Module 5: All About Passwords

@cybervalkyries

Why Your Password Matters

Passwords are the first line of defense for your online accounts. They protect your messages, photos, games, and personal information. Without a strong password, anyone could get access and cause serious trouble.

Think of a password as the key to your front door. If your key is weak or easy to copy, anyone can get inside. That's why creating strong passwords is more important than you might think. It's not just about keeping strangers out. It's about keeping control over your digital life.

What Makes a Password Strong?

A strong password is long, random, and hard to guess. It should include letters, numbers, and symbols combined in a random order. Avoid common words, names, or birthdays. Those are the first things hackers try.
For example, “P@ssw0rd123” looks complex but is very common and weak. Instead, a password like “fR7$9kBv2!” is much harder to guess. The longer and more **unpredictable your password, the safer your account** will be.
Try making a list of a few strong passwords you could use for your accounts! Make sure that they follow the criteria listed in the first paragraph of this page!

Many websites **require** your password to contain the following: numbers, uppercase/lowercase letters and special characters!

Why Not Use the Same Password Everywhere?

Using the same password for all your accounts is like using one key for your house, car, locker, and bike. If someone steals that key, they get access to everything.

Hackers use stolen passwords to try logging into many accounts. If you reuse passwords, one hack can lead to multiple problems. Use different passwords for each account to protect yourself. It might seem hard at first, but there are ways to manage this safely.

Password Managers are your best friend

Remembering dozens of strong, unique passwords sounds impossible. That is why password managers exist. They store **all your passwords in one secure place, encrypted with one strong master password.**

When you visit a website, the manager fills in your login details automatically. This means you only need to remember one strong password. Password managers also help create new, strong passwords whenever you sign up for something new.

Using a trusted password manager is one of the smartest things you can do for your online safety.

Think Twice: Two-Factor Authentication (2FA)

Two-factor authentication adds an extra step to logging in. After entering your password, you also need to enter a code sent to your phone or generated by an app.

This means even if someone steals your password, they cannot get in without the second code. It is like a double lock on your door.

Many popular websites and apps offer 2FA. Turning it on greatly improves your account security.

Common Password Mistakes

People often make mistakes that weaken their passwords. Using simple words, repeating characters, or including personal info like names and birthdays are common errors.

Avoid keyboard patterns like “123456” or “qwerty.” These are the first guesses hackers try.

Also, don’t share your passwords with friends or family, no matter how much you trust them. Once someone knows your password, they could misuse it without you knowing.

Avoid Using....

- **Your Birthday**
- **Any personal indentifying info (name, age, etc)**
- **A pet’s name**
- **Information that can be found online about you**

How Hackers Steal Passwords

Hackers steal passwords in many ways. They might trick you into entering your password on a fake website or use software to guess passwords automatically.

They can also steal passwords from websites that don’t protect them properly. That is why using strong, unique passwords everywhere is essential.

Being careful online helps keep hackers away from your accounts. So, don’t put in your account credentials in a free robux generator website. I’ve done it and got no robux.

Recognizing Fake Login Pages

Hackers sometimes create fake websites that look exactly like real ones to steal passwords. These are called phishing sites.

Before entering your password, always check the website address carefully. Look for the “https” at the start and a padlock icon. These mean the connection is secure.

If something feels off, do not enter your password. Instead, type the website address yourself or use a bookmark.

What to Do if Your Password Is Stolen

If you think your password has been stolen, act fast.

Change it immediately on that account and any others that use the same password.

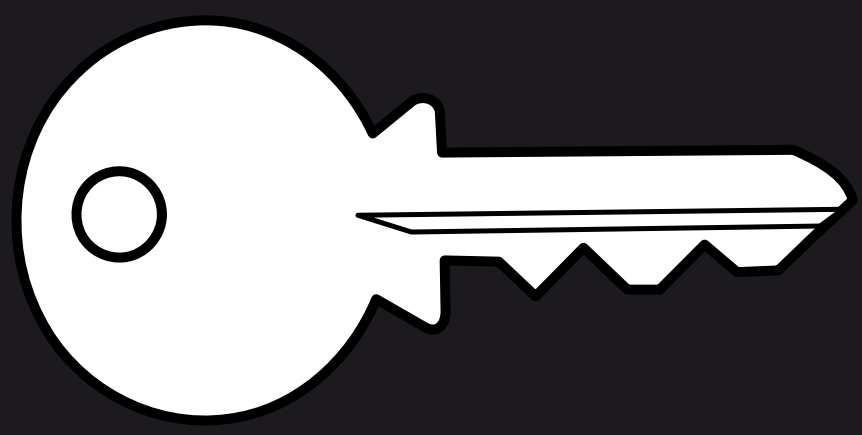
Check for suspicious activity like messages you did not send or purchases you did not make.
Notify a trusted adult or the website's support team if needed.
Keeping calm and acting quickly can prevent bigger problems.

Password Recovery Can Be Risky

Many websites let you recover lost passwords using your email or phone. Hackers try to trick these systems by pretending to be you.

Protect your email account with a strong password and 2FA. Be cautious if you get unexpected password reset messages. Always verify before clicking any link.

Your email is the key to many accounts, so guard it carefully.

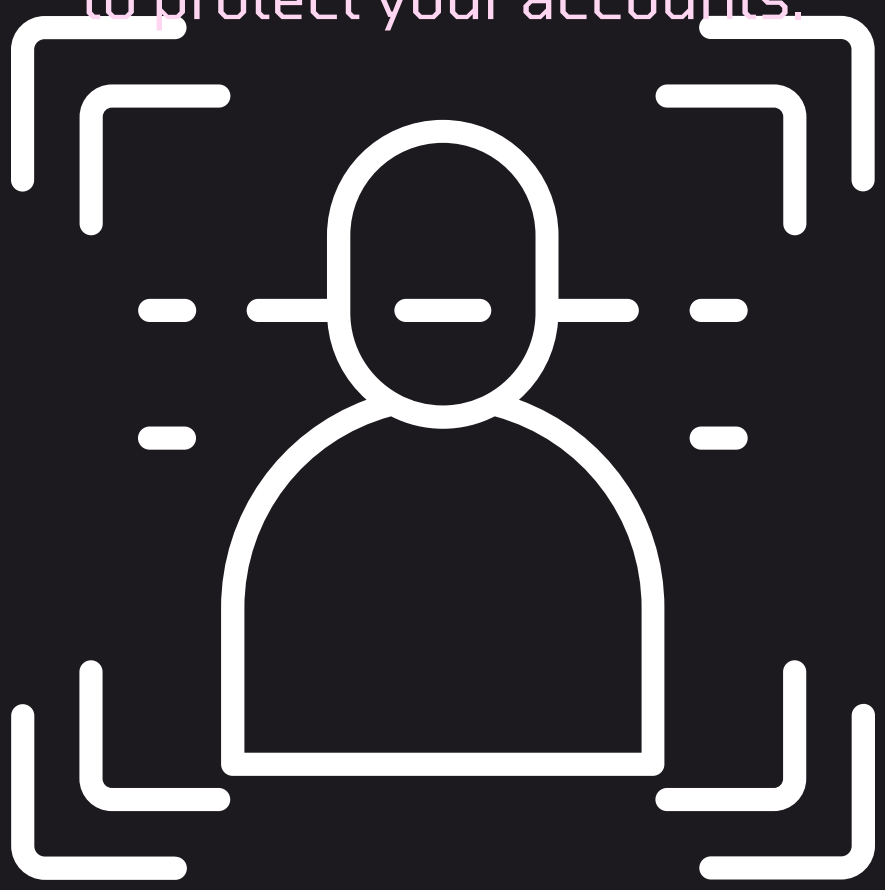


Using Biometrics

Your devices probably let you use fingerprints or face scans instead of passwords. These are called biometrics.

Biometrics can make logging in faster and safer because they are hard to fake. However, this does not mean that they are not prone to hackers.. Sometimes a photo or a fake fingerprint can trick the system.

Treat biometrics as a helpful extra, not the only way to protect your accounts.



Creating Passwords You Can Remember

Strong passwords do not have to be impossible to remember. Use a phrase or sentence and change some letters or add symbols.

For example, “I love cyber Valkyries 2025!” could become “ILcV@2025!” This is strong and easier to recall. Nope, this is not our password.

Finding a method that works for you helps keep your accounts secure without stress.

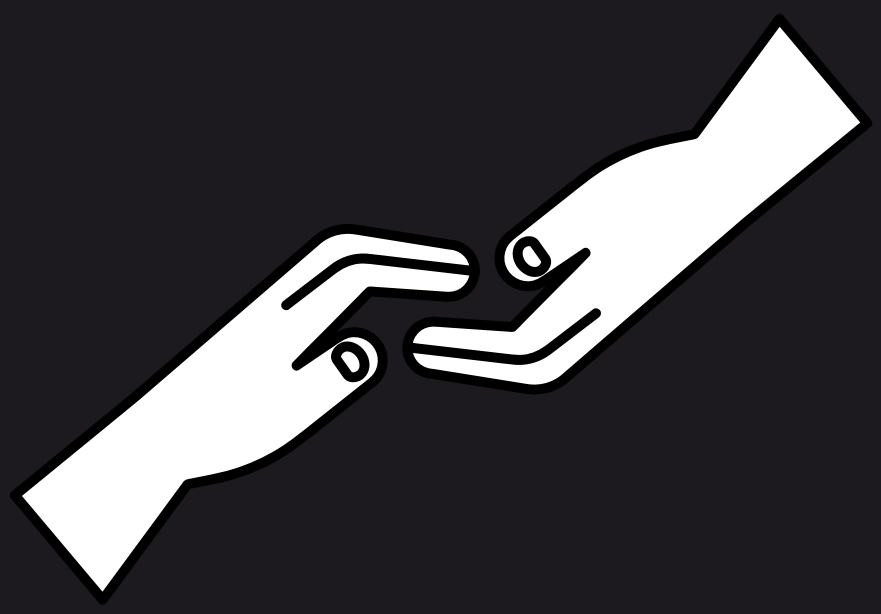
.

Sharing Passwords Safely

Sometimes you may need to share a password with a family member or trusted friend. Use safe methods like encrypted messaging apps or say it in person.

Avoid writing passwords down in places others can find them or sending them in regular chat apps.

Always change shared passwords afterward if possible to keep control.



Your Role in Online Safety

Strong passwords and 2FA are powerful tools, but they are only part of staying safe. Be alert to scams, suspicious messages, and anything unusual.
If something feels wrong, ask for help. You are the first and best defender of your online life. Your attention and choices protect your digital world every day.

Your Mission: Password Checkup

Today, review your passwords. Are they strong and unique? Do you use 2FA where possible?
If not, take time to change weak passwords and enable 2FA on your important accounts. Consider starting to use a password manager.
Help a friend or family member do the same.
Together, you can build a safer digital world.