NJ GMIS • EVERYDAY HOME CYBER SAFETY GUIDE

Personal Cybersecurity Tips & Tricks

Protecting Yourself, Your Family & Your Home Devices

Cyber hygiene doesn't end when you log off from work. Apply these essential, practical tips to secure your personal email, online banking, social media, and home Wi-Fi networks.

1 Personal Accounts & Password Hygiene

Adopt Passphrases Over Passwords

- **Length beats complexity:** Combine 4 or 5 random words into a memorable sentence (e.g., *BlueTiger$EatsPizza99!*).
- Easy for you to remember, virtually impossible for automated cracking scripts.
- Never reuse personal passwords across multiple critical accounts.

Enable 2FA On Everything

- Activate Two-Factor Authentication (2FA) on email, banking, and social media.
- Prefer **Authenticator Apps** (e.g., Google/Microsoft Authenticator) over SMS text codes.
- SMS messages can be intercepted via SIM-swapping or phone cloning fraud.

Use a Personal Password Manager

- Stop writing passwords on sticky notes or in phone memo apps.
- Use encrypted options like Bitwarden, 1Password, or Apple Keychain.
- Generates unique passwords for every site; requires remembering only one master key.

Check for Personal Data Breaches

- Check if your personal email or phone number was exposed in past corporate breaches.
- Visit trusted repository: **haveibeenpwned.com**.
- If flagged, update passwords immediately on affected services.

2 Mobile, Home Wi-Fi & Device Security

Secure Your Home Wi-Fi Router

- Change default admin credentials printed on the router sticker.
- Ensure encryption standard is set to WPA3 or WPA2-AES.
- Create a separate "**Guest Network**" for smart TVs, thermostats, and IoT devices.

Turn On Automatic Updates

- Outdated software is the #1 gateway for mobile malware.
- Enable auto-updates for iOS, Android, Windows, and macOS.
- Promptly update home smart cameras, web browsers, and anti-virus tools.

Public Wi-Fi & Charging Hazards

- Avoid logging into banking apps over open Wi-Fi at airports or cafes.
- Use cellular data hotspot or a personal VPN connection.
- Avoid public USB charging kiosks ("Juice

Smart Home & IoT Isolation

- Smart doorbells and cameras can be vulnerable entry points.
- Never leave default factory passwords on home cameras or baby monitors.
- Keep camera firmware updated via manufacturer

Personal Cyber Safety Guide (Cont.)

3 Spotting Personal Scams & Phishing Attempts

Smishing (Text Message Scams)

- Be skeptical of texts claiming "Unpaid Toll Balance (EZPass)", "Package Exception", or "Bank Fraud Alert".
- Never click links in unexpected text messages.
- Log into official websites directly via browser instead.

Grandparent & Urgent Family Scams

- AI voice cloning allows scammers to mimic relatives claiming emergency arrests or accidents.
- Establish a private **"Family Safe Word"** with children and seniors.
- Always hang up and call the family member back directly.

Marketplace & Payment App Fraud

- Treat Zelle, Venmo, and CashApp like physical cash—transfers are non-refundable.
- Refuse Marketplace buyers who offer overpayment via fake check or instant refunds.

Freeze Your Credit Reports

- The single best defense against personal identity theft.
- Prevents anyone from opening new credit cards or loans in your name.
- Freeze credit for free at all 3 bureaus: Experian, TransUnion, Equifax.

4 The 10-Minute Personal Cyber Audit Checklist

☐ Password Manager
Installed and master key backed up securely offline.

☐ 2FA App Configured
Enabled on primary personal email & banking accounts.

☐ Credit Freeze Set
Credit frozen across Experian, Equifax & TransUnion.

☐ Router Password
Default Wi-Fi router admin credentials updated.

☐ Guest Wi-Fi Network
Smart devices & TVs isolated on guest network.

☐ Auto-Updates On
Phone OS, laptops & tablets set to update automatically.

☐ Cloud Backup Active
Personal photos and documents backed up securely.

☐ Social Media Privacy
Profiles set to "Friends Only" to prevent impersonation.

☐ Family Safe Word
Agreed passphrase established for phone emergencies.

5 Where to Report Personal Cyber Fraud

If you fall victim to identity theft or financial fraud outside of work, immediately report it to:

- **Identity Theft Recovery:** IdentityTheft.gov (FTC Official Site)
- **Internet Crimes & Financial Fraud:** IC3.gov (FBI Internet Crime Complaint Center)
- **NJ Consumer Protection:** Contact your local police department and the NJ Division of Consumer Affairs.