

2.1 Authentication (passwords, MFA, passkeys, biometrics)

Core Concepts: Protect Yourself, Protect Your Data

When you log into a computer or website with a User ID and password, you are authenticating; proving you are who you claim to be. Get this topic right and you block 90% of account compromises.

2.1.1 Understanding Authentication

Authentication answers the question "who are you?" A User ID is your unique identifier (often an email address). A password is a single verification factor paired with your User ID. Together, they prove you're the legitimate owner of an account.

2.1.2 The Basics

- Use a password manager
- Create strong passwords
- Never reuse passwords
- Handle security questions carefully
- Set up a recovery email
- Enable login alerts

Use a Password Manager

A password manager stores all your login credentials, auto-fills them when you need them, and can generate secure, random passwords for each account. This means you only need to remember one

password, the master password for your password manager, or vault.

Why use a password manager?

- Creates strong, unique passwords for every account automatically
- Bypasses the clipboard, protecting against keyloggers
- Detects when you change passwords and can automatically update them
- Can store payment cards and bank accounts ("wallet" feature)
- Allows secure password sharing with family without revealing the actual password
- Provides emergency access features if you're hospitalized or otherwise incapacitated
- Can store additional information as notes, like answers to your security questions

NEVER use your browser's built-in password storage. While modern browser password managers have improved, dedicated password managers offer superior security features including cross-platform sync, security audits, secure sharing, and breach monitoring. Browser-based storage also creates a single point of failure if your browser is compromised.

Important: DO NOT FORGET YOUR MASTER PASSWORD! You can share this with a friend or family member who can store it in their vault in case you forget. If you use a password manager which offers account recovery, set it up and carefully protect the recovery information.

Recommended: Bitwarden (<https://bitwarden.com/>). It's web-based so you can access it anywhere, has browser plugins, mobile apps, and offers both free and premium service. It includes all the features mentioned above.

If you want, you can use my self-hosted Bitwarden service at <https://pass.landisfam.org>. This offers the same protections as Bitwarden's official service, but less likely to be targeted by attackers. However, I still cannot recover your account if you forget your master password.

Once enrolled, install the applications in your browsers and on your mobile devices. Enable auto-fill, and start populating your vault by logging into each email, financial, and health related accounts, since those contain your most sensitive information. When doing this, I recommend you reset each password, most password managers have a password generator, and secure them in your password manager. If you use a browser extension, most password managers prompt you to automatically add information for websites not already in the vault.

While going through this process, I also recommend you go through each site's security settings. Review your security questions (see that topic below) and force logout of all devices. Note that afterward you will have to log in again on all devices.

Create Strong Passwords

Passwords that are easy to remember tend to be easy to guess. The solution is to make them long, using a phrase you can remember, but would take an attacker a very long time to guess or to use brute-force methods to crack your account. Follow this link and experiment with different

passwords: <https://www.security.org/how-secure-is-my-password/>

How to Create a Strong Password:

There is an adage in Bridge (a card game for old people), "length over strength." A long, simple password is more secure than a short, complex password. Think of a line from your favorite song, poem, or quote. Take a few words from that line, capitalize some letters, mix in numbers, and add a special character or two.

Example: From Robert Frost's "The Road Not Taken":

- Simple version: Tw0r04ds! (would take 1 hour to brute force)
- Strong version: tworoadsdivergedinayellowwood (85 sextillion years)

Email accounts deserve the highest level of protection. When you forget a password, most sites send a reset link to your email. This means if someone gains access to your email, they can potentially reset passwords for all your other accounts. I recommend 16+ characters for email passwords.

Recommended password lengths:

Account Type	Password Length
Password Manager	20+ characters
Email	16+ characters
Everything else	12+

Of course, if you use a password vault, you can have the best of all worlds, and use unique, 20+ character, complex passwords for all your accounts without ever having to worry about forgetting them. Again, just make sure the password for your password manager is also strong, and have a recovery method in case you do forget it.

Never Reuse Passwords

Use a unique password for every account. If one site gets breached, attackers will try that password on other popular sites. Reused passwords mean one breach potentially compromises all other accounts which use that same password. Your password manager, once populated, can verify that all your accounts have unique credentials.

Handle Security Questions Carefully

Security questions are a weak way to verify your identity. The answers are often public information or easy to find through social media. When forced to use them:

- Don't pick anything that could be public record (first car, school names, family names)
- Consider using false or ironic answers. The system only compares how you answer when prompted with what you entered when you created the answer; it cannot validate if the answer you provided is actually true
- Example: "What was your first car?" Answer: "Matchbox"

Your password manager likely has a “notes” section for each item in your vault, or a separate “notes” folder. You can put your security questions in one of those.

Set Up a Recovery Email

Create a secondary email account to use as a recovery address for your primary email. If you can't access your main email, you can use the recovery email to regain access to your primary email account. Keep this secondary email account highly protected too, and only use it as a recovery account; do not use it for any other purpose.

Enable Login Alerts

Turn on notifications for new logins. Most services offer this. When enabled, you'll get an email or text when someone logs into your account from a new device or location. If it wasn't you, you'll know immediately. You can typically find this option in security settings.

2.1.3 Better Protection

- Expand password manager use
- Enable Multi-Factor Authentication (MFA)
- Use passkeys when available
- Understand when is best to use biometrics
- Check for compromised accounts regularly

Expand Password Manager Use

Once you have your critical applications vaulted (email, financial, and health-related accounts), you'll want to go back and begin adding other important sites and applications like cloud storage (Google drive, iCloud, OneDrive, Dropbox), social media, and shopping accounts. Follow the same process to change the password using the password manager's password generator, forcing logout of active logins, and updating security questions.

Enable Multi-Factor Authentication (MFA)

MFA adds a second step to logging in; usually a code sent to your phone or generated by an authenticator application. If you use MFA, even if someone steals your password, they can't access your account without this second factor.

Common MFA methods (from least to most secure):

- SMS text codes: Simple but vulnerable to SIM-swap attacks
- Email codes: Better than nothing but relies on email security
- Authenticator apps: Generate time-based codes even without cell service. Examples include Google Authenticator, Microsoft Authenticator, RSA Authenticator
- Passkeys: Biometric, cryptographic, or physical devices you plug into your device (covered in Extra Credit)

Where to enable MFA:

- Password manager (highest priority)
- Email, financial, and health service accounts
- Cloud storage (Google Drive, iCloud, Dropbox, OneDrive)
- Social media accounts
- Shopping accounts
- Any other account with sensitive personal information

Recommended: Google authenticator is used very broadly, is available in both android and apple app store, and has a cloud backup feature in case your device is lost, stolen, or breaks.

The option to enable MFA on a website or application is typically in security options. You will usually be offered a choice of authenticator the site supports. Select the authenticator you have installed on your phone, open that application on your phone, and scan the QR code provided by the website by clicking the `+` icon on the authenticator application.

Important: When you enable MFA, you'll receive recovery codes (usually 8-10 random codes). Store these safely, like in your password manager, as they're the backup if you lose your authenticator; phones break, can get stolen, or get lost. You can also install the authenticator application on multiple devices, such as a tablet, so if you lose one device you do not lose access. Plus it is easier to restore to a new device that way.

Use Passkeys When Available

Passkeys are a newer, phishing-resistant way to sign in. They use cryptography instead of passwords, and are built into many devices. They're easier to use than passwords and more secure than MFA. Enable them when offered. Major sites like Google, Microsoft, Apple, and others now support passkeys. To start using passkeys, enable them in the website or application, typically in security options. Once enabled, you will be prompted to generate a passkey, typically through fingerprint or facial recognition. Passkeys are device-specific, but can be linked across all your devices.

Understanding Biometrics

Fingerprints, Face ID, and other biometrics are convenient but come with trade-offs:

Pros:

- Can't be forgotten
- Quick and convenient
- Better than weak passwords

Cons:

- Can't be changed if compromised
- Can be forged (though it's difficult and expensive)
- Can be compelled by court order (unlike passwords, which are protected speech)
- Someone with physical access to you can use your biometrics (passed out at a party, etc.)

Best practice: Use biometrics as a second factor alongside passwords, not as your only authentication method. For banking apps with very sensitive data, consider using a PIN instead of biometrics for unlocking the app on your phone.

Exception - Passkeys: Passkeys are different. When you use biometrics to unlock a passkey, the biometric stays on your device and only unlocks a cryptographic key. The website never sees or stores your biometric data. This makes passkeys with biometric unlock more secure than traditional biometric-only authentication, and it's safe to use them as your primary sign-in method.

Check for Compromised Accounts

Visit <https://haveibeenpwned.com> every few months to see if your email addresses have appeared in recent, known data breaches. If you find your information was compromised:

- Change the password for that account immediately
- Review recent account activity for unauthorized access
- If you reused that password anywhere else, change those too
- Enable MFA if you haven't already

2.1.4 Extra Credit

- Use hardware security keys
- Use one-time passwords
- Use separate email accounts

- Conduct full account audits periodically

Use Hardware Security Keys

Hardware authenticators like YubiKey <https://www.yubico.com> are physical devices you plug into your computer or tap against your phone. They're the most secure form of MFA because they can't be phished, intercepted, or duplicated.

Hardware keys are ideal for:

- Password managers
- Email accounts
- Financial accounts

Tip: Set up two keys and keep one in a safe place as a backup. That way if you lose your primary key, you'll still have access.

Use One-Time Passwords for Apps

Some services let you create app-specific passwords, or one-time passwords (OTP), instead of using your main password. This is especially useful for email accessed through desktop or mobile applications. The password only works once to connect the first device that uses it. Even if malware captures it, it's useless to an attacker.

Set these up for any critical applications that contain sensitive information. It may take a little hunting to find these settings. In Gmail, for example, "App Passwords" are within the 2-step verification settings, beneath the list of second steps. Once you generate the one-time password, log out of that application on your device, then log back in using the one-time password. Repeat this for all devices (phone, tablet, desktop, and laptop applications).

Review Account Security Regularly

At least quarterly, check your important accounts:

- Check recent login activity for suspicious locations or times
- Review authorized devices and remove any you don't recognize or are no longer using
- Verify your recovery information (email addresses, phone numbers) is current
- Look for third-party apps with access and revoke any you don't use

Separate Email for Sensitive Accounts

Consider using a separate email account exclusively for your most sensitive sites (financial and health portals) that you never use for anything else (shopping, social media, or regular communication). This makes it much harder for attackers to find or target this email, since it won't be in typical data breach lists. Ideally, you should have a total of 3 or 4 email accounts. One, primary account you use for regular communication, a secondary email for sensitive sites like financial and health portals, and a recovery email address which you use to recover your email accounts if you lose access. A fourth email can be used to split out messages from shopping, social media accounts, and so forth, since those generate the most spam.

When providing an email address to a company you can also use <https://10minutemail.com>. This is a service which offers disposable email accounts; they are only valid for 10 minutes by default, although you can extend 10 minutes at a time. While this account is active you can send and receive email like any other email account. Using this keeps your regular email private if you just want to try out a service but aren't certain you want to use it long-term. Once you register this email address with any service, if you decide to keep that service, you can always change your email address to one of your others.

Revision #3

Created 2026-07-12 21:19:12 UTC by Chris Landis

Updated 2026-08-29 06:06:24 UTC by Chris Landis