Dos 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 passwords and do not use the same password for different programs or apps

Make sure passwords contain at least eight characters including upper case, lower case, numbers and special characters.

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 2FA for extra safety

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

Do: report any suspicious online activity and incidents to your manager

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 on emails if you are unsure of who they came from

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

Don't: use public WiFi hotspots for work

Public WiFi is rarely secure. Only use private, password protected networks.

Don't: use portable data storage devices on work on computers

Including USBs and hard drives as 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.

FreestyleTS