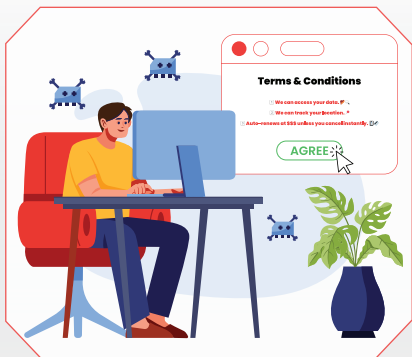
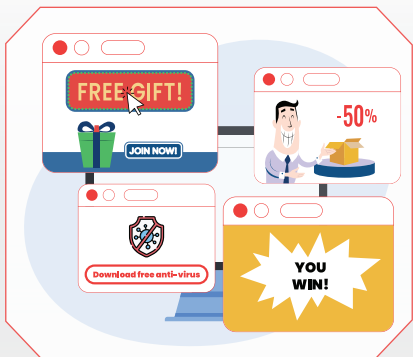




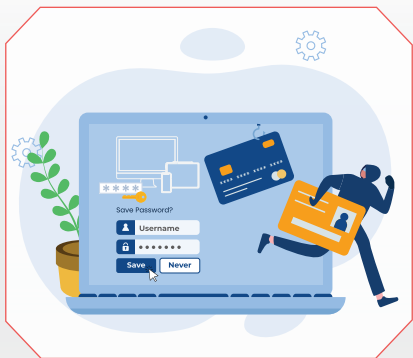
CYBER ALERT



Before you click 'agree' on any app or website, make sure you understand what you're agreeing to. Some terms and conditions can let apps collect personal information, which could be a privacy risk. Always take a moment to check what's being asked.



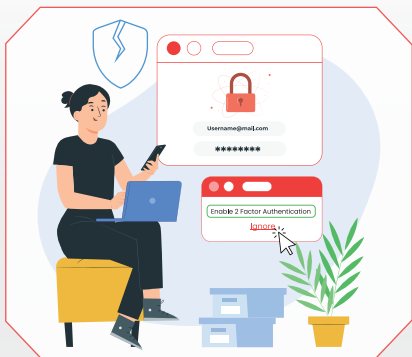
Enable pop-up and redirection blockers to stop ads and protect your device from harmful software like adware.



Avoid saving sensitive information such as passwords or credit card details in your browser.



Don't Click on links or
download files from
unknown sources.



Enable two-factor authentication (2FA) on your accounts to add an extra layer of security.



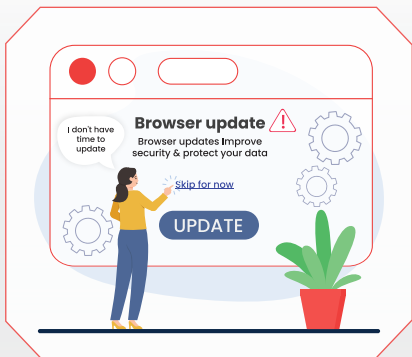
Always log out of your accounts when you're finished, especially on shared or public devices.



Turn off unnecessary permissions on applications such as location and camera.



Always use a strong
unique password and
never share it with anyone.



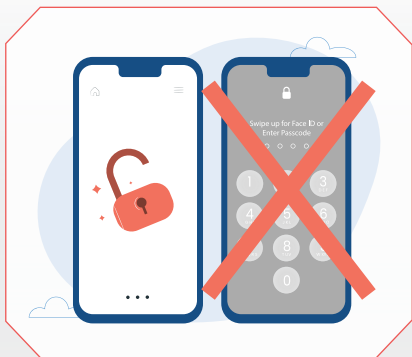
Keep your browser
up to date.



Keep your device's
operating system and
apps updated regularly.



Download an antivirus software from a trusted source and update it regularly.



Keep your devices locked with a password, PIN, fingerprint, or facial recognition for added security.



Disable automatic network connection feature to avoid connecting to insecure networks.



Avoid sharing your current location on social media platforms.



Check the reliability of the website/store before payment process and sharing of your information.



Cyber security is a
shared responsibility.

WATCH YOUR STUFF

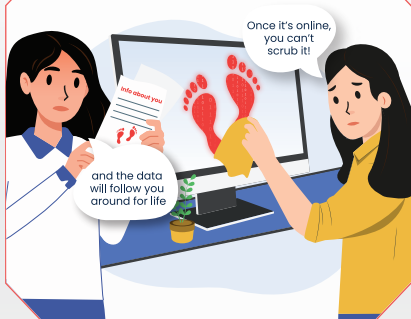


Don't leave your devices
unlocked and unattended
in public places.



Use blocking settings to protect yourself from random and fake accounts.

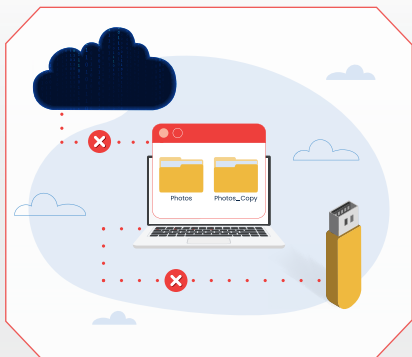
WE ALL LEAVE A DIGITAL FOOTPRINT



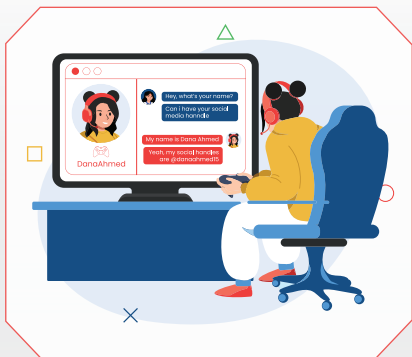
Practice good digital citizenship and leave a positive digital footprint.



Beware of offers and deals that are too good to be true.



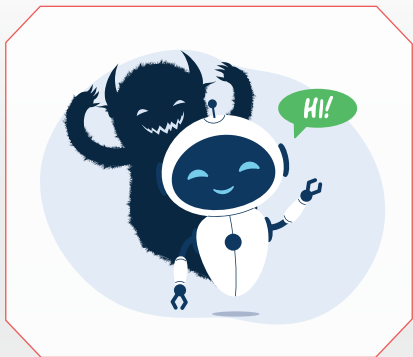
Keep a backup of your
important data on
cloud storage or an
external device.



Use a nickname that doesn't include your personal or private information when playing online.



Use a VPN or your personal hotspot on public Wi-Fi to keep your data safe.



Be careful when chatting with AI or chatbots. Don't share personal info, like your name or address, because they can be misused.



If you fall victim to a ransomware attack, don't pay any money to decrypt your files. It's better to ask for help from an adult or a cybersecurity expert.