Passwords, Passcodes, Passkeys – Oh My!

I'm a computer consultant, at least that is what it says on my Rotary name tag. You heard or read some of my Bio. The short story is that I really love computers and communications.

I listen to a weekly podcast by Steve Gibson called Security Now! and much of what I am presenting has been discussed at length on his podcast.

Today I'll provide an overview, a hopefully not too technical discussion of what you need to know about Cybersecurity. Whenever possible I'll use English!

I'll describe three things to START doing, one thing to STOP doing, and why now, this year — because of AI — everything is different. It is an amazing time to be alive; a sea change is occurring and it is bigger than many other changes we've experienced; Personal Computers was a big change in technology. The mouse with the graphical user interface was a game changer for useability of PCs. The Internet was a huge change as the World Wide Web changed our lives. The change we are going through in our shared computer history, will be viewed as a watershed moment in technology. It is a pleasure to share what we need to know as users because **what you don't know CAN hurt you**.

Why this matters right now

It is safe to say that Cybercrime now costs the world over a 1.2T a year. Cybersecurity Ventures, a research firm focused on the global cyber economy, estimates the number is closer $10.5T counting indirect costs like lost productivity from downtime and the cost of recovery.

June 2026 issue of The Atlantic, the article Assume You'll Be Hacked, is worth me quoting as it sums up the situation;

As AI tools have become extremely good at writing code, they've also become extremely good at pulling off cyberattacks. (Malware, after all, is still software.) The result has been a change in the scale, speed, and sophistication of hacks that is difficult to overstate: Among its tens of thousands of clients, the cybersecurity firm Palo Alto Networks identified a fourfold increase in daily attacks from 2024 to 2025. Hackers are developing AI-enhanced computer viruses that adapt on the fly to avoid detection. They are automating cyber-espionage campaigns on foreign governments. They are stealing data in minutes instead of hours. Alex Stamos, a former chief security officer of Yahoo and Facebook said, "There's a crazy amount of offensive activity happening right now. Companies are getting hacked every single day."

Good news: a handful changes of habits stops most of it.

The problem with passwords

Passwords fail three ways: reuse, weak choices, bulk theft.

The FortiBleed Campaign is a massive, global credential-theft and exposure campaign that targeted internet-facing Fortinet's FortiGate firewalls and SSL VPN gateways first exposed in June 2026.

Attackers verified working logins for 86,644 corporate firewalls in 194 countries. This was not a software bug — the attack was trying / testing reused passwords from old breaches on the Dark Web, automatically, continuously, 24/7!

None of those leaked credentials had a second factor enabled, which would have stopped their use by the hackers.

Banks, hospitals, government agencies are all falling prey to the criminals. If it happens to them, it will happen to us.

Fix #1 — Use a password manager

This is the fix for all three password problems at once. Please note the phishing-detector— your password manager fills passwords only when you are at the genuine domain. The URL must match what's in the password manager. I use and recommend Bitwarden, a free open source password

manager. Open source means the code is audited by many eyes as opposed to closed source proprietary software.

Clearly other great choices exist, and any password manager is better than the sticky notes or jumbled password sheets, password books, multiple passwords sheets or books, with jumbled passwords scratched out over and over. Oh my! I'm telling you what I see as a consultant is horrifying! I know computer users need help with this problem, and the Password Manager is the place to start. Apple Passwords (that's the name of the program that IS Apple's password manager. Google's Password Manager is built into the Chrome Browser. There's 1Password, and many others. Most important is that you must trust the password manager and remember one master password.

Fix #2 — Turn on two-factor authentication

Two-factor = something you know PLUS something you have.

Why avoid codes by SMS? The Small Message System is from the old days of Flip Phones and AOL Instant Messager. Worse, it is designed for our insecure phone communications equipment that can't be trusted to be secure!

As of April 2026, Microsoft is phasing out SMS for multi-factor auth and account recovery — They say it is 'a leading

source of fraud and the single most targeted vector for account takeover.'

Download one or more authenticator apps: Google Authenticator, Microsoft Authenticator, or OTP Auth on your mobile device. Schwab and Merrill Lynch are lagging behind the times and use Symantec's VIP Access because of heritage infrastructure, but under the hood it is based on the same time-based one-time password (TOTP) architecture as the other authenticator apps.

Fix #3 — Adopt passkeys wherever offered

Nothing to steal
Nothing to phish
Nothing to remember

Passkeys are the destination of our security journey. Simply: Passkeys are kind of like a Secrete Handshake; both sides know the handshake. Instead of a password which is a shared secret that the website stores, a passkey is a key pair — your device proves who you are without ever sending a secret that can be stolen or phished.

Passkeys are the future of signing in—simple, secure, and stress-free.

No typing, no guessing, no "forgot password" drama. With passkeys, you don't need to create and remember

passwords. Instead of typing a password, you use your phone or device to confirm it's really you.

A passkey is a digital credential that replaces passwords, allowing you to log into apps and websites using your device's biometrics (like Face ID or a fingerprint) or a screen unlock PIN. Note that the PIN is the weakest link! Maybe it is time to move from a 4 digit passcode to a 6 digit passcode. Mathematically, a 6-digit passcode is 100 times stronger than a 4-digit passcode.

Passkeys are significantly faster and more secure than traditional passwords and are highly resistant to phishing attacks

Microsoft is prompting all users to add passkeys as it retires SMS. The industry direction is clear.

The security ladder — where are you?

Who uses a password manager? Who has 2FA on their email? Who has a passkey anywhere? The goal is one step up the ladder this week.

"ClickFix" — the #1 trick on the internet today

ClickFix is 'the #1 means of tricking users into compromising their own PCs… it alone accounts for more than all other attack techniques combined. According to the Huntress

Cybersecurity Report: ClickFix was responsible for over 53% of all malware loader activity in 2025.

Why it works: it bypasses antivirus by making YOU the delivery mechanism.

Opera, a not well known web browser, just became the first browser to add 'Paste Protect' but Chrome/Edge/Safari users have no such shield yet, so it us up to **you** not to blindly copy and paste because you were told to.

AI just changed the game — for both sides

In April, engineers with NO security training used Anthropic's Mythos to find and exploit bugs. Thousands of high-severity vulnerabilities were discovered. These included a 27-year-old OpenBSD flaw. AI found a 21-year-old critical FreeBSD bug. Mozilla used Mythos to fix 400+ Firefox bugs in April — ~20x their normal. Moody's report shows exploit time fell from 700 days (2020) to 44 days (2025). Governments are worried — the US even had public access to Mythos banned pending guard rails. I'm worried!

The result: a tsunami of updates. Ride it.

Updates aren't an annoyance — they're the defense working.

Did your computer reboot this week? Microsoft's July 2026 Patch Tuesday (7/14/2026) released 570 security updates (covering 622 total CVEs if counting earlier July releases),

breaking all previous records as the largest Patch Tuesday in history. Historical Baseline: A typical Microsoft Patch Tuesday generally addresses between 60 and 130 vulnerabilities. Anything above 150 is traditionally considered unusually large. The AI Factor: Microsoft attributed this massive surge to their new multi-model agentic scanning harness (MDASH), an AI system utilizing over 100 specialized agents to locate software bugs much faster.

Have you heard of CISA? Cybersecurity and Infrastructure Security Agency- that’s the nation's principal cyber defense agency and the national coordinator for critical infrastructure security. Let’s hope they are well funded! Anyway…

CISA confirmed that ransomware gangs exploiting the 'BlueHammer' Windows Defender flaw — which was patched April 14 and is still being exploited in July. CISA now requires federal agencies to patch on much shorter timelines because AI shrank the window. Same logic applies to us at home.

If it can’t be updated, replace it – now

The FCC extended waivers so consumer routers can keep receiving updates, even if from China, precisely because router updates matter. Speaking of routers and networking

gear, 100,000+ exposed UniFi devices were attacked within days of a flaw's disclosure. I use UniFi and YES I had auto updates on.

Microsoft is extending the free Extended Security Updates (ESU) another year (into 2027) because so many people refuse to move to 11. My advice if you are on Windows 10, enroll in the ESU and plan to move to a new computer. One way to do that is use Windows Backup and OneDrive. URGENT: We all (myself included) need to prioritize our personal cybersecurity now BEFORE the cheap criminal AI tools arrive in the hands of the criminals.

Your checklist – start this week

Install a password manager
Turn on 2FA – app, not SMS
Say yes to passkeys
Never blindly paste what you don’t understand
    Ctrl-C/Windows Key-R/Ctrl-V
    Cmd-C/Open Terminal/Cmd-V
Let everything auto-update
Retire what can’t be updated

“What you don’t know can hurt you”

Now you know!

All of us hesitate to change our daily habits. I hope today’s presentation provides a bit of a nudge to improve those habits that will hurt you.

I credit Steve Gibson's Security Now podcast as the source of much of today's material. I encourage you to check out GRC.com.

Also included is a link to haveibeenpwned.com to see if your email address has been compromised.

There is so much we could have discussed about cybersecurity. I leave you with this list of local banks and their security and fraud resources.

I suspect you may have questions.