CYBER ATTACKS
EASY WAYS TO PROTECT YOUR SCHOOL OR COLLEGE

ACCOUNT MANAGEMENT

Ensure the relevant people know when staff resign so network accounts can be removed

Remove unwanted or unnecessary user accounts that you are responsible for

Change your password if accounts are compromised or you notice suspicious activity

WHY?
Forgotten accounts are an easy target for cyber criminals

PATCH MANAGEMENT AND SECURE CONFIGURATION

Update software and apps as soon as possible when updates are available

Delete unnecessary and unsupported software and apps

Only use approved and licensed software and apps from official app stores

WHY?
Updates patch weaknesses that cyber criminals can exploit

SYSTEM PRIVILEGES

Give colleagues appropriate levels of access for their role

Be extra careful if you have privileged access, as these accounts are targeted by cyber criminals

Do not let colleagues or pupils use your login details

WHY?
Incorrect access leads to unnecessary access to data, which is a data breach

CYBER ATTACKS EASY WAYS TO PROTECT YOURSELF

STAY ALERT

Check you are sending emails to the right people and use Bcc when necessary

Report anything suspicious to the relevant person or team in school

Avoid using public Wi-Fi such as in cafés or at conferences

WHY?

A common cause of data breaches is sending emails to the wrong people. Public Wi-Fi is insecure and targeted by cyber criminals

PHISHING ATTACKS

Check that emails, messages and social media posts are from who they say they are

Ensure links and attachments are legitimate before you open them

Be cautious if messages seem too good to be true or you're asked for personal information

WHY?

A successful attack can bring down the whole network

PASSWORD MANAGEMENT

Change default passwords as soon as possible

Never duplicate passwords across systems

Follow password advice and enable two-factor authentication if available

WHY?

Simple and duplicated passwords remain the most common vulnerabilities that criminals exploit