Wi-Fi & Home Network Security

CyberSafe
CYBERSAFE IN THE COMMUNITY

Why Secure Your Wi-Fi?

Central Gateway Role

Wi-Fi connects all your devices and serves as the main access point to your digital environment.

Risks of Unauthorized Access

Intruders can eavesdrop, steal data, or misuse your internet if your Wi-Fi is unsecured.

Proactive Security Measures

Changing passwords, enabling encryption, and monitoring devices strengthens your Wi-Fi security.

Protect Digital Privacy

Securing Wi-Fi protects personal data and prevents unauthorized bandwidth use.

Changing Default Router Credentials

Default Credentials Risk

Default router credentials are widely known and pose a security risk if not changed promptly.

Accessing Router Settings

Access the router setup page via a web browser using the IP address to change credentials.

Creating Strong Password

Use a long, unique password with letters, numbers, and symbols to secure your router.

Protecting Network Security

Changing default credentials protects your router’s configuration and network from unauthorized access.

Securing Wi-Fi Network Name and Password

Personalize Network Name

Avoid default SSIDs that reveal router brands; use unique names without personal info to enhance security.

Use Strong Wi-Fi Password

Set a strong, unique password with WPA2 or WPA3 encryption distinct from admin credentials.

Prevent Unauthorized Access

Treat your Wi-Fi password like a digital key and share only with trusted individuals to block intruders.

Using WPA2 or WPA3 Encryption

Importance of Encryption

Encryption protects data transmitted over Wi-Fi, preventing unauthorized access and eavesdropping.

WPA2 and WPA3 Standards

WPA2 is widely supported and secure, while WPA3 offers enhanced security features for modern routers.

Avoiding Outdated Encryption

WEP encryption is outdated and vulnerable, so it should not be used to protect your network.

Setting Strong Passwords

Setting a strong Wi-Fi password ensures only authorized users can connect to your network.

Disabling WPS and UPnP

Security Risks of WPS

WPS allows easy device connection but has known security vulnerabilities that risk unauthorized access.

Vulnerabilities in UPnP

UPnP automatically connects devices but can be exploited by malware to breach network security.

Disabling for Network Safety

Turning off WPS and UPnP enhances network protection and reduces risks of unauthorized intrusions.

Updating Router Firmware

Importance of Firmware Updates

Firmware updates fix security vulnerabilities and improve router performance, enhancing network security.

Methods to Update Firmware

Firmware can be updated via router admin interface or manufacturer's website for manual updates.

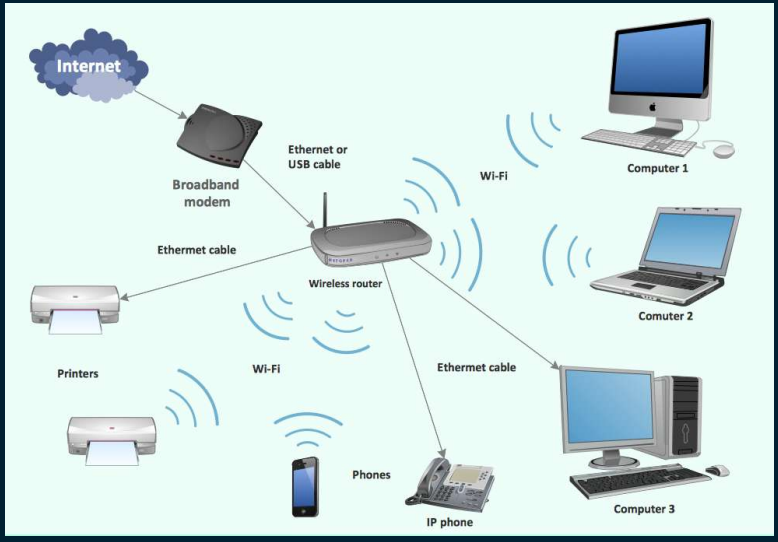
Automatic vs Manual Updates

Some routers update automatically; otherwise, set reminders to check updates at least twice yearly.

ISP-Provided Router Updates

If renting a router, ISPs (like Xfinity) may manage firmware updates; contact provider to confirm update process.

Monitoring Connected Devices



Identify Connected Devices

Check your router's device list regularly to recognize authorized devices like laptops and smartphones.

Detect Unauthorized Access

Unfamiliar devices on your network may indicate unauthorized access and potential security risks.

Secure Network by Password Change

Changing your Wi-Fi password disconnects all devices, allowing only trusted ones to reconnect.

CyberSafe
CYBERSAFE IN THE COMMUNITY

Using a Guest Network

Separate Guest Network

Guest networks provide internet access while protecting your main network and personal devices from visitors.

Password Management

Set a simple password for guests and update your main Wi-Fi password regularly to maintain security.

Access Restrictions

Guest networks restrict access to internal resources like computers and printers to keep your data safe.

Securing Smart Devices

Change Default Passwords

Always change default passwords on smart devices to prevent unauthorized access and improve security.

Keep Software Updated

Regularly update device software to patch vulnerabilities and enhance device functionality.

Secure Network Access

Use strong passwords and encryption on your network to safeguard smart devices from attackers.

CyberSafe
CYBERSAFE IN THE COMMUNITY

Caution with Public Wi-Fi

Risks of Public Wi-Fi

Public Wi-Fi networks are often insecure and shared passwords make data interception easier for attackers.

Avoid Plugging in to Public USB Chargers

These allow hackers to access your device directly

Avoid Sensitive Activities

Avoid online banking or shopping on public Wi-Fi to protect your sensitive personal information.

Use VPN or Secure Alternatives

Use a VPN to encrypt traffic or switch to cellular data or personal hotspot for safer internet access.

CyberSafe
CYBERSAFE IN THE COMMUNITY