proofpoint®

Security Essentials

Working remotely and on the web

Keep Private Data Private

Avoid illegal content

Don't download pirated files like "pre- release" movies and music or "cracked" software. These often contain malware.

Limit your social footprint

Be selective about what you post and who you connect with on social media.

Watch out for pop-ups

Don't interact with unexpected pop-up windows and ads.

They can install malware and viruses.

Think before you click

Watch out for suspicious emails and social media posts. Be cautious of shortened URLs.

Use Technical and Physical Safeguards

Enable security features

Activate firewalls, anti-virus, and wireless encryption. Password-protect all personal and business devices and systems.

Use secure sharing channels

Avoid taking sensitive files outside the office. If you must access confidential data remotely, use a secure server or other IT-approved channel.

Connect via VPN

Whenever possible, use a VPN when accessing business-sensitive data and systems.

Maintain separation

Do not allow children, family, or friends to use business devices for personal activities.

Have questions about working remotely? Contact your IT department.