UrCyberSecurity
EDUCATE. SECURE. THRIVE.

CYBERSECURITY AWARENESS

Your Digital Defense Guide

Essential practices every person should know

Cybersecurity is the practice of protecting your devices, data, and online activities from hackers, viruses, and digital threats. This guide covers the core habits that keep you and your organization safe.

CORE DEFENSE PRACTICES

Use Strong, Unique Passwords

WHY Weak or reused passwords make it easy for hackers to access multiple accounts at once.

TIP Create 12 to 16 character passwords mixing letters, numbers & symbols. Ex: **wFGWg)n3CEA4!**

+ Use a **password manager** you only need to remember one master password.

Enable Multi Factor Authentication (MFA)

WHY MFA adds a second lock even if your password is stolen, attackers can't get in.

TIP Enable MFA first on banking, email, and social media accounts.

+ An **authenticator app** (Google Authenticator, Authy) is more secure than SMS codes.

Keep Software Up to Date

WHY Updates patch security holes that hackers actively exploit in outdated software.

TIP Enable **automatic updates** on all devices, browsers, and apps.

+ Don't delay many attacks exploit vulnerabilities within days of public discovery.

Use a VPN on Public WiFi

WHY Public WiFi at cafes and airports is easy for attackers to monitor and intercept.

TIP A **VPN** encrypts your connection, hiding your activity from prying eyes.

+ Never access banking or sensitive accounts on public WiFi without a VPN active.

Install Antivirus Software

WHY Antivirus detects and removes malware before it can damage your system or steal data.

TIP Run scheduled weekly scans and keep virus definitions current.

+ Look for solutions with real time protection and web filtering built in.

Back Up Your Data Regularly

WHY Ransomware can lock all your files backups are your only recovery lifeline.

TIP Follow the **3 2 1 rule:** 3 copies, 2 different media types, 1 offsite/cloud.

+ Schedule automatic backups so you never have to think about it.

Secure Your Home WiFi Network

WHY An unsecured router lets neighbors or attackers access your entire network.

TIP Use a strong, unique WiFi password and enable **WPA3** encryption.

+ Disable remote admin access and change your router's default admin password.

Guard Your Personal Information

WHY Oversharing online fuels identity theft and targeted social engineering attacks.

TIP Review your social media privacy settings limit what strangers can see.

+ Never share your SSN, passwords, or financial info via email, phone, or text.

UrCyberSecurity
EDUCATE. SECURE. THRIVE.

CYBERSECURITY AWARENESS

Threats You Need to Recognize

Phishing, social engineering & AI powered attacks

Most cyberattacks start with deception, not technology. Attackers manipulate people into giving up access or information. Understanding these tactics including how AI is changing them is your strongest defense.

PHISHING AND SOCIAL ENGINEERING

Phishing Emails & Fake Websites

WHAT Fraudulent emails or sites impersonate trusted brands to steal your credentials or install malware.

⚑ FLAG Urgent language, misspellings, suspicious sender addresses, unexpected attachments or links.

TIP Hover over links before clicking. Navigate directly to websites don't click email links.

Spear Phishing and Targeted Scams

WHAT Personalized attacks using your name, role, or company info to appear far more convincing.

⚑ FLAG Emails referencing real details about you that request unusual actions or sensitive data.

TIP Verify any request for money or credentials via a **separate channel** call the person directly.

Voice & SMS Phishing (Vishing and Smishing)

WHAT Scammers call or text pretending to be your bank, the IRS, or tech support to extract personal info.

⚑ FLAG "Your account will be suspended!" or "You owe back taxes now!" high urgency, immediate action demanded.

TIP Hang up. Call back using the **official number** from the company's website never the number they gave you.

Pretexting and Impersonation

WHAT Attacker invents a false scenario fake IT support, new vendor to manipulate you into sharing access.

⚑ FLAG Unsolicited requests for passwords, system access, or sensitive documents even from apparent "coworkers."

TIP Verify identities through official channels. Legitimate IT staff **never** need your password.

AI POWERED THREATS

Deepfake Video and Audio Scams

WHAT AI can clone a person's voice or face in minutes used to fake emergency calls from "family" or fake executive instructions to wire money.

⚑ FLAG Urgent video or audio requesting money, credentials, or fast action even if the face or voice looks familiar.

TIP Establish a **family safe word** to verify real emergencies. Always call back on a known number.

AI Written Phishing and Chatbot Scams

WHAT AI generates flawless, personalized phishing emails and convincing fake chatbots nearly indistinguishable from real ones.

⚑ FLAG Perfect grammar no longer signals safety AI eliminates the old spelling error warning signs entirely.

TIP Focus on *what is being asked*, not how polished the message looks. Verify unusual requests independently.

QUICK REFERENCE KNOW THE TERMS

MALWARE
Malicious software designed to damage, disrupt, or gain unauthorized access to a system.

SOCIAL ENGINEERING
Psychological manipulation that tricks people into making security mistakes.

ZERO DAY
A software vulnerability unknown to the vendor, exploited before a patch is available.

RANSOMWARE
Malware that encrypts your files and demands payment to restore access.

MFA / 2FA
Requires a second proof of identity beyond your password to access an account.

VPN
Virtual Private Network encrypts your internet connection for privacy and security.

PHISHING
Deceptive emails or sites that trick you into giving up credentials or personal data.

DEEPFAKE
AI generated audio or video that realistically mimics a real person's voice or appearance.

ATTACK SURFACE
Every point where an attacker could try to enter or extract data from your environment.