Passwords Made Simple

Protecting Your Accounts

Adults aged 60 to 75 typically maintain between 10 and 25 active online accounts. These usually include a primary email, at least one bank or credit card account, a health portal for appointments and prescriptions, utility accounts such as electricity, gas, water, and internet, as well as shopping and social media profiles. Many also have logins for streaming services, pharmacy refills, travel websites, or sites related to their hobbies or news interests.

Managing this many accounts can sometimes result in weak passwords and errors, but **what are the most common mistakes people make with their online accounts?** We have categorized them based on relevance.

➲ Authentication and Password Management

- Using the same password on multiple sites — if one site is hacked, all other accounts using that password could be compromised.
- Choosing short, common, or easily guessed passwords (e.g., "password123", "qwerty", birthdates).
- Keeping passwords in insecure places like notes, photos, or plain-text files.

➲ Recovery Info and Over-sharing Personal Details

- Having recovery email addresses or phone numbers that one no longer controls, or forgetting to update them after changes.
- Having personal details available publicly (mother's maiden name, pet names, school names) that are used for account resets.

➲ Two-factor Authentication and Security Layers

- Relying solely on a password for high-risk accounts (e.g., email, banking, healthcare, or government services).
- Using only text messages as an additional verification method for account access.

➲ Everyday Threats and Unsecure Habits

- Responding to unexpected emails, texts, or messages that ask for passwords, verification codes, or personal details.
- Granting excessive app permissions or using third-party logins carelessly, signing into a new app with Google or Facebook to avoid creating a separate account.
- Not using a screen lock or PIN on phones and computers, or leaving devices unattended while signed in.
- Forgetting to sign out on shared devices or public computers.

The challenges we've just covered all concern how we verify our online identity. The techniques used to confirm your online identity are known as **"authentication methods,"** and we'll examine what they are, what each entails, and how to utilize them to secure your accounts.

Types of Authentication Methods

Instead of relying solely on a complex, hard-to-remember password, different authentication methods introduce a variety of additional protective layers. This allows for simpler, more memorable passwords since they are no longer the sole safeguard. With these extra security measures operating behind the scenes, you benefit from improved protection and a more seamless experience — even if your password isn't flawless.

Passwords

What are they: A secret string of letters, numbers, and symbols you type to sign in to an account.

How to use them: Create a unique, strong password for each account. Steer clear of common words, simple patterns, and obvious substitutions.

When to choose: Use a password for all online accounts (email, banking, social media, shopping, cloud), particularly when the service doesn't provide stronger sign-in methods (passkeys).

The primary risk involves passwords being stolen or guessed. Attackers might acquire them through phishing, crack weak or simple passwords, or exploit reused passwords across different sites, leading to unauthorized access to multiple accounts.

Best Practices

- Use a passphrase — choose three to five common words that usually don't go together and link them into one. They're easier to remember and more secure than short passwords. **Example:** BlueTrainMapleRocket.
- Prioritize length over including unusual symbols. Aim for at least 12 characters; 16 or more is preferable. **Example:**
  - **(12+):** sunflowerpaper9
  - **(16+):** honestmountainbicycle7
- Convert a sentence into a password — take the first letters of a memorable sentence, then add a number or punctuation.
  - **Example sentence:** I have tea at 4 pm every day!
  - **Password:** Ihta4ped!

PINs or Personal Identification Numbers

What are they: A short numeric code (usually 4–8 digits) used to unlock a device or confirm identity on that device.

How to use them: Choose a PIN that you can remember but others won't easily guess (avoid reused common combos, like 0000). Set that PIN only on the specific device—your phone, tablet, or laptop.

When to choose: Opt for this method when you want a simple, device-only unlocking option for your phone, tablet, or laptop, or as a dependable backup if biometric methods —fingerprint or face recognition, or passkeys—fail to work.

Main risk: A PIN can be easily observed or guessed through shoulder surfing or obvious choices like 1111. It can also be obtained if someone has physical access to your device. Because a PIN is device-specific and often short, it provides less security if it becomes exposed.

Best Practices

- Avoid common patterns like ascending (123…) or descending (432…) sequences, personal dates, birthdays (MMDD), birth years (YYYY), and the last four digits of phone numbers.
- Use a longer PIN if your device permits it (6 or more digits are more secure than 4).
- Never share your PIN or write it where others can easily see or access it. Change your PIN immediately if you suspect someone has seen it.
- Activate the device's lockout features so it automatically locks after inactivity.

One-Time Passwords (OTPs) and Authenticator Codes

What are they: Short six-digit codes used once, which expire quickly and serve as a second verification step after your password. The service you're signing into can send the code via text or email, or an **"authenticator"** app on your phone can generate a new code every 30 seconds. Either way, a new, one-time number is required to complete the sign-in process, so only someone with your phone or account can use it.

How to use them: After entering your password, open your authenticator app, check your text messages or email, and enter the most recent code displayed in the app.

When to choose: Enable OTPs as the second factor for accounts such as email, banking, cloud storage, and social media. Use them whenever a service offers two-factor or multi-factor authentication.

Main risk: text message codes can be intercepted. Criminals may read your texts if they break into your phone or accounts, or if they install malicious software. A more targeted trick is a **"SIM swap"**: attackers trick your mobile company into moving your phone number to a SIM card they control, so text codes go to them instead of you.

Best Practices

- Use text messages only if no better choice exists. If you must send a text, secure your mobile account with a carrier PIN— a short secret number set with your mobile provider to protect your account—and stay vigilant for unexpected service issues.
- Never share codes or enter them on sites accessed through suspicious links.

Passkeys or Passwordless Login

What are they: A way to sign in without a password—your phone or tablet holds a secret, and you approve logins with a simple action (fingerprint, face recognition, or device PIN).

How to use them: When a site or app presents **"Sign in with passkey,"** choose that option and follow the on-screen setup to register the passkey to your device — you'll confirm with your fingerprint, Face ID, or your device PIN. Once registered, future logins are approved on that device without needing to type a password.

When to choose: Use passkeys whenever a service supports them. They're easier and relatively safer than passwords because you approve sign-ins on your device instead of typing a password.

Main risk

- Losing the device can lock you out unless you've set up recovery options.
- If an attacker gains full control of an unlocked device, they could approve logins.

Best Practices

- Turn on **passkey sync** so your sign-in keys are safely saved to your online account (like iCloud or Google Drive). This lets you use the same passkeys on all your devices—phone, tablet, or computer—without needing to set them up again.
- Add a second device (like another phone or laptop) to your account. That way, if one device is lost or breaks, you can still get into your accounts using the backup.

Biometrics

What are they: Physical or behavioral traits: a fingerprint, a face, or a voice. They work like a unique key tied to who you are.

How to set them up: Navigate to your device's Security or Settings, select your preferred biometric option, and follow the on-screen prompts to register. Once configured, you can unlock your device or approve sign-ins via a fingerprint read or face scan instead of entering a password.

When to choose: Use biometrics when convenience outweighs the need for absolute control, and the device or service is from a trusted provider. For everyday, low-risk tasks—unlocking your phone, approving app sign-ins, or confirming small payments—biometrics are considered reasonably practical.

Main risk

- You can't change them — If a fingerprint or face template is copied, you can't replace it like a password.
- May fail or accept the wrong person — Sensors sometimes don't read you properly or may falsely match someone else.
- Biometric data held by a company could be at risk if that company experiences a breach.

Best Practices

- Avoid depending solely on biometrics for highly sensitive accounts—use passkeys whenever possible.

- Choose systems that store biometric data only on your device. Use biometric services that verify **“liveness”** (movement, blinking, depth).

Adaptive Authentication

It is a smart sign-in system that asks for extra verification only when a login activity looks suspicious. It's like a bank teller who usually recognizes you visually but asks for ID if you arrive at an unusual time or are dressed differently.

What Do They Monitor?

✓ Is this the same computer, tablet, or phone you usually use?

✓ Are you signing in from your town or from somewhere far away?

✓ Is it during your usual time to use the service, or very early/late?

✓ Are you doing your usual activities (reading mail) or unusual ones (downloading many files at once)?

What Would Adaptive Authentication Look Like?

1️⃣ You type in your password as usual.

2️⃣ The service quickly examines the signals above and matches them against a **“typical”** pattern.

3️⃣ If everything looks normal, you’re logged in without needing extra steps.

4️⃣ If something appears risky, the service requests **"step-up"** verification.

5️⃣ For example, it might send a push notification that says **“Allow sign-in?”**—and you need to respond **“Yes”** if it’s you or **“No”** if it wasn’t you who triggered the alert.

6 Once you provide the additional proof, the service grants access. If you cannot provide it, it blocks entry to protect your account.

Two-Factor and Multifactor Authentication

Here's a quick reminder: authentication is the process websites and apps use to verify it's really you trying to log into services.

A 'factor' is just a type of proof. There are three main types:

- ➔ Something you **know:** like a nickname only your childhood best friend knows — you don't carry it, you just remember it.
- ➔ Something you **have:** like your house key or your library card — it's something you keep close and use to unlock or access things.
- ➔ Something you **are:** like your voice when you sing your favorite song, or the way your hands fit into your garden gloves — it's uniquely yours.

What Is Two-Factor Authentication (2FA)?

Think of 2FA like locking your front door with a key, then requiring a code sent to your phone to unlock a second or inside door.

Key point:

2FA mainly uses exactly two different factors, and the most common combination is:

(something you know) + (something you have)

For Example:

You enter your password (something you know) on your device, and then the system sends a six-digit code to your phone. You input this code (something you have) to verify your identity. Together, these steps confirm it's really you.

What Is Multifactor Authentication (MFA)?

It's like adding more obstacles to bypass your security system — it requires multiple types of proof, not just two, as two-factor authentication does.

Key Points:

- MFA can incorporate two-factor authentication (2FA), but it provides more flexibility by allowing any mix of three authentication methods.
- MFA is widely used in banking and government systems.

For example:

Scenario #1: A user logs into their bank's website. They enter their username and password. The bank sends a push notification to their phone asking them to approve the login. After confirming, they are prompted to scan their fingerprint to verify their identity.

Scenario #2: A user logs into a government website to check their healthcare benefits. They enter their user ID and password to start. The site then calls their home phone or sends a one-time code to their mobile device. Before access is granted, they are asked to answer a personal security question — the street they grew up on.

MFA is most effective when the factors come from different categories: knowledge, possession, and inherence. As in scenario one, the password (knowledge), phone push notification (possession), and fingerprint (inherence) are used, making it much harder for an attacker to compromise all of them at once. In contrast, scenario two involved pairing possession (phone code) with two knowledge factors (password and security question), which results in weaker security.

What "Save My Password" Really Means

When a website or app asks **"Do you want to save your password?",** it means they offer to remember your login details for future visits. However, what that entails and whether it's safe depends on how and where it's stored.

What's Being Saved?

It's not just your password that's saved; your email or username is stored as well. Saving this information allows the system to automatically fill in your details the next time you visit.

Why Do Systems Offer This

- To make it easier and quicker for you, so you don't have to remember or retype your password every time.
- It's especially helpful if your password is long or complex.

When is the Right Time to Say Yes?

☑ If the device belongs solely to you (not shared with others).

☑ If the device is secured with a PIN or biometrics.

☑ If you tend to forget your passwords.

When is the Right Time to Say No?

🛑 If you're using a public or shared device, like at a hotel.

🛑 If you're unsure whether the system is secure or trustworthy.

🛑 If you're accessing a sensitive account, like banking.

Can You Change Your Mind Later?

- Yes! You can delete saved passwords anytime through your browser or device settings. Look for the **"Passwords"** or **"Privacy & Security"** menu to view and delete them.
- You can also disable auto-save features if you prefer to type passwords manually. Look for the **"Autofill"** menu to turn off saving.

Where Are Passwords Stored?

In the browser's password storage: Internet search apps like Chrome, Safari, Edge, and Firefox store passwords in their own free-to-use password managers. When you sign into the browser and enable sync (using Google, Apple ID, or Microsoft), those saved passwords are uploaded to your account and synchronized across your other devices. Make sure to protect that account with a strong password and two-factor authentication.

In the device's built-in secure storage: Some devices have a default, ready-to-use, safe area for passwords. For instance, iPhones or iPads have the Keychain, which can fill in logins for users without needing a separate app.

In a password manager app: Separate pay-to-use password managers (like 1Password, LastPass, Bitwarden, etc.) store and organize your usernames and passwords, generate strong passwords, and fill them in on websites and apps. They can keep passwords only on one device or sync them across devices, depending on your settings.


Connecting Generations
Cyber-Seniors™


be well
ILLINOIS


aetna


BEYOND
FORCE


trail
TOTAL RETIREE ADVANTAGE ILLINOIS

DEFINITIONS

***App permissions:** are the permissions that an app can use on your phone or tablet — camera, contacts, location, microphone, or storage. When an app requests permission, it's asking to do something.

***Authenticator app:** functions as a compact ticket machine in your pocket, generating a new, single-use code every 30 seconds. When a website demands proof after your password, you use the latest code (the short code) from the app to verify your identity. Popular authenticator apps include Google Authenticator, Microsoft Authenticator, and Authy.

***Auto-saving or autofill** refer to closely related features: auto-saving remembers your username and password when you sign in, and autofill automatically fills those saved details into login forms later. They often work together: the browser or app asks to save (auto-save) and then uses that saved info to fill in fields (autofill).

***Biometric sensors** are the parts of a device, like the camera used for face unlock, that scan a unique part of your body.

***Breach** in technology is when someone breaks into a computer system, app, or online account and accesses data they shouldn't. After a breach, your information may be copied, leaked, or used for fraud.

***Built-in** (technology) means a feature or tool that comes already included inside a device, app, or system—no extra downloads or purchases needed.

***Cloud:** refers to online storage and services accessed over the internet instead of on your own device; it allows you to save files, photos, and backups online and access them from any device. E.g., iCloud and Google Drive.

- **Backups** are copies of your files, photos, or settings saved to the internet so you can restore them if your device is lost, broken, or reset. They run automatically or on demand, allowing you to recover data from any device after signing into your account.

***Device's lockout features** are built-in settings that temporarily block access after repeated wrong attempts—like requiring wait times, erasing data after many failures, or locking the device until a backup PIN, passcode, or account recovery—helping prevent strangers from guessing passwords or accessing data.

***Face ID** is a way to unlock your phone or apps by having the device scan your face—if the face matches the stored pattern, it opens without a password.

***Hacking** is when someone gains unauthorized access to your device, account, or data by bypassing passwords or security measures—to view, steal, modify, or control information or systems without your permission.

***Login:** is the information you provide to a website, app, or computer to verify your identity. Usually, this includes a username or email and a secret password known only to you. When you try to log in, the system checks whether the username exists and if the password matches its records. If both are correct, access is granted; otherwise, if not, access is denied.

***Malicious software (malware)** is any program secretly put on your computer, phone, or tablet to steal data, spy on you, or break things. Examples include:

- **Viruses** that spread and damage files.
- **Spyware** that reads your emails and passwords.
- **Ransomware** that locks your files and demands money to unlock them.

***Passkey sync** backs up your device's passkeys (the quick way to sign in without typing passwords) to your online account so they automatically appear on any device where you sign in.

***Phishing** is a trick where scammers send fake emails, texts, or websites pretending to be someone you trust (like your bank) to steal your passwords, money, or personal information.

***Plain-text files** are basic documents that include only readable characters such as letters, numbers, punctuation, and line breaks. They do not contain any fonts, colors, bold text, or images. Think of them like a simple notepad note—just words and lines.

***Public computers** are machines in places like libraries, hotels, or internet cafes that are accessible to everyone, often store temporary data, and may be less secure, so avoid signing into personal accounts or entering sensitive info on them.

***Privacy and security menu** (in password settings) is the place in an app or browser where you control how passwords are saved, shared, and protected.

***Push notification** is a short message that pops up on your phone or tablet from an app or service (like a bank or email) to alert you — for example, "You received a new message" — without you having to open the app.

- **Temporary data** is short-lived information stored temporarily by a computer during use, like visited websites, opened files, form entries, search history, and cached images. On public computers, this data remains until it is cleared or the session ends, making it visible to the next user unless it is automatically deleted.
  - **Cached images** are pictures a website keeps on your device briefly, so pages load faster next time.
  - **Search history** is a list of past searches and sites you visited, allowing you to find them again.

***Recovery email** is a secondary email address you provide to a service (like your primary email provider) so you can regain access if you forget your password or your account is locked.

***Sensitive accounts** are online or device accounts that hold your most important personal, financial, or health information. They need stronger protection because if someone else gets in, they can steal money, personal data, or access other services tied to you.

***Screen lock** is a security feature on your phone, tablet, or computer that prevents others from opening it without your permission. It appears when your device wakes up and prompts for a PIN, password, pattern, fingerprint, or face scan to unlock.

***Shared devices** are devices like phones, tablets, or computers used by multiple people—family, coworkers, or guests—where each person may have their own accounts or everyone shares a single profile. Sharing enables others to view apps, messages, or files unless individual accounts or guest modes are configured.

- **Guest mode** is a temporary, limited profile that lets someone use a device without accessing the main user's apps, accounts, or files; when finished, the guest session's data is deleted.

***Signing in:** is the process of entering your username (or email) and password — or using a linked account like Google or Apple — to prove you are who you say you are and gain access to a website or app. Once signed in, the site remembers your identity so you can see your personal settings, messages, or saved data.

***Signing out:** is the action of ending your session on a website, app, or device so it no longer recognizes you as the active user; it usually requires clicking a "Sign out" or "Log out" button and helps protect your account by preventing others from accessing it on that device.

***SIM swap,** also called SIM swapping, is a scam where a fraudster tricks your mobile carrier into moving your phone number to a SIM card they control. Signs include sudden loss of service, unexpected verification texts, or account alerts.

***SMS (Short Message Service)** is a simple text message sent between phones. It lets you send short written messages (no pictures or videos) to another person's phone number.

***Social media:** are websites and apps where people share posts, photos, videos, and messages to connect, follow others, and join conversations online.

***Streaming services:** Let you watch videos, listen to music, or view live shows online instantly without downloading. Faster internet ensures smoother playback. Examples include Netflix and Spotify.

- **Downloading** is getting a video, song, or file from the internet onto your device, allowing offline access. Unlike streaming, it saves the file locally, which may take time based on file size and internet speed.

- **Playback** is playing recorded audio or video to watch or listen to again. It begins when you press play and ends when the file finishes or you stop it. Controls include play, pause, rewind, fast-forward, and volume.

***Suspicious links** are web addresses in emails or texts that look odd or unexpected and can take you to fake pages or download harmful software. Signs include unfamiliar senders, misspelled addresses, urgent demands, or shortened links.

***Sync (short for "synchronize")** means copying your information so it's the same on all your devices. For passwords, turning on sync sends your saved logins from one device (like your phone) to your other devices (like your tablet or computer) so you can sign in everywhere without retyping. Sync keeps things up to date.

***Third-party** means a person or company that is not the main one you're using.

***Unlocking a device** means opening your phone, tablet, or computer so you can use it, for example, by entering a personal identification number.

***Verification message** is a code or link sent by text or email to confirm it's really you when signing in, changing a password, or setting up an account; you enter the code or click the link to prove your identity.