Password Safety & Two-Factor Authentication 🔐

Passwords are the keys to your online accounts. Using strong passwords – and protecting them – is vital to your cybersecurity. **Two-Factor Authentication (2FA)**, also known as two-step verification, adds an extra lock on your accounts that can stop hackers even if they somehow get your password. Let's break down best practices:

Create strong, unique passwords: The days of using your pet's name or "123456" as a password are (hopefully) long gone. A good password should be **long** (the longer the better; aim for at least 12 characters, and 14+ is even better) and **unique** for each account. It should mix letters (upper and lower case), numbers, and symbols. Avoid real words or personal info. For example, **do not use** your name, your family's names, birthdates, or common words like "password" or patterns like "abc123". Those are the first things hackers will try. Instead, think of a phrase or a combination of random words and numbers that only you know. One method is the **"passphrase"** approach: string together a few random words that mean something to you but no one else. For instance, Daisy7CoffeeTrain! – it's long (18 characters) and has a mix of letters (some capitalized), a number, and a symbol. It's easier to remember than a random string like xY#5^kLm0* but just as strong. Another example: SilverBatteryHorse92? – again, a random combo of words with some numbers and a symbol. Another example is to pick the first and last letters of the words in a favorite phrase or song and put them together with numbers and symbols. These are just examples; create your own. The key is **length and randomness**.

No reuse, ever: This is very important – **use a different password for every account**. Why? Because if one website gets breached and leaks your password, hackers will try that same email/password combo on other sites. If you reused the password on your email and banking – boom, they're in those too. Yes, it's harder to remember multiple passwords, but there are ways to manage (see below). At minimum, make sure your **email password** is unique (never used anywhere else) and very strong, because if someone gets into your email, they can use the "Forgot Password" on your other accounts to reset those.

Consider a password manager: If you find it overwhelming to remember dozens of complex passwords, you're not alone. Password manager apps (like **LastPass, 1Password, Dashlane, Bitwarden**, or others) can help by securely storing all your login credentials in an encrypted vault. You only have to remember one master password to open the manager, and it will generate and remember crazy complex passwords for all your sites. Many security experts recommend using these. There is a bit of a learning curve, but once set up, they can make your life easier (they can auto-fill logins for you on websites). If you're not comfortable with that, the old-fashioned way is to **write down your**

passwords on paper. This goes against what you might have heard, but writing them down and keeping that paper in a **very safe place at home** can be okay – certainly better than reusing one easy password everywhere! If you do this, don't label it "Passwords" openly; keep it somewhere an intruder wouldn't easily find. And of course, don't carry it around with you. The biggest threat is remote hackers, not someone breaking into your home for your Facebook password, so a hidden paper list has its merits for memory. Just remember to update it when you change passwords.

Never share your passwords: Treat your passwords like your toothbrush – don't share them with anyone else. Scammers may sometimes pretend to be tech support or a bank and ask for your password – real companies **never ask for your actual password**. They might ask security questions to verify your identity, but not your password itself. Also, be wary of forms or websites that ask for your password outside of the normal login process – it could be a phishing attempt to steal it.

Two-Factor Authentication (2FA): This is a crucial security step. 2FA means that to log in, you need something *in addition* to your password – typically a one-time code. The most common 2FA method is **SMS codes –** the site will text a 6-digit code to your phone whenever you (or someone) tries to log in. You then enter the code to complete login. Many sites also offer **authenticator apps** (like Google Authenticator, Microsoft Authenticator, or Authy). These apps link to your account and generate login codes that refresh every 30 seconds. They're a bit more secure than SMS (SMS can be intercepted in rare cases), but SMS codes are still FAR better than nothing. Some sites (especially banking) may use more advanced 2FA like a physical token or security questions or email confirmation codes. No matter the form, the idea is: **even if a bad guy knows your password, they can't get in without that second factor (the code or token)** which only you have. Microsoft stated that enabling MFA (multi-factor auth) can **block over 99.9% of automated attacks** on accounts. That's huge! It's like adding an alarm system to your house on top of the lock.

Enable 2FA on important accounts: Ideally, use it everywhere it's offered. At minimum, turn it on for your **email, financial accounts (banks, investment, PayPal, etc.)**, and any account that contains sensitive info (medical portals, shopping sites with your credit card saved, social media accounts to prevent hijacking). It might feel a tiny hassle during login, but you usually can "trust" a device for 30 days so you're not prompted every single time on the same computer. The extra 10 seconds to get a code is well worth the security. To enable 2FA, go into the account's settings (look for "Security" or "Login Settings") and find the two-factor or two-step verification option. You'll likely need to provide a phone number for texts or set up an authenticator app. They often also give **backup codes** – be sure to save those (write them down and keep with your password list, for example), in case you lose your phone.

Be cautious of 2FA fatigue or tricks: One emerging scam is if someone already got your password and tries to login, you'll get an unexpected 2FA code on your phone. They might then email or text you pretending to be the company: "We noticed unusual login attempt, please provide the code you just received to confirm it's you." Don't do it! If you get a login code you didn't request, that means someone *else* tried your password. Never give a 2FA code to anyone. That code is only to be typed by you into the real login screen of that service. If you get one out of the blue, it's safest to change that account's password because it could mean your password was guessed or compromised.

Secure your phone too: Because 2FA often relies on your phone, make sure your phone itself has a lock (PIN, fingerprint, etc.). You wouldn't want a thief to steal your phone and have easy access to your SMS or authenticator app. Most smartphones have options for a 6-digit PIN or biometric lock – use them.

Regularly update critical passwords: It's a good practice to change your important passwords once in a while, or immediately if you suspect it might have leaked. You don't need to change passwords super frequently (the old advice of every 3 months is now considered overkill for most people, unless an organization requires it), but **do change them if a site has a breach** or if you suspect someone learned it. Also, check if any of your accounts have had known data breaches (websites like haveibeenpwned.com let you enter your email and see if it appeared in a breach). If so, update those passwords.

In summary: Use **strong, unique passwords** and take advantage of **2FA** wherever you can. Yes, it's a bit more effort upfront to set up, but it dramatically increases your safety online – sort of like locking all your doors and adding a security alarm. Most of the big hacks you hear about (celeb social media hacks, etc.) could have been prevented with a stronger password or 2FA. You have the power to make it extremely hard for hackers to get into your accounts.

Password & 2FA Checklist:

- ☐ My passwords are **long, complex, and unique** for each account (no easy-to-guess words or repeats).
- ☐ I have turned on **two-factor authentication** on my important accounts (email, bank, social media, etc.), so even if my password is stolen, my account is protected.
- ☐ I store my passwords securely – either in a trusted password manager or in a safe physical place – and I **never share** my passwords or verification codes with others.