Computer Security Tips

LOCK YOUR DEVICE WHEN UNATTENDED

This protects company information and prevents your username or account being misused.

CHOOSE A STRONG PASSWORD

Make it easy to remember, but avoid using obvious names, dates or addresses. Use over 10 characters including a mixture of uppercase, lowercase, symbols and numbers.

DON'T STORE FILES ON PERSONAL DEVICES, EMAILS OR CLOUD STORAGE

Personal devices and services are not subject to the same security measures as your company's IT system. Any work-related information stored on them can be comprised without the company being aware of the security breach.

DON'T LEAVE SENSITIVE PRINTOUTS LYING AROUND

Company information needs to remain hidden from visitors and unauthorised viewers.

BEWARE OF PHISHING EMAILS

Cybercriminals often send deceptive emails with the intent to steal information or install malicious software, by convincing readers to open an attachment, click a link or enter details on a webpage. If you click on a link or download a file from a phishing email, you should notify IT support immediately. These emails often contain:

- Impersonation of a popular brand or website
- Spelling and grammar mistakes
- A high number of links throughout the email
- Links with text that doesn't match the destination URL (hover over a link to inspect it)
- Links to websites with foreign domain extensions, such as .ru
- Threats to shut down your accounts or services

ENSURE THAT FILES ARE BACKED UP

Save files in the correct folder so they can be backed up. Your IT provider will instruct you on where to save your work files.

Computer Security Tips

BEWARE OF PHISHING PHONE CALLS

Some criminals will try to obtain sensitive details over the phone, in order to impersonate a person or company, access an account or make a transaction. You should be suspicious of unsolicited calls which ask for sensitive information. These callers may impersonate well-known brands such as banks, utilities or phone companies.

GET PERMISSION TO CONNECT PERSONAL DEVICES

This reduces the risk of accidentally transferring malware from personal smartphones, tablets, computers, USBs or CDs onto company devices or networks.

REPORT LOST OR STOLEN DEVICES

The sooner the IT team knows about missing devices, the faster they can assess the risk and take precautionary measures.

REPORT SUSPICIOUS ACTIVITY

If something doesn't seem right on any of your devices or accounts, then notify IT support. It's important for them to be aware of a threat as soon as possible.