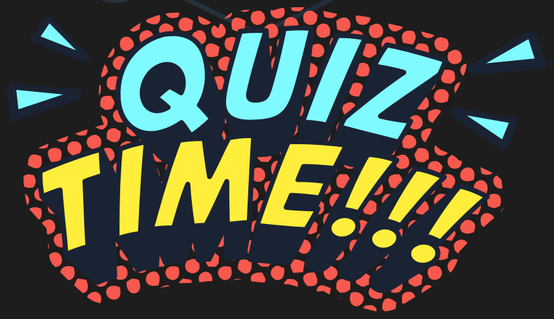
What is the primary goal of "containing" an attack?

A. Removing all malware from the affected device

B. Restoring lost or corrupted data

C. Preventing the attacker from causing further damage or spreading malware

D. Identifying the source of the attack



Question

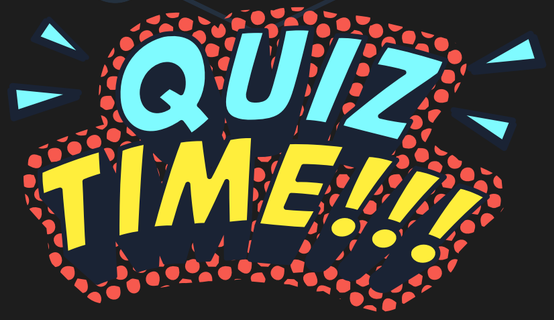
Which of the following is NOT a recommended way to contain a security breach on a device?

A. Disconnect the device from the internet.

B. Turn off Wi-Fi and Bluetooth.

C. Remove any connected external drives.

D. Immediately delete all files on the device.




?
Q&A