

Do's and Don'ts of Cyber Security



Do: be aware of your surroundings



If you are away from your usual place of work or in a public space, be aware of those around you when working with sensitive information of any type.



Do: use strong unique passwords



Use a unique password of at least 12–16 characters for each account. A password manager can help you create and store them securely.



Do: ensure your laptop is always using the latest software version



Set it to auto-update to be sure you are always running the latest version.



Do: lock your devices when leaving them unattended and enable MFA for extra safety



Make sure your devices and accounts are secure any time they are out of sight.



Do: report any suspicious online activity and incidents to your IT team



If you see something unusual, tell someone. The sooner a leak is detected, the sooner it can be stopped.



Don't: install personal programs or apps on company computers and ensure all programs you are approved in advance



Unapproved software may not be licensed, may leak sensitive data, or allow cyber criminals access to company systems.



Don't: click suspicious links or attachments



Be especially wary of emails containing links and never click on suspicious links without checking with the IT department first.



Don't: use public WiFi hotspots without protection



Password-protected Wi-Fi isn't automatically secure; it's safer to use a trusted VPN or mobile hotspot.



Don't: use unapproved USB drives or external storage devices on work computers



They risk carrying a virus or code which could compromise security systems.



Don't: share passwords or allow others to use your computer



All activity on your computer and work devices is your responsibility, don't risk someone else causing a security breach using your devices.