Top five hacker movies

#1: **Hackers (1995)** - Stylized, neon, gleefully unrealistic, and a cult classic. Nails the rebellious subculture vibe and created memes galore. *"Hack the planet."*

#2: **Sneakers (1992)** - A heist caper about a ragtag team of security specialists who get pulled into a conspiracy involving a universal code-breaking box. Smart, funny, and surprisingly respectful of real cryptography and accurate social engineering. *"SETEC ASTRONOMY"*

#3: **WarGames (1983)** - A teenager dials into a military supercomputer and nearly triggers WWIII. It captured phone phreaking and hacking culture before most people knew what a modem was. *"Shall we play a game?"*

#4: **The Matrix (1999)** - Neo starts as a hacker and the film's aesthetic shaped how a generation pictured cyberspace. The movie begins with real-time network surveillance and call tracing. *"I know kung fu."*

#5: **Johnny Mnemonic (1995)** - A "mnemonic courier" with a cybernetic implant in his brain that lets him smuggle data. A virtual-reality cyberspace sequence and a dolphin that hacks encryption. *"I want room service!"*

Honorable mention: **Tron (1982)** - The original journey inside the computer, inspiring a generation of hackers, programmers, and cyberpunk dreamers. *"End of line."*

Bonus TV Series: **Mr. Robot (2015)** - The gold standard for realistic hacking depicted on screen. A brilliant but socially anxious cybersecurity engineer moonlights as a vigilante hacker before being recruited into an anarchist collective. *"Hello, friend."*

Volume 2 - June 2026

Personal Security

We live in a world drenched
in software and connectivity.

The modern digital age lets us do remarkable things, but the same tools have a dark side.

Hackers, scammers, and even governments exploit the vulnerabilities in our devices to drain accounts, steal identities, and watch what we do.

You need to take steps to defend yourself.

This volume of the Cruft Manor zine covers what you can do to protect yourself and your family.

"Hack the planet"

What Signal is and how to use it

Signal is a free, open-source messaging app with end-to-end encryption on by default, meaning only you and the people you message can read the contents - not Signal, your carrier, or anyone intercepting the traffic.

Install it from your app store and register with a phone number; you can then set a Signal PIN and a username so you don't need to share your number.

Use it for texts, voice/video calls, and group chats that you want to **keep private**.

Enable disappearing messages (open a conversation and set a timer) so messages auto-delete after a chosen interval.

You can verify a contact's "safety number" in person. Open a conversation with them, tap their name, choose "View Safety Number," and scan the QR code on their phone, which marks them as verified.

Signal collects minimal metadata and its protocol is widely audited, making it a standard recommendation for **private communication**.

Cruft Manor is published by Michael Pusateri
michael@pusateri.org
www.cruftbox.com
Bluesky: cruftbox.com

Updating your software

In today's hostile computing environment, it's important to keep your operating system and software updated.

If your phone wants to update, **do it**, don't wait.

If your laptop or desktop computer asks you to update, **click yes**, don't ignore it.

Most operating systems will update in the background, but not always promptly.

To update your operating system:

Mac - Open the Apple menu, choose System Settings, click General, then Software Update.

Windows 11 - Open Start, choose Settings, then click Windows Update and select Check for updates.

You can also update your software by opening a terminal window and entering a single command.

These commands will update the software you have on your computer.

OS	Command
Windows (Apps)	winget upgrade --all
macOS (Apps)	brew update && brew upgrade
Ubuntu / Debian	sudo apt update && sudo apt upgrade -y
Fedora	sudo dnf upgrade --refresh -y
Arch Linux	sudo pacman -Syu

How a VPN works

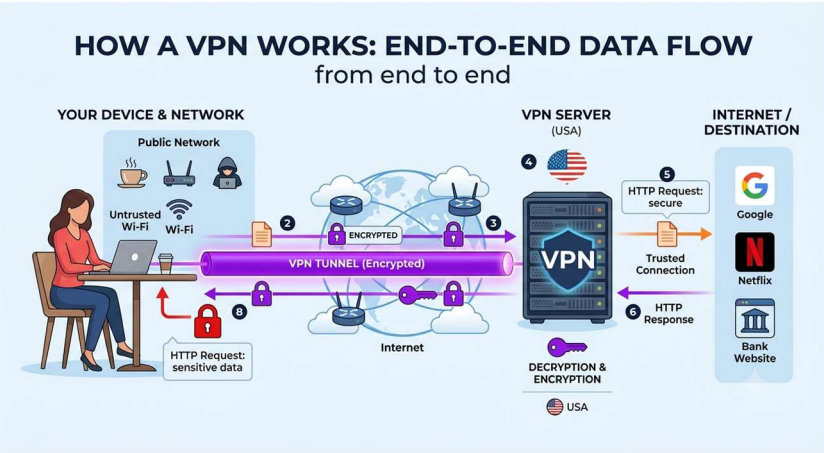
Using a VPN (Virtual Private Network) helps prevent your internet traffic from being monitored. A VPN creates an encrypted tunnel between your device and a server run by the VPN provider.

Rather than going straight to websites, your traffic travels through this tunnel first, so anyone watching your local network, be it public wifi, your ISP, or a nation state hacker, sees only encrypted data heading to the VPN server, not which sites you visit.

The site you reach sees the VPN server's IP address instead of yours, hiding your actual location.

HTTPS protects your interactions with a website, while a VPN prevents someone from seeing what sites you are visiting.

This defends against local eavesdropping, basic tracking, and lets you appear to browse from another location.



You can use VPN apps on your phone and your computer.

A VPN does not make you anonymous (logins, cookies, and browser fingerprints still identify you), but it is a good idea to use anytime you are not at home and using wifi.

Remember: a VPN provider itself can see your traffic, so a trustworthy company with a "no logs" policy is essential.

Code Words

Your family should agree on code words and phrases to communicate secretly, in ways others won't notice.

Talk it through on the phone, not over text, to choose words and phrases that work for your family.

Memorize and rehearse them. Never write them down. Don't keep a copy on your phone or online.

Bona fides - confirms someone's identity or that all is genuine/fine. Use a challenge and countersign so someone who overhears can't fake it. Challenge: "*How's grandpa?*" Correct reply: "*He still likes apple pie.*" A wrong or missing reply means something's off.

Duress - covertly signals you're being coerced while acting normal. Example: "*Things are peachy.*" It sounds like reassurance, but family knows it means "I'm being forced — play along, don't react, get help quietly." Receiver: stay normal, don't acknowledge, quietly call for help.

Distress - signals you need help or extraction now. Choose something that doesn't exist in your life so it can't happen by accident, like a pet you **don't** own. Text or say "*I forgot to feed the fish.*" It means "come get me immediately, no questions." Receiver: go to their location or call 911, don't ask questions.

Stand-down - cancels a false alarm. Pick one word (e.g., "*midnight*") so a mistaken signal can be called off cleanly.

Spotting scams

Scammers don't hack you, they trick you into helping.

The pitch is always the same: **urgency plus a link**. "Your package couldn't be delivered." "Suspicious sign-in, verify now." "Your bank account is locked."

Slow down. Urgency is the tell.

Check the link before you touch it. On a computer, hover over it and read the real domain in the corner of the screen. The text can say apple.com while the link goes to apple-secure-login.ru.

On a phone, press and hold to preview the address. If the domain isn't exactly right, it's fake.

Texts from a random number with a link are almost always a scam. Banks, the post office, and the DMV don't text you links to log in. Neither does the IRS.

If a message wants you to act in the next ten minutes, that pressure is the scam, not a coincidence.

Real companies never ask for your password, your 2FA code, or your full card number by email or text.

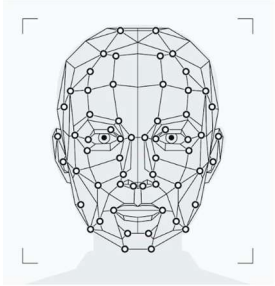
When something feels off, **don't reply and don't click**.

When in doubt, it's a scam. Costs nothing to ignore.

Locking your phone at a public gathering (turning off facial recognition)

Biometric unlocks like Face ID and fingerprint make life easy but can be used against you to invade your privacy.

Courts in the US generally treat a phone passcode differently from a fingerprint or face scan, because biometrics don't require your conscious cooperation, **authorities can legally compel you to unlock your phone using your face.**



Powering your phone off entirely is the strongest protection, since your data is fully encrypted at rest before the first unlock.

If you want to use your phone, before entering a protest or large crowd, you can switch to passcode-only mode.

But if you need to lock your phone quickly, without diving into settings menus, here is how to do it.

On iPhone, press and hold the side button plus a volume button until the power-off slider appears, then cancel. This disables Face ID until you re-enter your passcode.

On Android, hold the power button and tap "Lockdown" (enable it first under Settings > Security).

When either kind of phone is locked like this, it won't show notification content, maintaining your privacy.