Password Security

Always use a strong and unique password and do not reuse passwords across websites

Weak and Reused Passwords Risks

Financial risks

Privacy risks

Account access risks

Tips for Strong Passwords

Avoid personal information	Avoid personal details in passwords (name, birthday, pet name).
Use a mix of letters (Uppercase and lowercase, numbers, and Special Characters.	Mixing letters(Upper and Lowercase), numbers, and special Characters strengthens passwords.
Avoid common dictionary words	Avoid dictionary words; they make passwords easier to crack.
Use a random password generator	Use a password generator for strong, random passwords.
Do not share your passwords	Never share your passwords with other people.
Do not write down your passwords	Never store passwords insecurely or write them down.
Do not email or text your passwords	Never share passwords via email, text, or phone.

Unsafe Websites

Websites with phishing, malware, or unwanted software considered unsafe.

Measures to avoid unsafe websites:

1) Look for HTTPS in the URL.
2) Avoid anonymous proxy sites.
3) Check for a padlock symbol in the address bar.
4) Use of Modern browsers, which have filters and security tools that block unsafe websites.

Pop-up

Pop-up ads appear in new windows while browsing and can be intrusive. Some pop-ups urge people to perform an action by providing false information and they may contain malware or malicious links that could download ransomware or compromise systems.

Malicious Pop-up ad

Requires a payment	"Does a pop-up ask for payment? Legit sites don't use pop-ups for payments."
Provides a phone number to call	"Does the pop-up ask you to call a number? Verify it with the official site to avoid fraud."
Includes typos, spelling, and grammatical errors	"Typos and errors are common signs of online fraud."

Scareware pop-up

"Scareware is a social engineering trick, using pop-ups to scare users into clicking fake virus removers or system supports."
I. Tricks users into believing their system is infected.
II. Includes a fake support link or phone number.
III. Attempts to extort money or gain remote access.
IV. Displays fake compromise warnings, often with unstoppable audio.
V. Asks to install virus protective software or removers
1. Be vigilant
2. Know the signs of scareware
3. Contact your cybersecurity team

Social Networking Cyber Threats

Social media connects people and businesses but comes with cybersecurity risks.

Threats and vulnerabilities to take into account:

Phishing

Social engineering

Malware

Identity Theft

Account hijacking