Cyber Security

2024

Personal Cybersecurity

Vathna.lay@cadt.edu.kh

Identifying Ways You May Be Less than Secure

- Your home computer(s)
- Your mobile devices
- Your Internet of Things (IoT) devices
- Your networking environment
- Your working environment

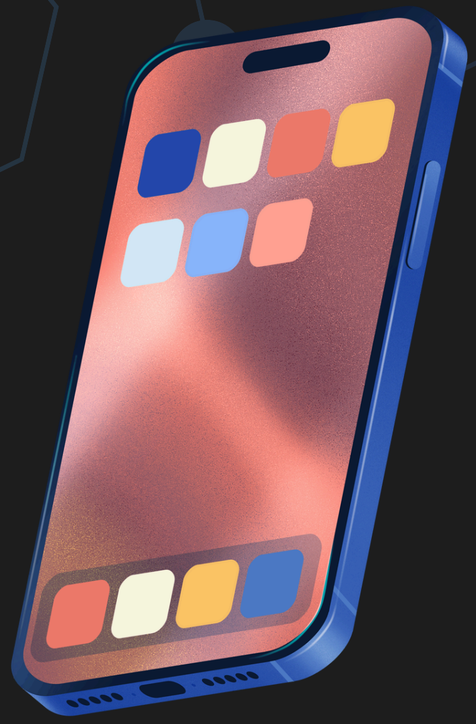
Your home computer(s)

Is Your Home Computer a Sitting Duck for Cyberattacks?

- **Breached:** Imagine someone breaking into your house
- **Malware (The Digital Disease):** Like a cold or flu, malware infects your computer
- **Shared Computers** (Sharing is NOT Always Caring)
- **Connections to Other Networks** (The Open Door Policy)
- **Physical Security** (The First Line of Defense)

Mobile Devices: A Cybersecurity Minefield?

- Always connected
- Data Goldmine
- Communication Hub
- Unwanted Messages
- Limited Security
- Easy to Lose or Damage
- Risky Wi-Fi
- Device Disposal



(IoT): A Security Nightmare?

- Explosive Growth
- Everyday Objects, Now Connected
- Inadequate Security
- Open Doors for Hackers
- Real-World Risks

Beyond Your Computer

- **Networking Equipment Under Attack:** Your router, modem, and other network devices aren't immune to hacking
- **Work-From-Home Dangers**
- **The "Bring Your Own Device" Risk**
- **Beware of Nosy Colleague**

Identifying Risks

- You Can't Protect What You Don't Know
- Digital Assets
- Why Inventory Matters
  - Identify Vulnerabilities
  - Track Threats
  - Recovery Planning

Protecting against Risks

- **Perimeter Defense**
- **Firewall/Router**
- **Security Software**
- **Your Physical Computer(s) and Other Endpoints**
- **Backups (Your Safety Net):**

Perimeter Defense

- **Filtering Traffic:** The firewall/router examines each packet of data entering or leaving your network, checking it against a set of rules.
- **Blocking Threats**
- **Protecting Your Devices**

Your Router: The Unsung Hero of Home Cybersecurity

- **More Than Just Internet Access:** Your router is a powerful security tool, acting as a firewall to block unwanted traffic and protect your devices.
- **Router Security Checklist**
  - **Updates:** Keep your router's firmware up to date.
  - **Replace Old Routers**
  - **Strong Passwords**
  - **Unique Wi-Fi Name (SSID)**
  - **Encryption:** Enable WPA3 encryption if possible, or at least WPA2.

Your Router: The Unsung Hero of Home Cybersecurity

- **Router Security Checklist**
  - **Strong Wi-Fi Password:** Use a complex password to prevent unauthorized access.
  - **Disable Older Wi-Fi Protocols:** Stick to Wi-Fi 6 and 5 for better security and performance.
  - **MAC Address Filtering/Guest Network:** Control who can connect to your network, especially if you have visitors.
  - **Optimal Placement**
  - **Disable Remote Access**

Security software

- **Essential Tools:**
  - **Antivirus**
  - **Personal Firewall**
  - **Antispam**
  - **Remote Wipe:** This allows you to erase data on a lost or stolen mobile device.
  - **Strong Passwords**
  - **Auto-Updates**

Backups & Detection

- **Backups:** Your Digital Insurance Policy
  - **Full Backup:** Copies all your data.
  - **Incremental Backup:** Copies only changes made since the last backup.
  - **Cloud Backup:** Stores your data securely off-site.
- **Detection:** Your Early Warning System
  - **The Importance of Early Detection**
  - **Security Software's Role**
  - **Be Observant**

Responding: Don't Panic, Act Fast!

- **Backups:** Your Digital Insurance Policy
  - **The Importance of Rapid Response**
  - **Security Software's Role**
  - **Your Responsibility**
- **Recovery:** Bouncing Back from a Cyberattack
  - Assess the Damage
  - Restore from Backups
  - Seek Help if Needed

Question

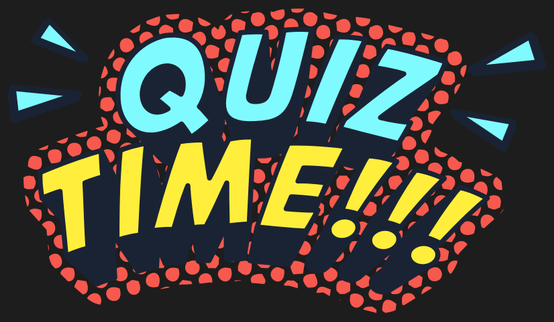
Which of the following is NOT a common sign of a compromised home computer?

(A) Unexpected pop-up ads or messages

(B) Slow performance

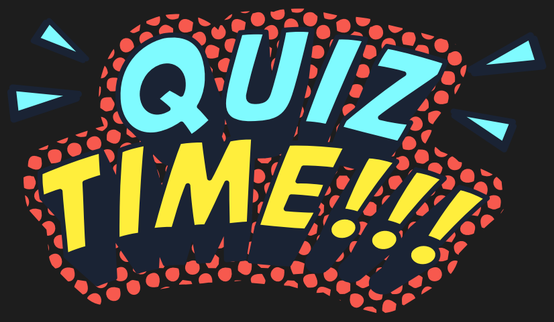
(C) Unexplained changes to files or settings

(D) Regular software updates



Question

What is the PRIMARY purpose of a firewall/router in a home network?



(A) Boosting Wi-Fi signal strength

(B) Filtering traffic and blocking unauthorized access

(C) Storing backup data

(D) Providing internet connectivity

Question

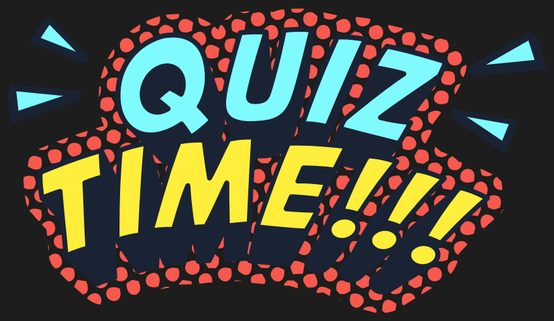
Which of the following is the MOST secure encryption standard for Wi-Fi networks?

(A) WPA

(B) WEP

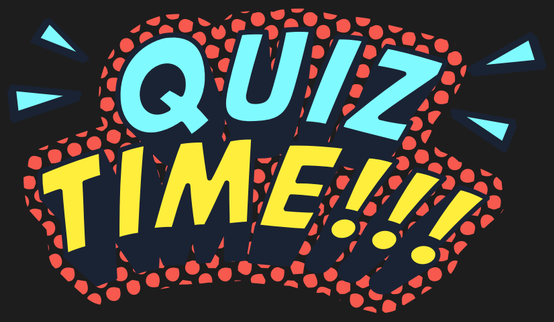
(C) WPA2

(D) WPA3



Question

What is the MAIN reason for creating a backup of your computer data?



(A) To free up storage space on your hard drive

(B) To protect against data loss due to hardware failure, theft, or accidental deletion

(C) To speed up your computer

(D) To share files with others

Question

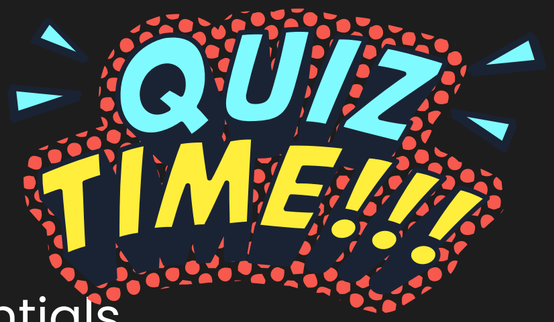
Which of the following is a common method used by hackers to gain access to home networks?

(A) Exploiting vulnerabilities in outdated router firmware

(B) Guessing weak Wi-Fi passwords

(C) Using phishing emails to trick users into revealing login credentials

(D) All of the above



Question

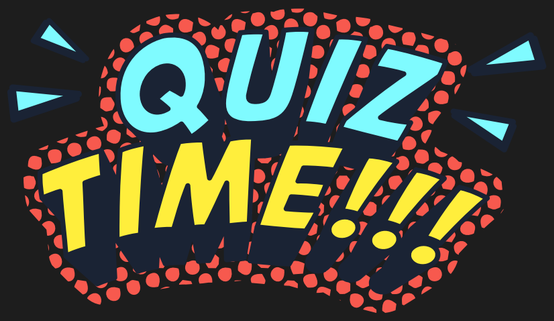
What is the primary function of antivirus software?

(A) Encrypting sensitive files

(B) Blocking spam emails

(C) Detecting and removing malicious software

(D) Creating strong passwords



Question

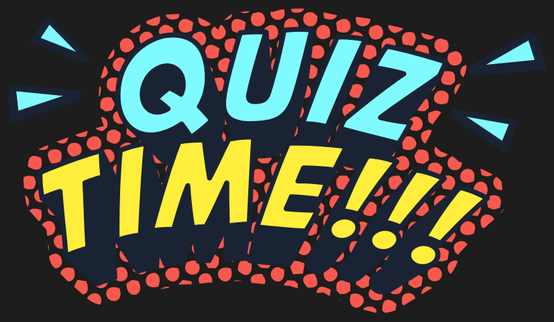
Which of the following is an example of a physical security measure for your computer?

(A) Using a strong password

(B) Installing antivirus software

(C) Keeping your computer in a locked room

(D) Encrypting your hard drive



Question

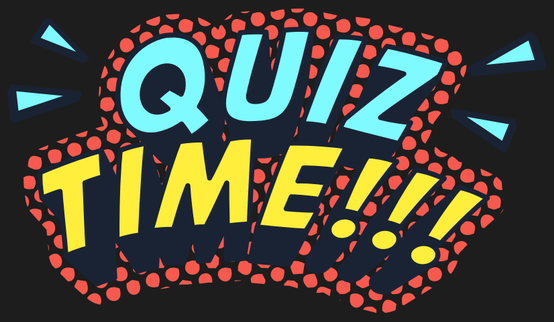
What is the first step in securing your digital life?

(A) Installing a firewall

(B) Creating a strong password

(C) Taking an inventory of your digital assets

(D) Encrypting your data



Question

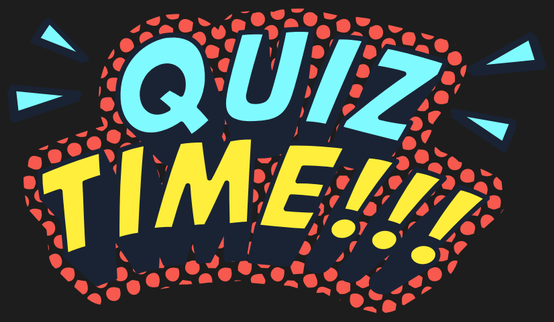
What should you do if you suspect your computer has been infected with malware?

(A) Disconnect from the internet

(B) Run a full system scan with your antivirus software

(C) Change your passwords

(D) All of the above



Question

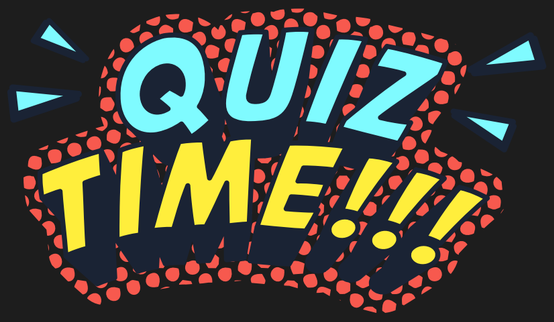
Which of the following is NOT a best practice for disposing of old electronic devices?

(A) Using a data wiping tool to erase sensitive data

(B) Removing the hard drive and physically destroying it

(C) Simply deleting files and throwing the device away

(D) Donating the device to a reputable organization

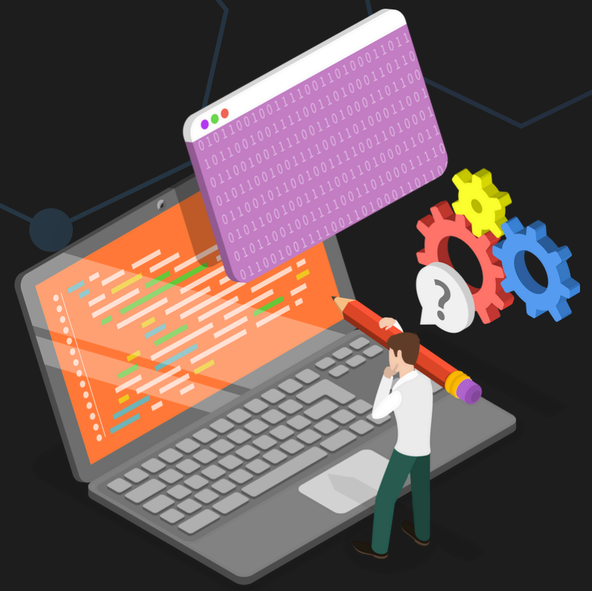


Evaluating Your Current Security Measures

- Software
- Hardware
- Insurance
- Education

Software

- Legitimacy
- Support
- Updates
- Security Software
- Additional Protections
- Permissions



Hardware Security: The Foundation

- Trusted Source
- Brand Reputation
- Physical Protection
- Travel Security
- Power Protection
- Firmware Updates
- Router/Firewall Security
- BIOS Password
- Unused Wireless Protocols

Cybersecurity Insurance

- **Data recovery:** Restoring lost or stolen data.
- **Legal fees:** Defending yourself against lawsuits or regulatory actions.
- **Notification costs**: Notifying customers or clients of a data breach.
- **Business interruption:** Lost income due to downtime caused by a cyberattack.

Education (Starts at Home)

- Family Cyber-Rules
- Phishing Awareness
- Cyber Hygiene
- Password Management
- Oversharing on Social Media
- Think Before You Click
- Think Before You Share
- Think Before you post

Question

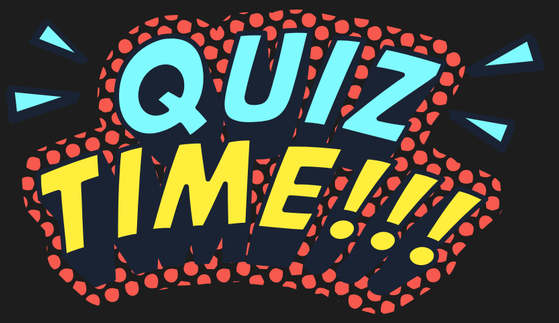
Which of the following is NOT a reason to be cautious about sharing personal information online?

A. The risk of identity theft.

B. The potential for your data to be sold to third parties

C. The possibility of cyberbullying or harassment

D. The convenience of auto-filling forms.



Question

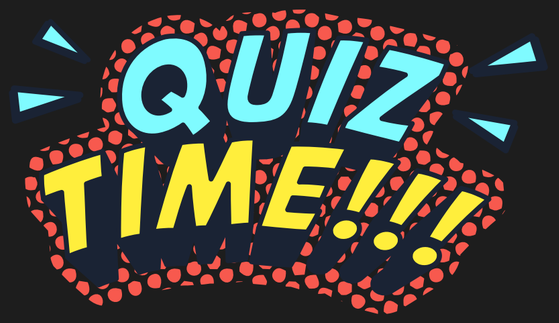
What is a common example of oversharing personal information in a physical setting?

A. Sharing your credit card details with a friend

B. Providing your Social Security number on a doctor's office form

C. Posting your vacation photos on social media

D. Using a public Wi-Fi network for online banking



Question

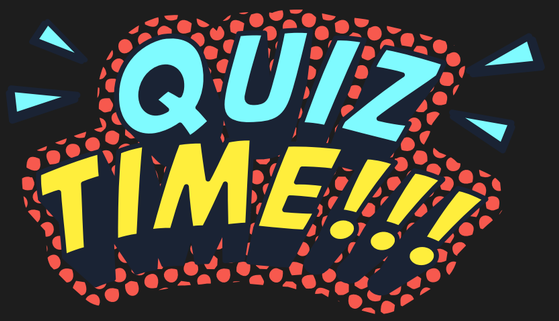
How does oversharing personal information increase your risk of a privacy violation?

A. It makes you a more attractive target for hackers.

B. It gives companies more data to use for targeted advertising

C. The more places your data is stored, the greater the chance of a data breach exposing it.

D. All of the above



Question

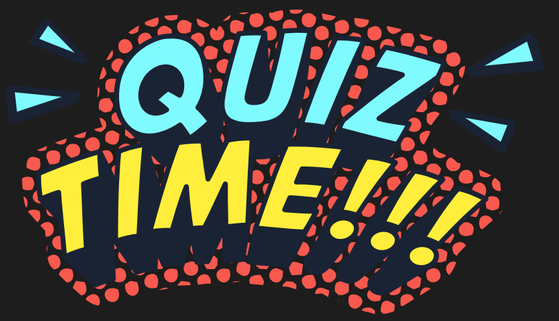
Which of the following is the BEST way to protect your privacy online?

A. Use strong passwords and two-factor authentication.

B. Be selective about the information you share.

C. Read privacy policies before using websites and apps.

D. All of the above..



Question

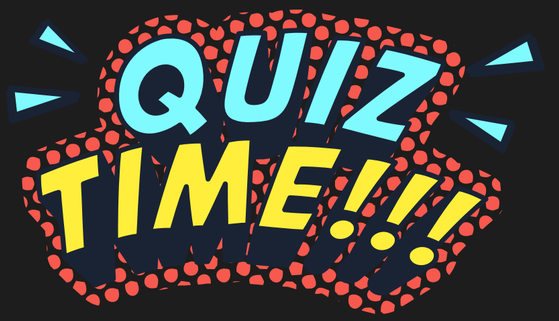
When is it okay to share personal information with a company or organization?

A. When they ask for it.

B. When you trust the company.

C. When you need their services or products.

D. When the information is absolutely necessary for the transaction or service.



Question

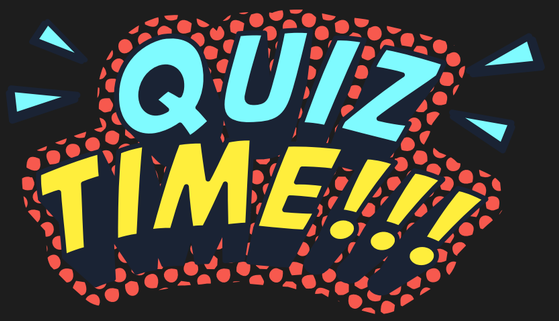
Why is it important to "think before you share" on social media?

A. To avoid embarrassing yourself.

B. To protect your personal information from being misused.

C. To prevent identity theft.

D. Both b and c.



Question

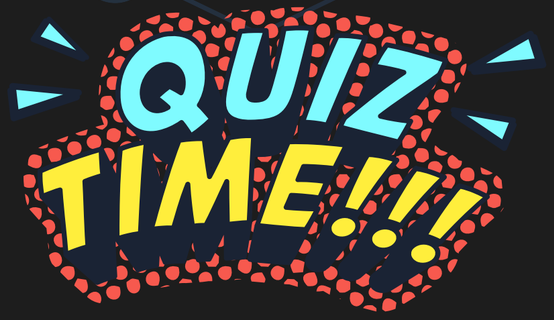
Which of the following is NOT a potential consequence of oversharing personal information?

A. Targeted advertising

B. Identity theft

C. Financial fraud.

D. None



Question

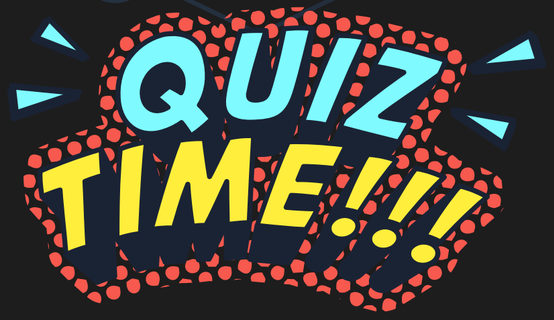
Which type of hacker is often hired by companies to test their security systems?

A. Black hat hacker

B. Gray hat hacker

C. White hat hacker

D. Blue hat hacker



Question

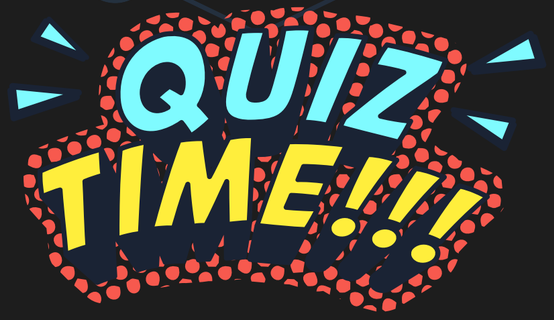
How can you reduce your risk of privacy violations due to data breaches?

A. Avoid using online services.

B. Limit the amount of personal information you share online and offline.

C. Only share information with government agencies.

D. Use a different password for every website and app.



Question

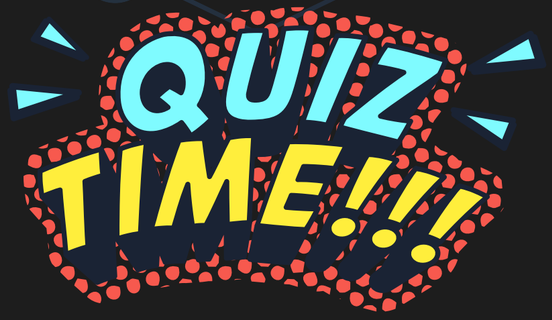
What should you do if a website or app asks for more information than you're comfortable sharing?

A. Provide fake information.

B. Leave the fields blank.

C. Consider whether you really need to use the service or app.

D. All of the above



Question

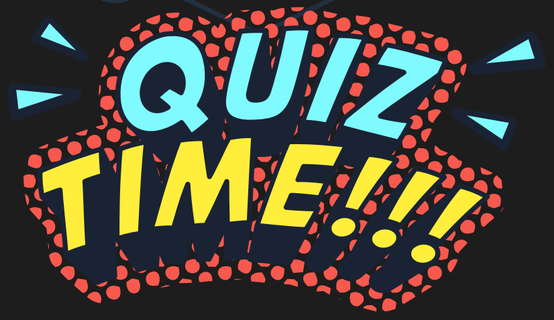
What is the main message of "think before you share"?

A. Be suspicious of everyone who asks for your personal information.

B. Never share any personal information online.

C. Be mindful of the information you share and who you share it with..

D. Only share personal information with family and friends..




?
Q&A