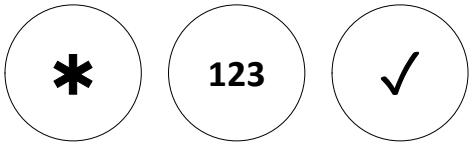


Passwords, Passcodes, Passkeys – Oh My!

Practical cybersecurity for home users and small businesses

Lee Lasson • July 16, 2026

Why this matters right now

$1.2+ trillion

estimated global cost of cybercrime in 2025 — and rising

"Assume You Will Be Hacked"
— The Atlantic, June 2026

4×	increase in daily attacks seen by Palo Alto Networks, 2024 → 2025
Everyone	hospitals, banks, utilities, schools — and small businesses
Why now?	AI writes code — and malware is software. Attacks are faster, cheaper, and far more convincing

The problem with passwords

We reuse them

One leaked password unlocks your email, bank, and business accounts. Criminals try leaked passwords everywhere — automatically, around the clock.

We pick guessable ones

Pets, birthdays, "Password123!" — cracking software tries billions of guesses per second.

They get stolen in bulk

Breaches you never hear about leak your passwords. They're sold and traded for years.

86,644

company firewalls worldwide broken into this year — using nothing but reused and never-changed passwords. Not one had a second factor in the way.

"FortiBleed" campaign, June 2026

Fix #1 — Use a password manager

1 **One strong, unique, random password for every site — and you only remember one.**

It remembers, so you don't

Generates and fills long random passwords. A breach at one site can't follow you anywhere else.

It's a phishing detector

It only fills passwords on the REAL site. On a fake look-alike site it stays silent — that silence is a warning.

Trusted choices

Bitwarden (free, excellent), 1Password, or the built-in Apple / Google managers. A manager beats everything else.

Fix #2 — Turn on two-factor authentication

A password is something you know.
Add something you have: a 6-digit code that changes every 30 seconds.

✓ Do this

- Use an authenticator app: Google Authenticator, Microsoft Authenticator, or OTP Auth.
- Start with the accounts that matter most: email, bank, anything with your money or your name.
- A stolen password alone is now useless to the thief.

✗ Avoid codes by text message

Texted codes can be intercepted and phone numbers hijacked. Microsoft calls SMS “the single most targeted vector for account takeover” — and is retiring it entirely this year in favor of passkeys.

Fix #3 — Adopt passkeys wherever offered

A passkey is a cryptographic key stored on YOUR device, unlocked with your fingerprint, face, or PIN.

Nothing to steal

The website never holds your secret — a data breach there can't leak a password you don't have.

Nothing to phish

A passkey only works on the genuine site. A fake site gets nothing. It cannot be tricked out of you.

Nothing to remember

Faster than typing a password and waiting for a code. Sign in with a touch or a glance.

Already offered by Google, Apple, Microsoft, Amazon, banks, and more. Microsoft now prompts every user to add one. When a site offers a passkey — say yes.

How Passkeys Work

Passkeys rely on a technology called public key cryptography and utilize the industry standard known as WebAuthn. Here is the step-by-step process of how they operate:

1. **The Key Pair:** When you set up a passkey for a website or app, your device generates two unique, linked keys: a **public key** and a **private key**.
2. **Key Storage:** The public key is sent to the website's server. The private key stays locked securely on your device (in your phone's secure enclave or a password manager) and is never shared.
3. **Authentication:** When you want to log in, the website sends a digital "challenge". Your device receives this challenge, verifies it's you via your fingerprint or face, and signs it using your private key. It then sends the signed response back to the website.

Verification: The website uses the public key it has on file to check the signature. If it matches, you are instantly logged in.

The security ladder — where are you?

RISKY

Password only

One leak or one guess and you're done. This is where most people still are.

GOOD

Password + app code

Stops nearly all remote break-ins. Do this everywhere, today.

BEST

Passkey

Phishing-proof by design. Adopt it as sites offer it.

Each step up removes an entire category of attack.

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

53%

of ALL malware-delivery activity in 2025 came from this one trick — more than every other attack technique combined.

Source: Huntress report, via Security Now #1086

1. **A pop-up interrupts you**
   A fake "verify you're human," "fix this error," or "update" box appears on a website or in email.

2. **It asks you to copy & paste**
   "Press Windows+R, then Ctrl+V, then Enter." The page has silently loaded a malicious command into your clipboard.

3. **You infect your own PC**
   That pasted command downloads malware. No virus needed — you typed it in yourself, past every defense.

THE RULE: Never paste anything into your computer that you did not write and do not understand.

AI just changed the game — for both sides

New AI systems — Anthropic's Mythos, Microsoft's MDASH, OpenAI's Daybreak — now find software flaws automatically. Thousands of them, some hidden for decades.

27 years

age of a flaw AI found in OpenBSD — software famous for its security. It found a 21-year-old critical bug in FreeBSD, too.

400 bugs

fixed in Firefox in a single month using AI — about 20× the normal rate.

700 → 44 days

time for criminals to exploit a newly disclosed flaw, 2020 vs. 2025. AI is collapsing it further.

Defenders have these tools first. Criminals are next — free copycat AI tools are already circulating.

The result: a tsunami of updates. Ride it.

↻

Noticed your phone, browser, and apps updating constantly?
That's AI finding and fixing decades of buried flaws.

Every update is a patched hole

And every published fix is also a road-map: criminals use AI to build attacks on the not-yet-updated within days.

Turn on automatic updates

Windows, Mac, phone, browser, apps — let them update themselves. Restart when asked. Don't snooze it for weeks.

Waiting is the risk

Ransomware gangs are exploiting a Windows flaw patched back in April — today. Only the un-updated are victims.

If it can't be updated, replace it – NOW!

!

AI is finding old flaws in old products.
If the maker no longer fixes them,
every newly found flaw stays open forever.

Old routers & Wi-Fi gear

The #1 forgotten device. If yours no longer gets firmware updates, it's a permanently open door. Check the model's support status — or replace it.

Out-of-support computers

Windows 10 got a reprieve — free security updates now run into 2027. Enroll, and plan your move before support truly ends.

Smart gadgets & old apps

Cameras, doorbells, storage boxes, ancient software: no updates = retire it, or wall it off from anything that matters.

Your security checklist — start this week!

Install a password manager

Bitwarden, 1Password, or Apple/Google built-ins. Fix your worst reused passwords first.

Turn on 2FA — app, not SMS

Email and bank first. Then everything with money or your identity.

Say yes to passkeys

Whenever a site offers one. Start with Google, Apple, or Microsoft.

Never blindly paste what you don't understand

No legitimate site EVER asks you to press Windows+R and paste. That's ClickFix — walk away.

Let everything auto-update

Computers, phones, browsers, apps. Restart when asked.

Retire what can't be updated

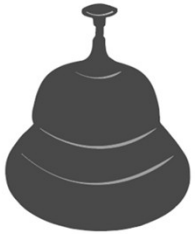
Old routers, out-of-support PCs, abandoned gadgets.

"What you don't know <u>can</u> hurt you. Now you know."

Learn more

Security Now! podcast — Steve Gibson & Leo Laporte (twit.tv/sn)
GRC.com — free security tools and research
HaveIBeenPwned.com — see if your accounts have been breached
Bank of Estes Park https://www.bankofestespark.com/security/fraud-awareness/
Meritrust Credit Union https://colorado.meritrust.org/support/security-fraud/
Bank of Colorado https://www.bankofcolorado.com/personal-banking/cybersecurity-for-consumers
U.S. Bank https://www.usbank.com/customer-service/online-security.html
KeyBank https://www.key.com/about/security/privacy-security.html

Questions?
Need technical assistance?



FrontDesk, Inc.
CREATIVE & TECHNICAL SERVICES

Lee Lasson	lee@frontdesk.com
Windows & Mac	O: 970.586.4760
Networking Services	C: 970.227.8915
Onsite & On-line	frontdesk.com