PREVENTING CYBERCRIME

Essential Steps for Digital Safety

Protecting Yourself and Your Data in an Interconnected World

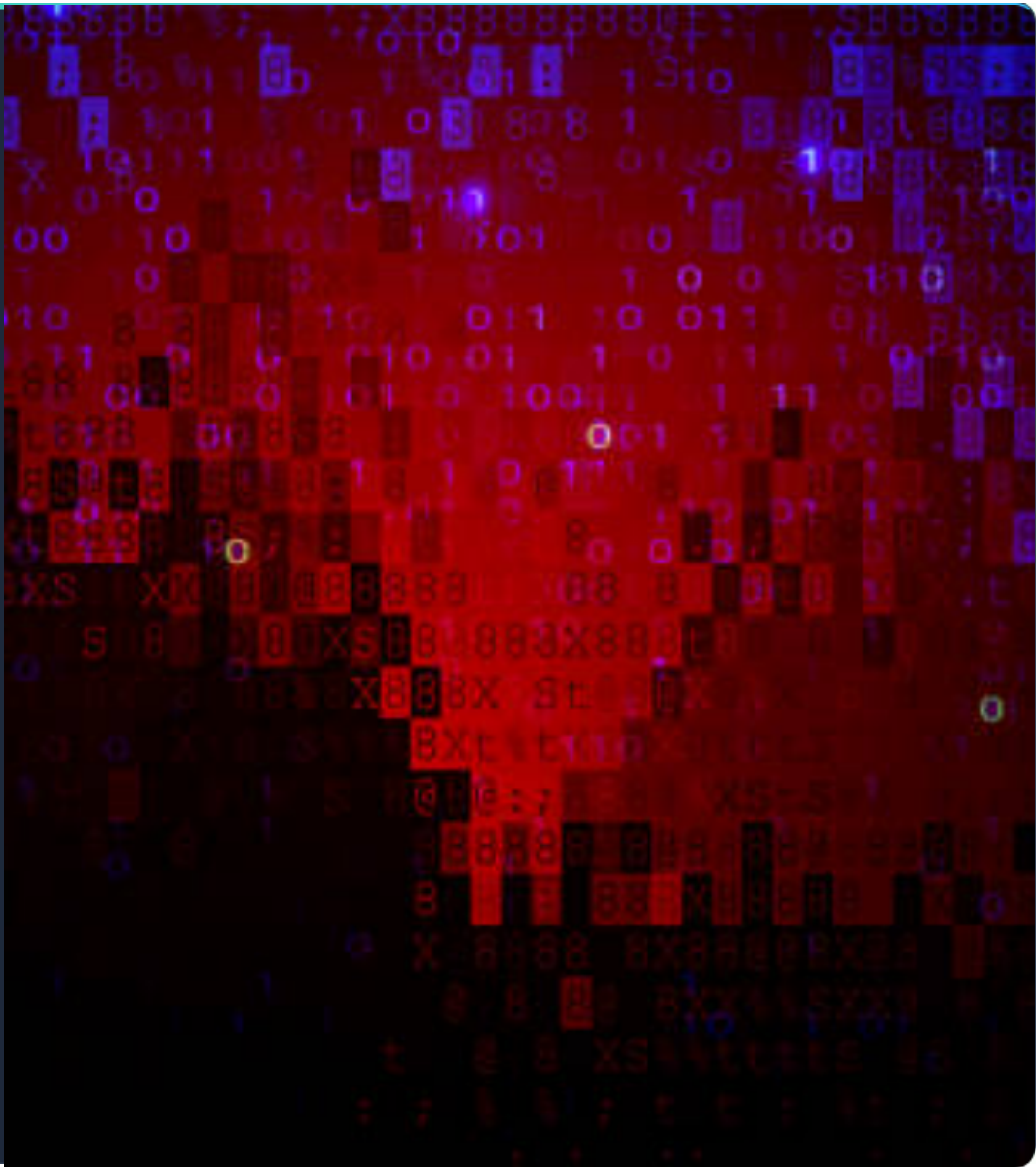
COMMON THREATS

⚠ **Social Engineering:**
The art of manipulating people into giving up confidential info (Phishing, Vishing).

⚠ **Malicious Code:**
Software designed to infiltrate or damage a computer system without consent (Malware, Viruses).

⚠ **Digital Extortion:**
Malicious software that blocks access to a computer system until a ransom is paid (Ransomware).

⚠ **Identity Theft:**
The fraudulent acquisition and use of a person's private identifying information for gain.

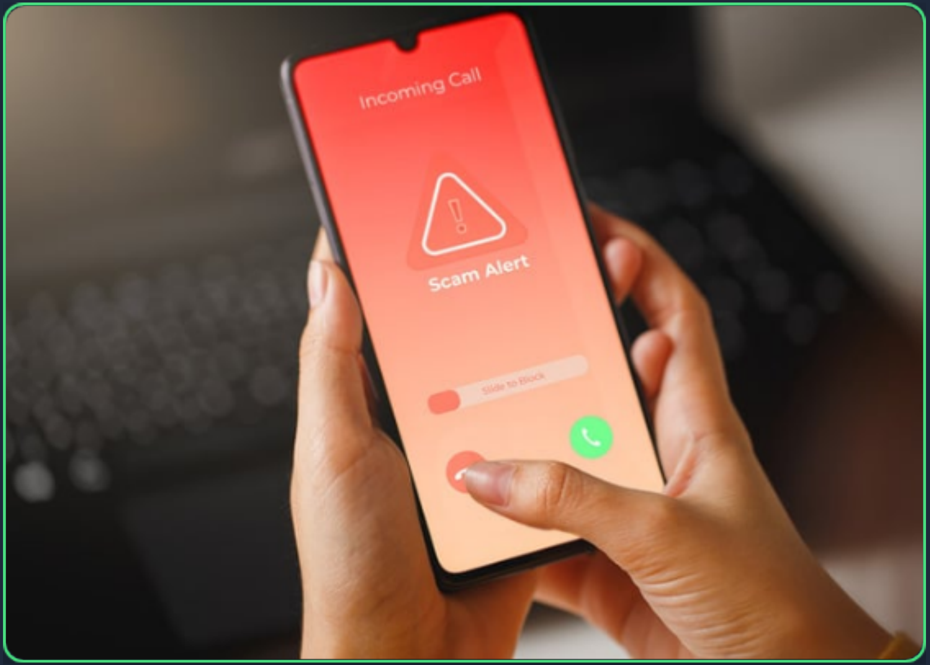


SOCIAL ENGINEERING TACTICS

- **The “Urgent” Message From A Family Member in Distress:** You receive an email from a family member (or on behalf of that person) demanding you buy gift cards or wire money immediately.
- **The Fake Support Call:** A caller claims your computer has a virus and asks for remote access to "fix" it.
- **Baiting:** A USB drive labeled "Payroll" or "Photos" is left in the parking lot to tempt curiosity.
- **Romance Scams:** A long-term online relationship that eventually asks for money for an "emergency."

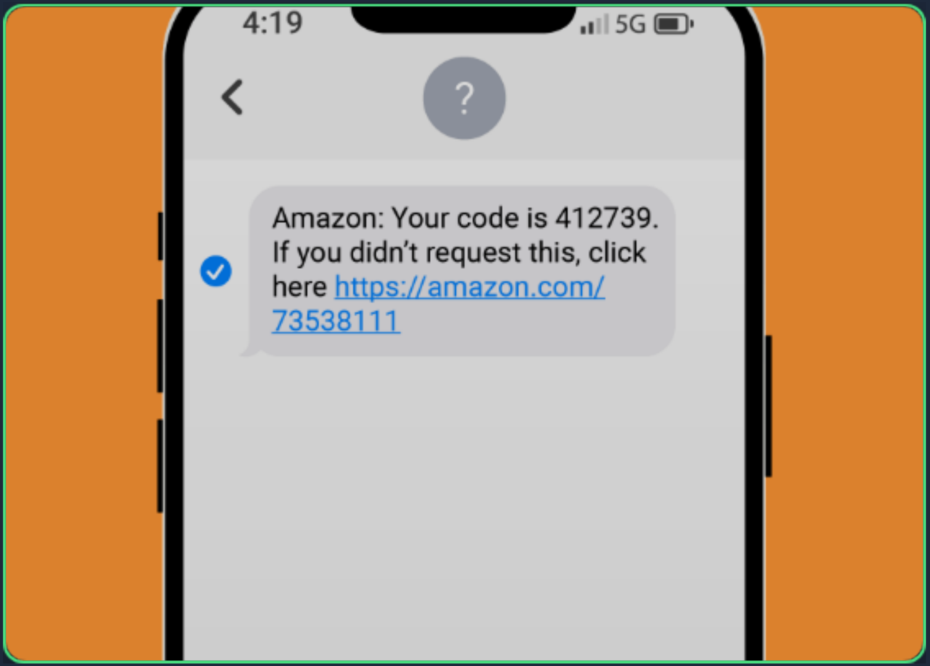
UNKNOWN CALLER? THE PROTOCOL

- **The Golden Rule:** Don't answer. Let it go to voicemail. 90% of scam calls will stop right here.
- **Don't Press Buttons:** If a robocall says "Press 1 to be removed," hang up. Pressing it just confirms your number is active.
- **Verify Independently:** If a voicemail claims urgent trouble (IRS, Amazon, Bank), never call that number back. Look up the official number yourself.
- **Automate Defense:** Use features like "Silence Unknown Callers" (iOS) or "Filter Spam Calls" (Android) to block the noise.



UNIDENTIFIED TEXT MESSAGE? DON'T ENGAGE.

- **The "Stop" Trap:** Don't reply, even to say "STOP". It only confirms your number is active and human-monitored.
- **The Link is Lava:** Never click links. They are the primary delivery method for malware and phishing sites.
- **Block & Report:** Use the platform's native tools (iMessage, WhatsApp, Messenger) to Block and "Report Junk" immediately.
- **Lock Down:** Adjust privacy settings to prevent non-contacts from adding you to groups or sending DMs.



Amazon: Your code is 412739. If you didn't request this, click here https://amazon.com/73538111

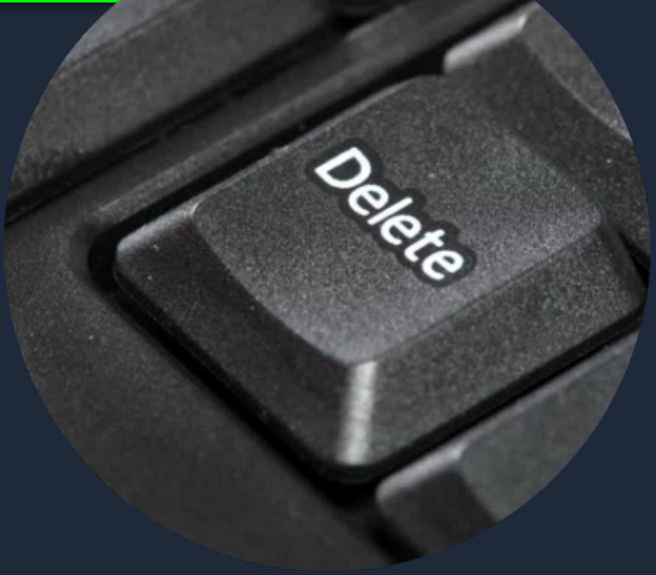
Typos & Wrong Numbers

A single typo can cost you your identity. Scammers count on your mistakes.

! **The URL Trap:** Typing amazn.com instead of amazon.com can land you on a perfect replica site designed to steal your login.

! **The Wrong Number:** Dialing a support line incorrectly can connect you directly to a scam call center that poses as your bank.

! **The Fix:** Slow down. Verify. Use Bookmarks.



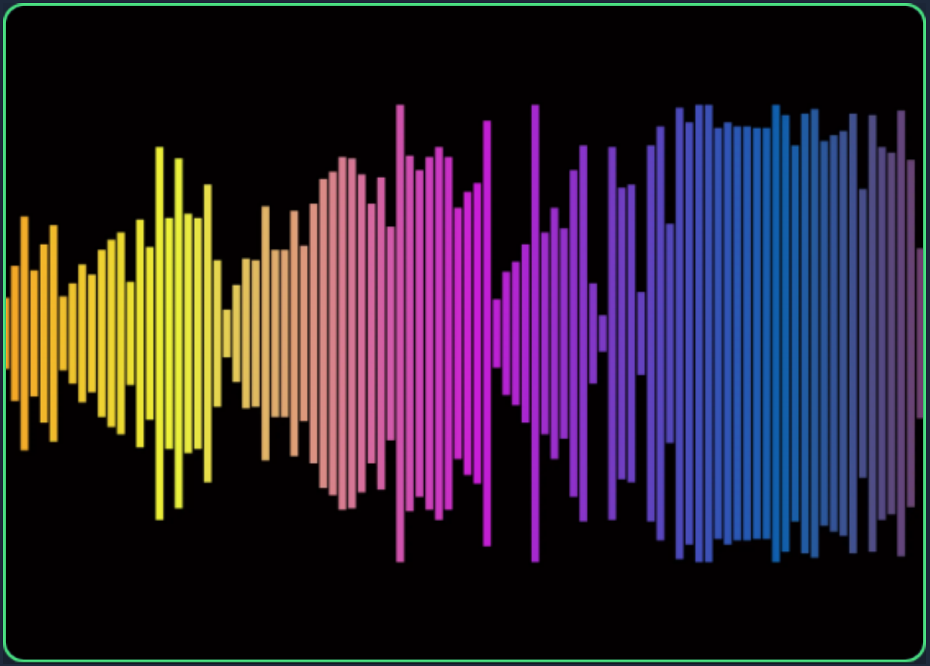
THE "SAY YES" TRAP & VOICE CLONING

THE TRAP: PHRASES THEY USE TO ELICIT THE DESIRED RESPONSE

- "Can you hear me?"
- "Is this [Your Name]?"
- "Are you the homeowner?"
- "Sorry, bad connection. Can you hear me now?"

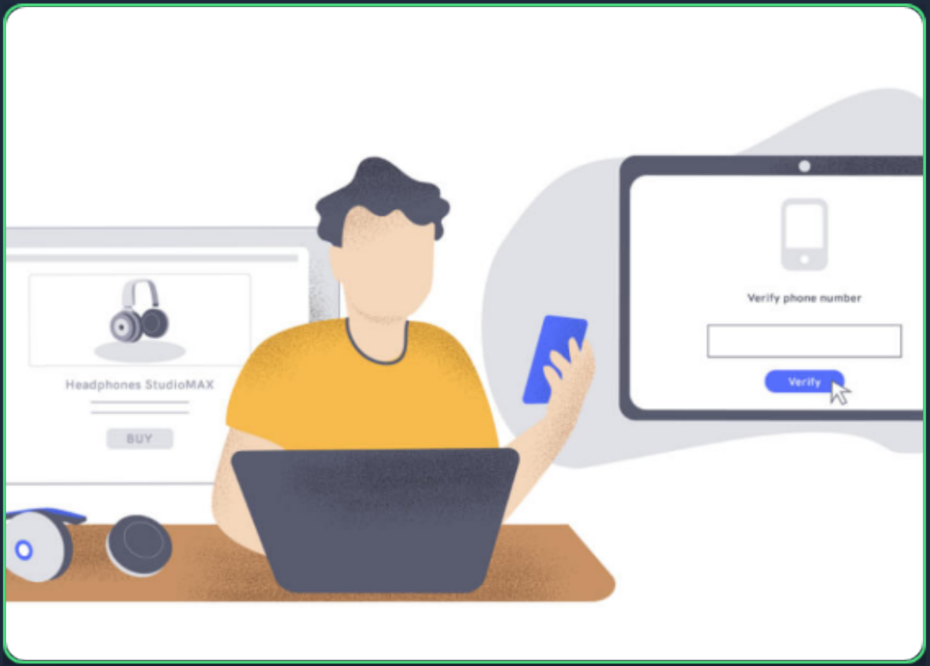
THE DEFENSE

Don't Answer. If you do, **stay silent** until they speak. If asked "Can you hear me?", **hang up** immediately or ask "Who is calling?". Never say "Yes".



DEFEATING AI IMPERSONATION

- **The "Safe Word":** Establish a unique code word (e.g., "Solar Flare" or "Blue Horizon") known only to your inner circle to confirm identity in a crisis.
- **Challenge Questions:** Ask about offline memories: "What color was the rental car in Hawaii?" or "What's the name of the stuffed dog on my bed?"
- **The "Call Back" Rule:** If a family member calls in "trouble" but sounds odd, hangs up and call their saved contact number immediately.
- **Trust No Voice:** AI can clone voices in seconds. If the request involves urgent money or secrecy, verify first.



VECTORS OF IDENTITY THEFT

DATA BREACHES

Corporate leaks expose millions of records, including SSNs and passwords, to the dark web.

PHISHING

Deceptive emails or texts trick you into revealing login credentials or financial details.

PHYSICAL THEFT

Dumpster diving for bank statements, or stealing mail and wallets to get physical IDs.

SKIMMING

Hidden devices on ATMs or gas pumps that steal magnetic strip data when you swipe.

PREVENTING ID THEFT: PROACTIVE MEASURES

- **Freeze Your Credit:** The #1 proactive step. It locks your credit report so no one can open new accounts in your name.

  Shred Everything: Don't just toss bank statements, pre-approved credit offers, or medical bills. Shred them to prevent dumpster diving.

- **Monitor Reports:** Check AnnualCreditReport.com (it's free) regularly for mystery accounts or inquiries.

- **Guard Personal Info:** Don't share your birthday, mother's maiden name, or pet names on social media. These are common security questions.

YOUR FIRST LINE OF DEFENSE

🔑STRONG PASSWORDS

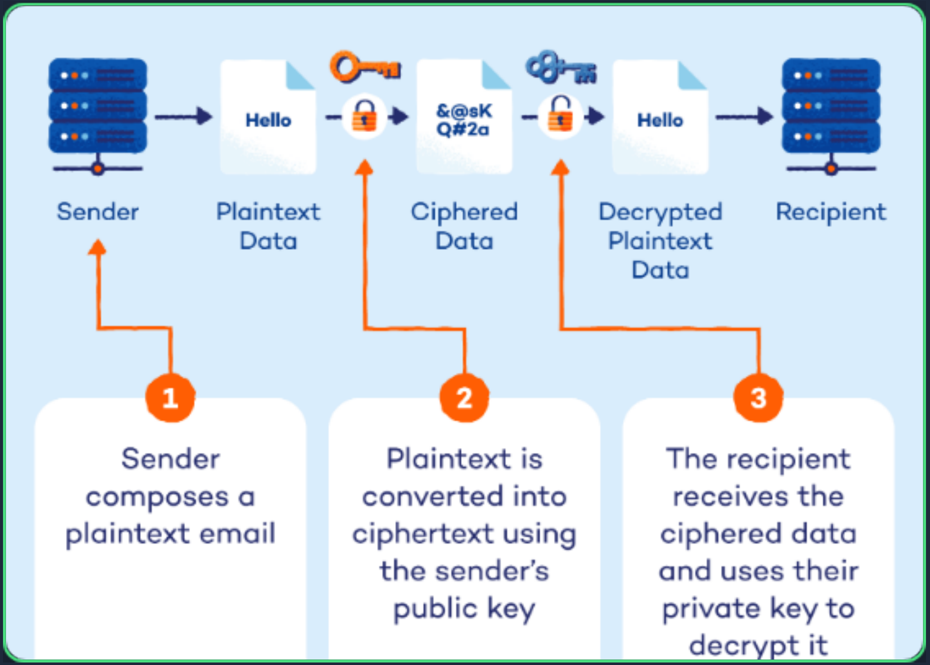
- Use a **Passphrase** (4+ random words).
- Minimum **12-14 characters**.
- **Unique** for every account.
- Use a **Password Manager** (e.g., 1Password, Bitwarden).

🛡MULTI-FACTOR AUTH (MFA)

- Requires two or more verification factors.
- **Factor 1:** Password (Knowledge).
- **Factor 2:** Code from App (Possession).
- **Action:** Enable on all financial & email accounts.

STRATEGIC EMAIL SEGMENTATION

- **The "Secret" Account:** Create a separate email address exclusively for financial and sensitive services.
- **Zero Exposure:** Never use this address for shopping, newsletters, or social media.
- **Breach Isolation:** If a retail site is hacked, your banking username remains unknown to criminals.
- **Obscurity:** Avoid using your real name in this address to prevent targeted guessing.



1 Sender composes a plaintext email

2 Plaintext is converted into ciphertext using the sender's public key

3 The recipient receives the ciphered data and uses their private key to decrypt it

SETTING UP MFA: A QUICK GUIDE

- **1. Get the App:** Download an authenticator app (e.g., Google Authenticator, Microsoft Authenticator) from your app store.
- **2. Find Settings:** Log in to your account, go to Security settings, and select "2-Step Verification" or "Turn on MFA".
- **3. Scan:** Select "Authenticator App" on your screen, then use the app on your phone to scan the displayed QR code.
- **4. Verify:** Enter the 6-digit code generated by the app into the website to confirm the setup.

DEVICE HYGIENE

UPDATES

Enable **automatic updates** for OS and apps. Patches fix vulnerabilities hackers exploit.

ANTIVIRUS

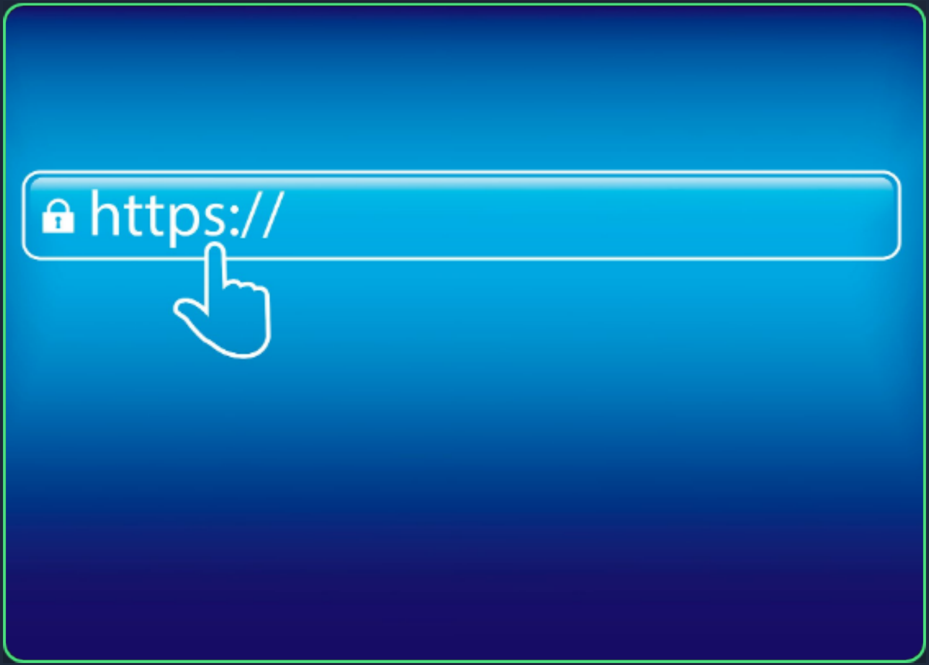
Ensure active protection is running and set to scan automatically.

BACKUPS

Follow the **3-2-1 Rule**: 3 copies, 2 media types, 1 offsite. The ultimate defense against ransomware.

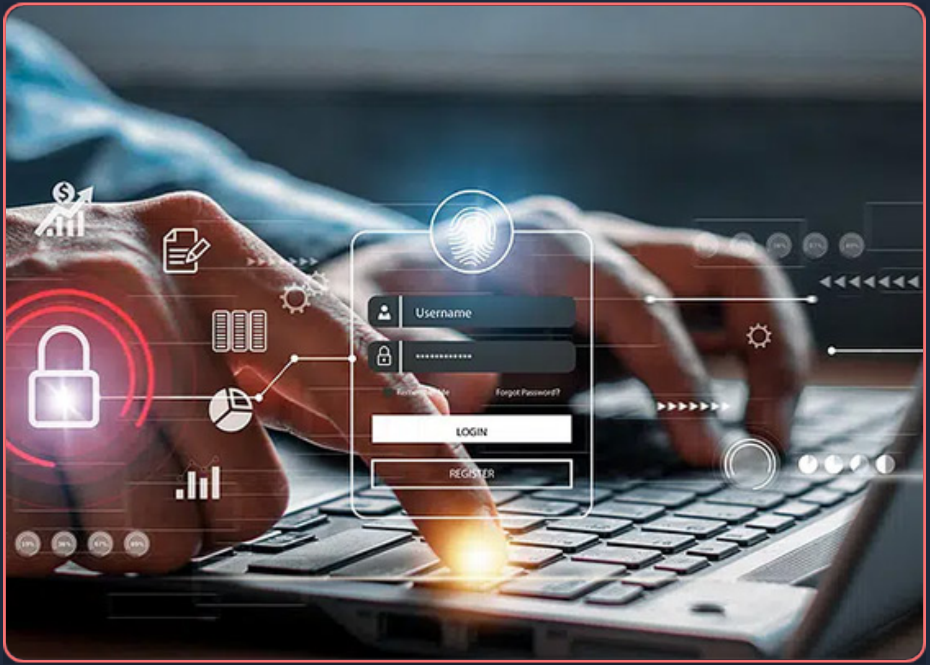
NETWORK & BROWSING

- **Router Security:** Change default admin passwords and use WPA3 encryption.
- **Check for HTTPS:** Ensure the "lock" icon is present before entering data.
- **Public Wi-Fi:** Avoid sensitive transactions or use a VPN to encrypt your traffic.
- **Be Skeptical:** Never click links in unsolicited communications.



CLICKED A BAD LINK? IMMEDIATE STEPS

- **Sever the Connection:** Immediately unplug the Ethernet cable or turn off Wi-Fi. This stops malware from "phoning home."
- **Close & Quit:** Force close the web browser immediately. Do not interact with pop-ups. Use Task Manager or Force Quit.
- **Credentials Check:** If you entered a password *after* clicking, treat it as stolen. Change it immediately from a *different*, safe device.
- **Scan for Intruders:** Run a full system antivirus scan (offline if possible) to catch any payloads that might have downloaded.



IDENTITY STOLEN? RECOVERY PLAN

- **Freeze Your Credit:** Immediately contact Equifax, Experian, and TransUnion to freeze your reports. This stops thieves from opening new accounts.
- **File an Official Report:** Visit IdentityTheft.gov to file an affidavit. This creates a recovery plan and is often required by banks to dispute fraud.
- **Alert Financial Institutions:** Contact the fraud departments of your banks and credit card issuers to close compromised accounts.
- **Audit Everything:** Review your credit reports for unauthorized inquiries and check all account statements for suspicious activity.

EMAIL COMPROMISED? ACT FAST.

Recover Access: Immediately change your password. If locked out, use the "Forgot Password" or recovery email options.

Crucial Step: Check **Forwarding Rules** & Filters. Hackers often auto-forward your bank alerts to "Trash" to hide their activity.

Secure Perimeter: Force "Sign out of all other sessions" in settings and reset your MFA.

Damage Control: Notify your contacts to ignore suspicious requests and check connected financial accounts.

LOCKED OUT? RECOVERY STEPS

🏁 **The Race:** Act immediately. Go to the official recovery page (e.g., g.co/recover) before the hacker changes your recovery options.

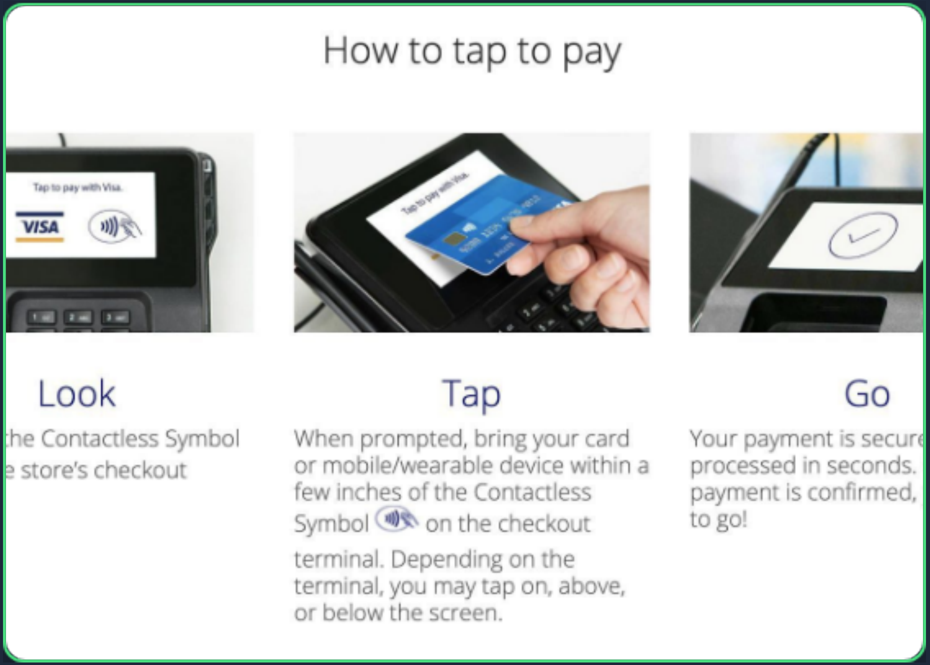
🏠 **Home Field Advantage:** Use a device (phone/laptop) and location (home Wi-Fi) where you usually sign in. This is a powerful identity signal.

The Backup Route: Select "Try another way" if primary options are changed. Answer security questions or verify previous passwords if prompted.

🏛 **The Fallout:** If recovery fails, contact support immediately and alert your bank to freeze assets.

FINANCIAL DEFENSE: SMART PAYMENTS

- **Credit > Debit:** Use Credit Cards for daily spend. They offer a legal buffer against fraud. If a debit card is hacked, your *actual* cash is gone.
- **Tap to Pay:** Use Contactless or Chip readers. Avoid swiping, which exposes your card's magnetic strip data to skimmers.
- **Instant Alerts:** Turn on SMS/Push notifications for every transaction over $1. Catch fraud in seconds, not weeks.
- **Virtual Cards:** Use disposable card numbers (e.g., Privacy.com, Apple Pay) for subscriptions to hide your real details.



How to tap to pay

Look

he Contactless Symbol
e store's checkout

Tap

When prompted, bring your card or mobile/wearable device within a few inches of the Contactless Symbol on the checkout terminal. Depending on the terminal, you may tap on, above, or below the screen.

Go

Your payment is secur
processed in seconds.
payment is confirmed,
to go!

THE "LOW BALANCE" FIREWALL

- **Separate Savings:** Keep the bulk of your money in a High-Yield Savings Account (HYSA) that has no debit card attached.
- **Daily Driver Limit:** Only keep 1-2 weeks of expenses in the checking account linked to your debit card.
- **Damage Control:** If your card is skimmed or stolen, criminals can only drain the small "daily" buffer, protecting your life savings.
- **Just-in-Time Funding:** Use your banking app to instantly transfer funds from savings *only* when you need to make a larger purchase.

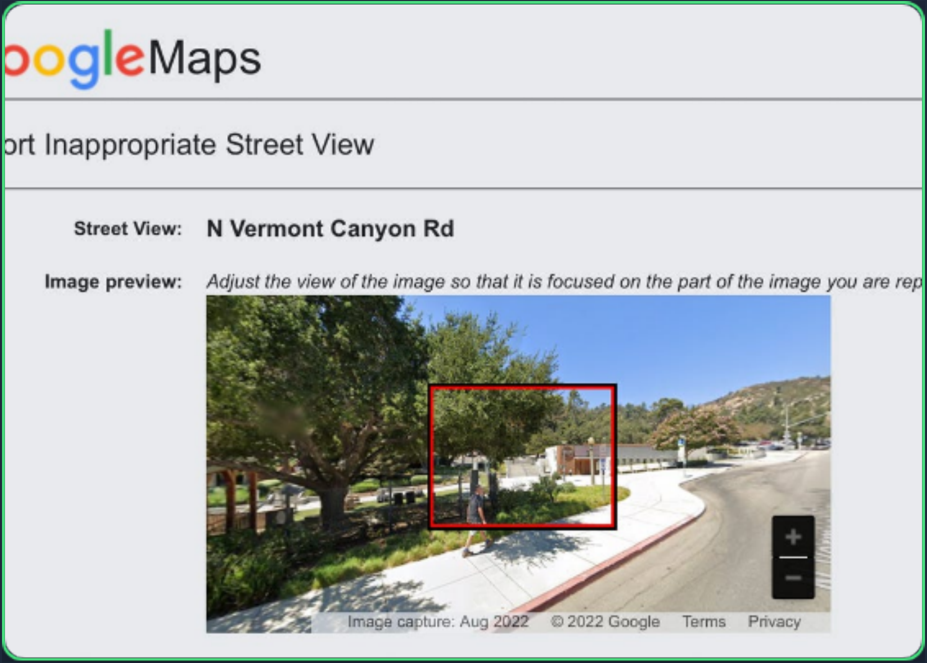
ANTI-SURVEILLANCE: HOME DEFENSE

Digital Camouflage: Request to **blur your home** on Google Street View, Apple Maps, and Bing. This hides entry points, windows, and assets from criminals casing neighborhoods online.

Social OpSec: Never post vacation photos in real-time. Post them *after* you return. "Checking in" at the airport is a beacon for an empty house.

Visible Deterrence: Install visible (not hidden) security cameras and motion-sensor lights. Criminals look for the path of least resistance.

Wi-Fi Anonymity: Rename your router to something generic (e.g., "Blue_Sky") rather than "Smith_Family_House" to prevent drive-by digital mapping.



oogleMaps

ort Inappropriate Street View

Street View: N Vermont Canyon Rd

Image preview: *Adjust the view of the image so that it is focused on the part of the image you are rep*

YOU ARE NOT ALONE

NATIONAL ELDER FRAUD HOTLINE

Call Toll-Free:
1-833-FRAUD-11
(1-833-372-8311)
The area code is 833 not 888. Dialing 888 connects you with a scam!

Hours of Operation:
Monday – Friday, 10:00 a.m. – 6:00 p.m. ET

Personalized Support:
Managed by the U.S. Department of Justice. Case managers provide personalized support for victims age 60+.

We Help You Report:
We will assist you in filing reports with the FBI and other agencies.

QUESTIONS?

Stay Safe & Secure.