The importance of cyber security

Technology is changing rapidly and councils are increasingly making local public services available digitally, with workforces increasingly working online and working more collaboratively with partner organisations.

Not only is cyber security crucial to ensuring that services are kept up and running, it is also important that the public trusts us with their information.

A cyber attack could have very serious consequences by disrupting services – many of which serve the most vulnerable – and damaging the council's reputation. Healthy cyber security is therefore essential in ensuring that day-to-day services are kept up and running.

The council has technical controls in place to protect the network. However, sensitive information or data may be unintentionally released into the public domain due to simple human error, or a lack of awareness about the particular risks involved.

Personal cyber security tips

We are all responsible for protecting the council's information assets – following these three practical top tips help to keep the council's information safe:

- **Do not** click on an email link if you don't recognise the sender or subject - just delete it.
- **Do not** reveal your user ID or password to anyone over the telephone.
- **Do not** use weak passwords that can be easily guessed.
- **Do not** share passwords.

Watch these youtube videos on the importance of IT security for more essential hints and tips:

Phishing and Spear Phishing

Staff Security Awareness

Scams

Scams are designed to fool you into giving valuable information away, without realising it.

Cyber crime often relies on psychological scams to mislead you into revealing information, but as always, the last line of defence is you.

For each of the main sections summarised below, there is more detailed, essential guidance provided in the menu above, to help ensure that we all **'think before we click'.**

Remember, if it doesn't seem right, stop and report it immediately to the Network Security Team. See contact details at the foot of this page.

- **Email** is one of the main ways we communicate in our professional and personal lives but it's often an open door for malicious attacks into the entire council and our partner organisations.

- **Phishing** is an attack that uses email to trick or fool you into taking an action, such as clicking on a link, divulging information or opening an attachment.

- **Spear phishing** is tailored personal attacks– using personal information the hacker has gathered about you.

- **Telephone scams** are still common and text message scams are on the increase, with some of us using smartphones to access council networks and data via clicking on a link

- **The Internet** is constantly evolving, so it's important to stay safe and secure online especially when working in public spaces where it's essential to remain vigilant by looking after council equipment and information as well as ensuring the security of public wi-fi.

- **Social media** is closely woven into society and the council is increasingly using social media channels like Twitter to deliver and promote services.

- **Saving, sharing and storing electronic documents** must only be done via the council's own safe internal and online services for communication and storage.

Network Security Team contact information

Telephone: 0121 303 4743

Email: network.security.team@birmingham.gov.uk