Awareness Module 2 Cheat Sheet

by gonax133 via cheatography.com/211069/cs/45682/

Why Secure Browsing & Mobile Use Matters

✓ Protects against financial fraud, identity theft, and account takeover.
✓ Prevents malware infections from unsafe sites, downloads, and pop-ups.
✓ Safeguards personal privacy and organizational data.
✓ Maintains public trust in digital services.

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."

***Example**: Fake "Windows Firewall Protection" alert*

Scareware pop-up

Scareware is a type of online scam that tries to make you believe your device is infected. It usually shows fake warning messages, sometimes with loud or unstoppable audio, to create panic. These messages often include a fake support link or phone number, urging you to call for help. If you do, the scammers may try to trick you into paying money or giving them remote access to your device. In many cases, they will also push you to install supposed "antivirus" or "virus remover" software, which is actually malicious..

How to Protect from Scareware

- Don't install software from unofficial sources.
- Don't call numbers in pop-ups.
- Use browser pop-up blockers.
- Remove with antivirus software.
- Contact cybersecurity team.

Unsafe Websites

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

***Risks:** Malware, ransomware, phishing, identity theft, fraud.*

Measures to avoid unsafe websites:

1) Look for HTTPS:// and padlock in the URL.
2) Avoid anonymous proxy sites. (may steal data)
3) Avoid risky downloads (torrents, illegal sites).
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.

Password

Passwords are the first line of defense for your digital identity. Weak or reused ones can lead to financial fraud, exposure of private data, and account takeovers that can expose critical data.

Password Security & Best Practices

Tips for Strong Passwords

Use uppercase + lowercase + numbers + special characters.

Avoid dictionary words/common phrases.

Use long passphrases (easy to remember, hard to guess).

Check strength (e.g., Password Monster).

Avoid personal info (name, birthday, pet).

Use password manager like 1Password, Bitwarden, Dashlane, LastPass for security

Best Practices

✓ Never reuse passwords.
✓ Enable MFA.
✓ Don't write, email, or text passwords.
✓ Don't share passwords.
✓ Log out from shared/public computers.
✓ Regularly update after breaches.
✓ Review/remove unused accounts.

Social Media & Online Privacy

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

Threats and vulnerabilities to take into account:

1) Phishing, malware, identity theft.

2) Account hijacking via weak passwords or phishing.

3) Fake job offers & “get to know me” quizzes (data harvesting).

4) Impersonation/brand spoofing.

Best Practices

- Strong, unique passwords + MFA.
- Adjust privacy settings (limit data exposure).
- Think before posting (avoid sharing location, job, travel).
- Be selective with connections.
- Report fake accounts/suspicious activity.
- Stay updated on evolving scams.