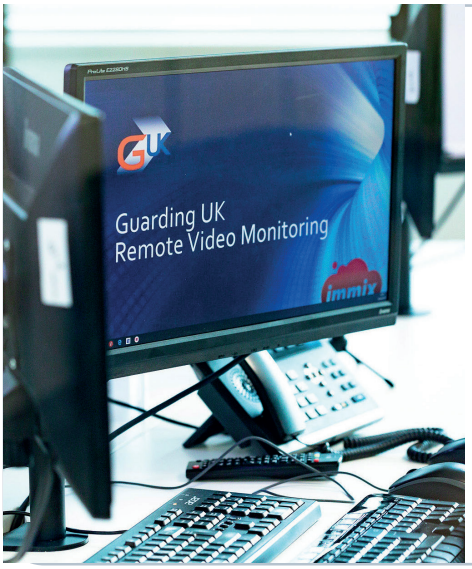
Cyber Security Refresher

February 2024

Whilst there is no current specific threat to GUK, like all businesses, we may become the target of a cyber attack which can be costly and disrupt our business.

You should all have completed the 'My Pathway' Cyber Security training.
You should revisit this training to refresh your knowledge

Cyber attacks can take many forms - here's a little reminder about the most common:



Phishing
Phishing is the most common type of common type of attempted attack that GUK has experienced. Hackers will impersonate a real company or individual to obtain details such as logins, bank details, company, and personal information.

The attacker may attempt to make the request look like it has come from a legitimate source. For example it might look like an email from a supplier saying that they have changed their bank account and requesting payment to a new account number. Any such request must be verified before any action is taken.

Our use of mimecast holds and blocks suspicious email. If you have any doubt about the source of an email held by mimecast, you should block it.

Prevention
As well as using mimecast to avoid Phishing schemes please observe the following: -

- Do not click on links or attachments that you do not recognise.
- Be especially wary of zip or compressed files.
- Do no provide sensitive information such as usernames and passwords over email.
- Watch out for email senders that use suspicious or misleading domain names.
- Be cautious about opening attachments or links if you receive an email from an external source.

Some Basic Security Practices to Adopt
Below are some best practices to adopt to ensure your Cyber Security:

- When prompted to change your access password do so.
- Ensure that your password is complex.
- Do share passwords, write them down or email them to yourself.
- If away from your desk close your screen and lock your PC.
- Initiate PC updates when prompted to do so.
- Clear your desk when finished and do not leave documents unattended.
- Do not bring or use personal memory sticks or external drives.
- Do not access restricted websites or download any material on your work laptop.
- Always keep your laptop secure.

GUK Security & Services Solutions
RUK Reception & Concierge Services