STAYING SAFE FROM ONLINE VIRUSES

Mankato computer Technology University

Introduction

- Staying safe from online viruses is essential to protect your devices and personal information. Here are practical tips to reduce the risk:

Install Antivirus Software

By following these steps, you'll significantly reduce the risk of falling victim to malware and other cyber threats.

Use reputable antivirus software and keep it updated.

Enable real-time scanning to detect threats immediately.

Installing antivirus software is a critical step to protect your devices from online threats. Here's a step-by-step guide: *Choose Reputable Antivirus Software*

Research and select a trusted antivirus program. Popular options include:

Free Options: Avast, AVG, Microsoft Defender (built into Windows 10/11)

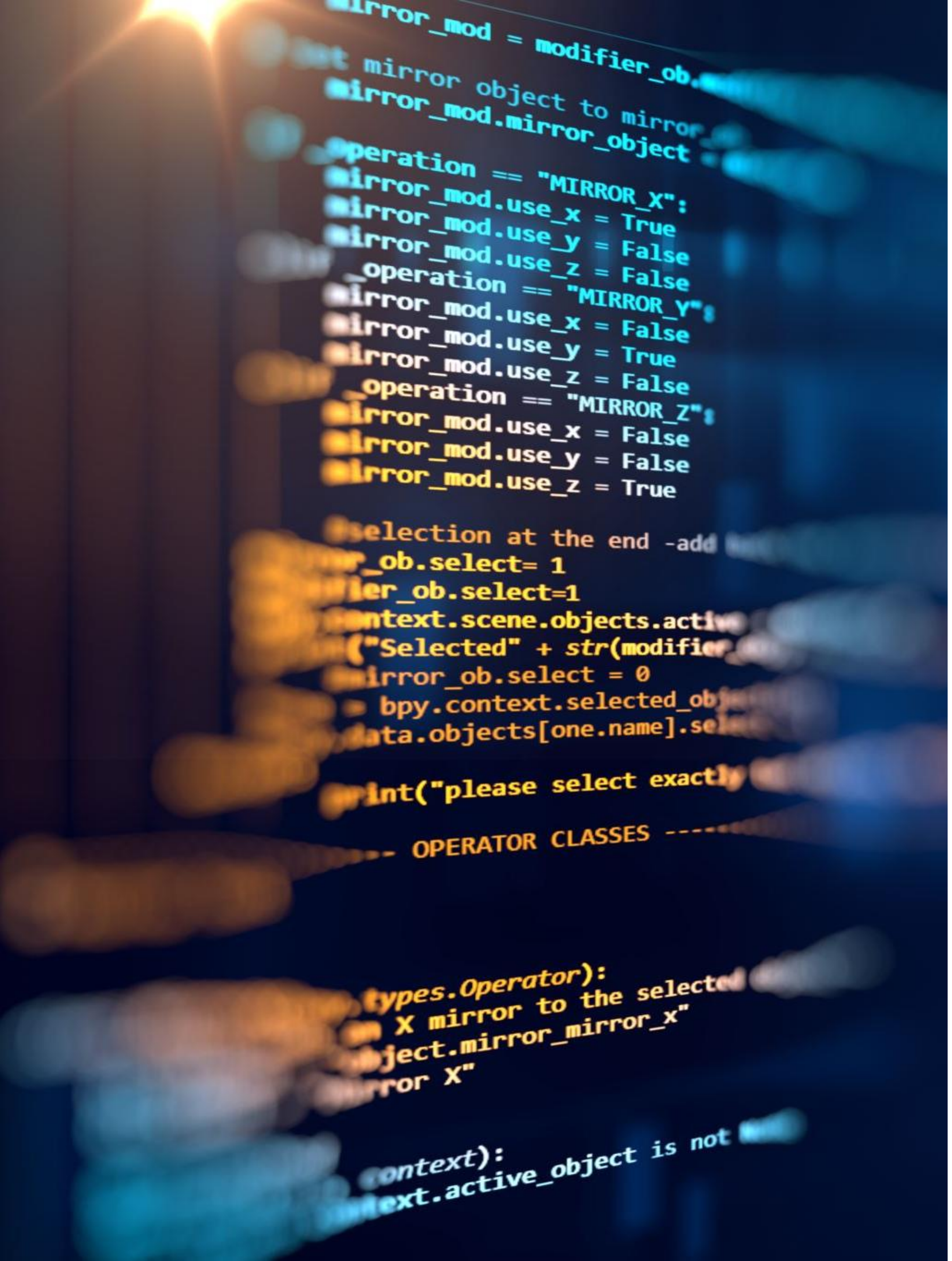
Paid Options: Norton, McAfee, Bitdefender, Kaspersky

Consider your needs (e.g., personal vs. business use, budget, features).

Download from the Official Website

Visit the official website of the antivirus provider.

Avoid third-party sites or pop-ups offering free downloads to prevent malware.



Update the Virus Database

- Once installed, allow the software to update its virus definitions. This ensures it can detect the latest threats.

Run an Initial Scan

PERFORM A FULL SYSTEM SCAN TO CHECK FOR EXISTING VIRUSES OR MALWARE.

FOLLOW THE SOFTWARE’S RECOMMENDATIONS IF THREATS ARE DETECTED.

Set Up Automatic Scans

Schedule regular scans (e.g., daily or weekly).

Enable real-time protection to monitor your device continuously.

Keep Software Updated

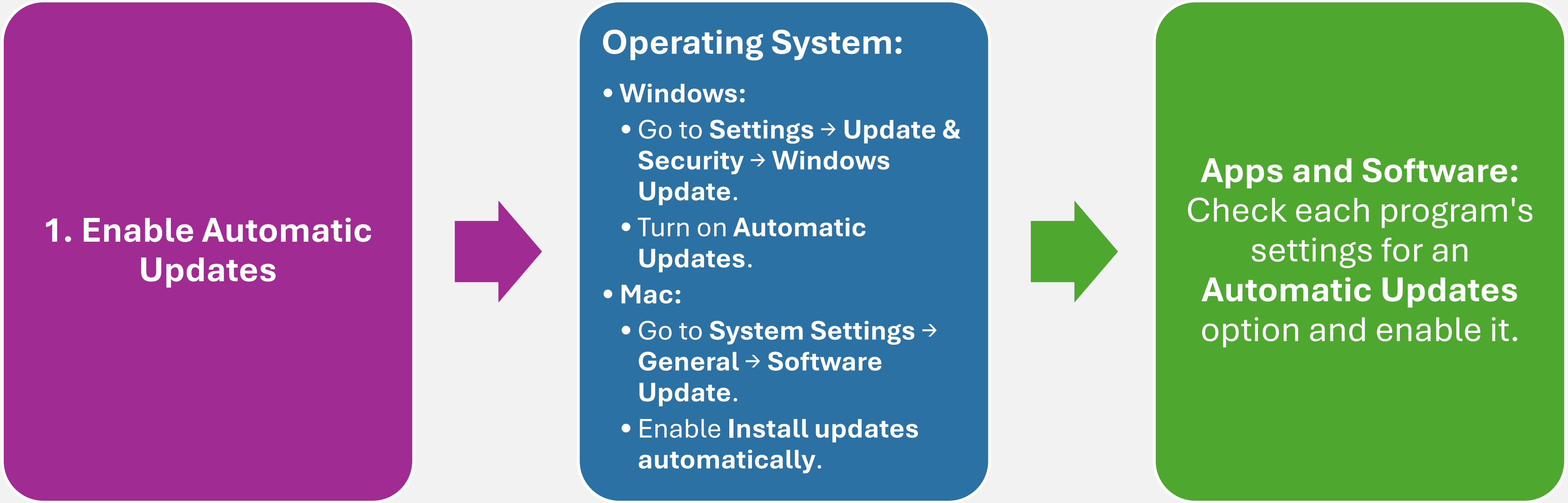
Keeping your software updated is vital to protect against vulnerabilities, bugs, and cyber threats. Here's a step-by-step guide to ensure your system stays up to date:

Regularly update your operating system, browsers, and other software to fix security vulnerabilities.

Enable automatic updates whenever possible.

How to Keep Software Updated

Keeping your software updated is vital to protect against vulnerabilities, bugs, and cyber threats. Here’s a step-by-step guide to ensure your system stays up to date:



1. Enable Automatic Updates

Operating System:

- **Windows:**
  - Go to **Settings** → **Update & Security** → **Windows Update**.
  - Turn on **Automatic Updates**.
- **Mac:**
  - Go to **System Settings** → **General** → **Software Update**.
  - Enable **Install updates automatically**.

Apps and Software: Check each program's settings for an **Automatic Updates** option and enable it.

Manually Check for Updates

Operating System:

- Windows: Go to **Settings** → **Update & Security** → **Windows Update**, then click **Check for updates**.
- Mac: Open **System Settings** → **General** → **Software Update** → **Check Now**.

Apps and Browsers:

- Open the app, go to its **Help** or **About** section, and look for an **Update** option.

Update Drivers and Firmware

Keep hardware drivers (e.g., graphics, sound, and network) and device firmware updated for optimal performance and security.

Use your operating system's update tools or download updates directly from the manufacturer.

Secure Your Mobile Devices

Android: Go to **Settings** → **System** → **System Updates** and check for updates.

iOS: Go to **Settings** → **General** → **Software Update**.

Stay Informed

- Follow tech news or subscribe to updates from your software providers to learn about critical patches or major updates.

Restart When Required

- Some updates require a restart to install fully. Don’t delay restarting to ensure your system is up to date.

Remove Unsupported Software

- Uninstall software that no longer receives updates or security patches.

Conclusion

- By consistently updating your software, you'll protect your devices from vulnerabilities and improve their overall performance and security.

Be Cautious with Email Attachments

Email attachments are a common way for hackers to spread malware, ransomware, and other threats. Here’s how to handle them safely:

Avoid opening email attachments or clicking on links from unknown or suspicious senders.

Verify unexpected emails from trusted contacts by contacting them directly.

- **1. Verify the Sender**
- Check the sender’s email address carefully for misspellings or odd domains.
- Be wary of emails from unknown senders or addresses that look suspicious.
- **2. Be Skeptical of Unexpected Attachments**
- Even if the email is from a known sender, confirm they sent it, especially if the email content is vague or the attachment was unexpected.
- Call or message the sender directly to verify.
- **3. Look for Warning Signs**
- **Red flags include:**
  - Urgency or threats, such as "Act now or your account will be closed."
  - Poor grammar, spelling mistakes, or unusual phrasing.
  - Generic greetings like "Dear Customer" instead of your name.

- **4. Avoid Clicking Directly**
- Don’t open attachments directly from the email.
- Download them and scan with antivirus software before opening.
- **5. Scan Attachments with Antivirus Software**
- Use your antivirus program to scan attachments for malware before opening them.
- Many email providers (e.g., Gmail, Outlook) automatically scan attachments, but manual scanning adds an extra layer of security.
- **6. Avoid Opening Certain File Types**
- Be cautious with executable files and macros, such as:
  - **.exe**, **.bat**, **.cmd**, **.js**, **.vbs**
  - **.docm**, **.xlsm** (documents with macros)
- Legitimate businesses rarely send executable files.

- **7. Preview Attachments Instead of Downloading**
- Many email services allow you to preview attachments online without downloading. This is safer than opening files directly.
- **8. Use Sandboxing Tools**
- Open suspicious attachments in a sandbox or virtual machine environment to prevent malware from affecting your main system.
- **9. Keep Your Email Provider Updated**
- Use a modern, secure email service (e.g., Gmail, Outlook) with built-in spam and phishing filters.

- 10. Enable Two-Factor Authentication (2FA)
    - Protect your email account with 2FA to prevent unauthorized access.
- 11. Educate Yourself About Phishing
    - Learn to recognize phishing scams where attackers disguise themselves as legitimate entities to trick you into opening malicious files.
- 12. What to Do If You Accidentally Open a Suspicious Attachment
    - Disconnect your device from the internet immediately.
    - Run a full antivirus scan.
    - Monitor your accounts for unusual activity.
    - Seek professional help if malware is detected.

By staying vigilant, you can minimize risks and protect yourself from email-borne threats.

Download Only from Trusted Sources

Download files and apps from official websites or reputable app stores.

Avoid using pirated or cracked software, as they often contain malware.

Tips for Downloading Only from Trusted Sources

- Downloading software, files, or apps from unverified sources can expose your device to malware, ransomware, and other security threats. Follow these tips to ensure safe downloads:

1. Stick to Official Websites

- Download software and apps only from the official website of the developer or manufacturer.
- Look for "https://" in the URL and verify that the domain matches the legitimate provider.

2. Use Reputable App Stores

- **For Mobile Devices:**
  - Android: Use the Google Play Store.
  - iOS: Use the Apple App Store.
- Avoid third-party app stores, as they often host compromised or fake apps.

3. Verify Digital Signatures

- Check if the software has a digital signature or certification.
- On Windows, right-click the installer, select **Properties**, and go to the **Digital Signatures** tab.

4. Research Before Downloading

- Look up reviews or feedback about the software or website.
- Check forums or trusted review sites like CNET, Trustpilot, or G2 for ratings.

5. Be Wary of Ads and Pop-Ups

- Avoid clicking on ads, pop-ups, or "Download Now" buttons that appear on unofficial websites.
- These often lead to malicious downloads or phishing attempts.

6. Avoid Torrents and Cracked Software

- Pirated or cracked software is a common source of malware.
- Use legitimate, licensed versions of software to stay secure.

7. Scan Downloads with Antivirus Software

- Before opening a downloaded file, scan it with antivirus software.
- Some antivirus programs allow you to scan files directly from your browser.

8. Check File Extensions

- Be cautious of file types commonly used to spread malware:
  - Executable files (**.exe**, **.bat**, **.cmd**).
  - Script files (**.js**, **.vbs**, **.ps1**).
  - Files disguised as documents (**.pdf.exe**, **.doc.scr**).
- Legitimate software should match expected file types.

9. Review Permissions

- Before installing an app or program, review the permissions it requests.
- Avoid apps that ask for excessive access unrelated to their function.

10. Use Secure Download Managers

- Consider using download managers like **Free Download Manager** or **Internet Download Manager** to ensure safe downloads and avoid corrupted files.

11. Check File Sizes

- Verify the file size against the size listed on the official website. Extremely small or unusually large files could indicate tampering.

12. Enable Browser Security Settings

- Use browsers with built-in security features that warn against unsafe downloads (e.g., Google Chrome, Microsoft Edge).

What to Do If You Suspect a Malicious File

- **Stop the Download Immediately.**
- **Run a Virus Scan.**
- Use your antivirus program to scan the file or your entire device.
- **Delete the File Safely.**
- If identified as unsafe, delete it permanently and clear your recycle bin.
- **Monitor Your Device.**
- Watch for unusual behavior like slow performance, unexpected pop-ups, or unauthorized activity.

By downloading only from trusted sources, you can minimize the risk of introducing harmful software to your device.

Use Strong Passwords

Use unique, strong passwords for each account, combining letters, numbers, and special characters.

Consider using a password manager to store and generate secure passwords.

How to Use Strong Passwords for Better Security

- Strong passwords are one of the most effective ways to protect your accounts and personal data from hackers. Here’s a guide to creating and managing strong passwords:
- **Characteristics of a Strong Password**
- **Length:** At least 12–16 characters.
- **Complexity:** Include a mix of:
  - Uppercase letters (A, B, C...)
  - Lowercase letters (a, b, c...)
  - Numbers (1, 2, 3...)
  - Special characters (!, @, #, $, etc.)
- Avoid common words, phrases, or predictable patterns like "password123."

Examples of Strong Passwords

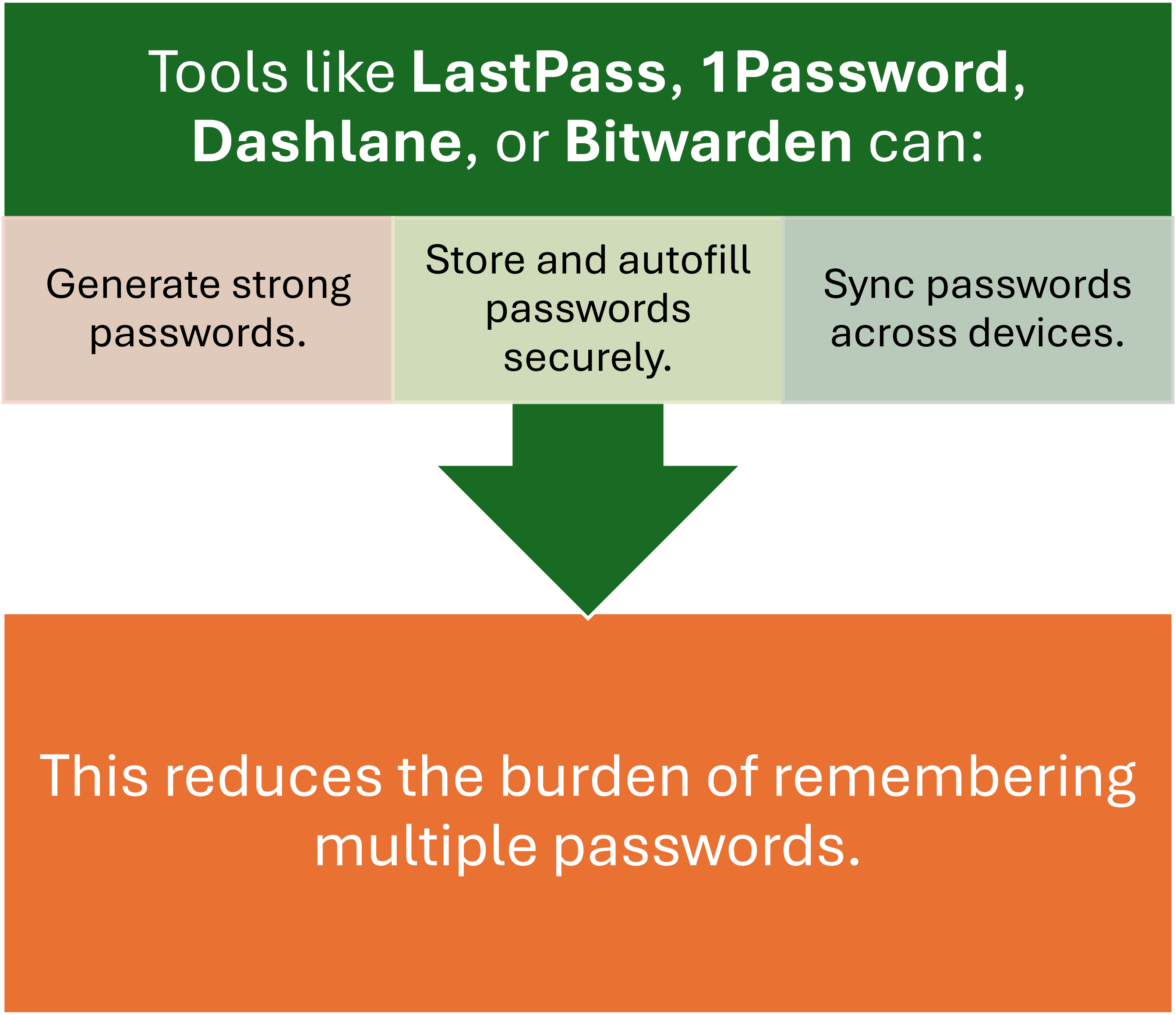
Random: 4Gv!q9R*pLz@6Tn&

Passphrase: OrangeElephant$Taco77!

Avoid These Common Mistakes

- Using personal information like names, birthdays, or pets' names.
- Reusing passwords across multiple accounts.
- Simple passwords like "123456," "qwerty," or "password."
- Sequential patterns or repeated characters (e.g., "abc123," "aaaaaa").

Use Password Managers



Tools like **LastPass**, **1Password**, **Dashlane**, or **Bitwarden** can:

Generate strong passwords.

Store and autofill passwords securely.

Sync passwords across devices.

This reduces the burden of remembering multiple passwords.

Change Passwords Periodically

Change passwords for critical accounts (e.g., banking, email) every 6–12 months.

Immediately update any password if you suspect a security breach.

Use Unique Passwords for Every Account

Never reuse passwords across multiple sites.

If one account is compromised, others won’t be at risk.

Secure Your Password Storage

If writing passwords down, store them in a secure location (e.g., a locked drawer or safe).

Avoid saving passwords in plaintext on your computer or phone.

Practice Good Password Hygiene

Log out of accounts on shared or public devices.

Avoid using browsers to remember passwords unless protected by a master password.

By using strong, unique passwords and leveraging tools like password managers and 2FA, you can significantly improve your online security.

Enable Two-Factor Authentication (2FA)

Add an extra layer of security to your accounts with 2FA.

Use authenticator apps or hardware keys instead of SMS where possible.

Avoid Public Wi-Fi

Public Wi-Fi networks, such as those in cafes, airports, or hotels, can expose you to cyber threats, including hacking, eavesdropping, and malware attacks. Here’s why you should avoid public Wi-Fi and how to stay safe when you must use it.

Use a Virtual Private Network (VPN) if you need to connect to public Wi-Fi.

Avoid accessing sensitive accounts, like banking or email, on public networks.

Risks of Public Wi-Fi

- Man-in-the-Middle (MITM) Attacks
- Hackers intercept data between your device and the network, gaining access to sensitive information like passwords and credit card details.
- Unsecured Networks
- Many public Wi-Fi networks lack encryption, making your data vulnerable to snooping.
- Rogue Hotspots
- Cybercriminals create fake Wi-Fi networks with names similar to legitimate ones, tricking users into connecting.
- Malware Distribution
- Hackers can exploit vulnerabilities to install malware or spyware on your device.

Tips to Stay Safe on Public Wi-Fi

- **1. Avoid Using Public Wi-Fi for Sensitive Activities**
- Avoid logging into online banking, email, or other accounts with personal information.
- Postpone online shopping or transactions until you’re on a secure network.
- **2. Use a Virtual Private Network (VPN)**
- A VPN encrypts your internet connection, protecting your data from hackers.
- Reputable VPN services: **NordVPN**, **ExpressVPN**, **ProtonVPN**, **Surfshark**.
- **3. Disable Automatic Connections**
- Turn off settings that automatically connect to available Wi-Fi networks.
- On your device:
  - **Windows:** Settings → Network & Internet → Wi-Fi → Manage known networks.
  - **Mac:** System Settings → Wi-Fi → Turn off "Ask to join networks."
- **4. Verify the Network**
- Confirm the exact network name with the establishment to avoid connecting to rogue hotspots.
- Avoid networks that don’t require a password.
- **5. Enable Firewall and Antivirus Protection**
- Ensure your device’s firewall is active.
- Keep your antivirus software updated to block potential threats.

Tips to Stay Safe on Public Wi-Fi

- **6. Use HTTPS Websites**
- Look for “https://” in the URL bar before entering sensitive information.
- Install browser extensions like **HTTPS Everywhere** to enforce secure connections.
- **7. Turn Off File Sharing and Airdrop**
- Disable file sharing to prevent unauthorized access.
    - **Windows:** Control Panel → Network and Sharing Center → Advanced sharing settings.
    - **Mac:** System Settings → Sharing → Turn off file sharing.
- **8. Use Your Mobile Network Instead**
- Use your smartphone’s cellular data or a personal hotspot when available.
- Ensure your hotspot is password-protected to prevent unauthorized access.
- **9. Log Out After Use**
- Log out of all accounts and disconnect from the Wi-Fi when you're done.
- Forget the network in your settings to prevent automatic reconnection.
- **10. Monitor Your Accounts**
- Regularly check your bank statements, credit cards, and online accounts for unauthorized activity after using public Wi-Fi.

What to Do If You Suspect a Breach

1. Disconnect from the network immediately.
2. Run a full antivirus and malware scan.
3. Change passwords for important accounts, starting with email and financial accounts.
4. Monitor for unusual activity or unauthorized logins.

- By avoiding public Wi-Fi or taking precautions when using it, you can significantly reduce your risk of falling victim to cyber threats.

Be Careful with Links

Links are a common method cybercriminals use to trick people into revealing personal information, installing malware, or falling for scams. Being cautious with links is essential for staying safe online. Here's how to handle links securely:

Hover over links to check their destination before clicking.

Avoid shortened or suspicious URLs.

Verify the Source

- Check the Sender: Only click links from trusted and verified sources.
- Be Wary of Unknown Contacts: Links from unknown senders or unexpected emails should raise suspicion.
- Watch for Spoofing: Cybercriminals may use email addresses that look legitimate but contain subtle changes (e.g., paypa1.com instead of paypal.com).

Hover Over the Link

- Preview the URL: Hover your mouse over the link (on desktop) or long-press (on mobile) to see the full URL.
- Look for Mismatches: Ensure the previewed URL matches the claimed destination.
- Watch for Shortened Links: Use tools like CheckShortURL to expand shortened URLs before clicking.

Look for Secure Connections

CHECK FOR HTTPS: ENSURE THE URL STARTS WITH HTTPS://, INDICATING A SECURE CONNECTION.

VERIFY THE PADLOCK ICON: CLICK THE PADLOCK IN THE BROWSER'S ADDRESS BAR TO SEE THE SECURITY CERTIFICATE DETAILS.

Avoid Clicking Links in Suspicious Emails or Messages

- Phishing Emails: Be cautious of links in emails claiming urgent actions, like account suspension or prizes.
- Unusual Greetings: Generic phrases like "Dear Customer" instead of your name may indicate phishing attempts.
- Spelling Errors: Poor grammar or misspellings in the email or link are red flags.

Avoid Clicking Links in Pop-Ups or Ads

Pop-ups and ads often contain links leading to malicious sites. Close them without interacting.

Use ad blockers to minimize exposure to malicious ads.

Avoid Links in Unsecured Messages

Be cautious with links shared in SMS, messaging apps, or social media, especially if they appear suspicious or unsolicited.

Scammers often use messaging platforms for phishing (e.g., "Your package is delayed, click here to track").

Watch Out for Typosquatting

Cybercriminals create fake websites with URLs that mimic legitimate ones by changing letters (e.g., amazonn.com instead of amazon.com).

✓ Double-check the spelling and ensure the domain matches the official site.

Avoid Download Links Without Verification

Do not download files from untrusted links or sources.

Links to executable files (.exe, .bat, .zip) may contain malware.

Use Technology to Help

Antivirus Software: Enable link protection features.

Email Filters: Use email services with strong spam filters to block suspicious messages.

Browser Security Settings: Use browsers with built-in phishing protection (e.g., Google Chrome, Microsoft Edge).

What to Do If You Clicked a Suspicious Link

- Disconnect from the Internet: This prevents further damage if malware is downloaded.
- Run a Security Scan: Use antivirus software to check for malware or viruses.
- Change Passwords: If the link led to a login page, change the password for that account immediately.
- Monitor Your Accounts: Watch for unusual activity in your bank accounts, email, or social media.
- Report the Link: Notify your email provider or the relevant platform about the suspicious link.

Monitor Permissions

Limit app and software permissions to only what's necessary for functionality.

Regularly review and adjust permissions on your devices.

Educate Yourself

Stay informed about common online scams, such as phishing, and learn how to recognize them.

Be skeptical of offers or messages that seem too good to be true.

Back Up Your Data

Regularly back up important files to an external drive or secure cloud storage.

This ensures you can recover data in case of a ransomware attack.

Conclusion

- Staying vigilant and proactive can help you avoid most online threats. If you suspect your device has been compromised, disconnect it from the internet, run a virus scan, and consult a professional if needed.