CYBER SECURITY IN THE WORKPLACE

Everyone in your organisation who has access to IT systems – from boardroom through to temporary employees – should be given regular training on cyber security.

The following issues serve as useful reminders for business owners when considering their cyber security needs and practices.

PASSWORDS

All devices should be protected: use a screenlock password for PCs and laptops, or other authentication methods such as fingerprint security where appropriate.

Two-factor authentication (2FA) is an excellent way of protecting access to your accounts. The usual way of implementing this is via a code sent to your smartphone after you have keyed in your password.

Encourage good password practices among both staff and customers according to company policy.

People will often forget passwords and request new ones: never send these via plaintext.

Work account passwords should not be used for other websites.

Do not share passwords. Staff with access to the same company accounts should set up their own passwords.

OUTSIDE THE OFFICE

Advise staff to avoid connecting to public WiFi networks where possible; mobile 3G or 4G networks are properly secured.

SHARE!

And finally….if hackers have successfully compromised your organisation, please share the details with the relevant authorities. The information Commissioner's Office will also need to be advised of any data loss, and online fraud or other scams can be reported on the UK's Action Fraud website.

IF YOU WOULD LIKE ANY FURTHER INFORMATION AND ADVICE ON CYBER SECURITY IN THE WORKPLACE, PLEASE CONTACT US AT INFO@CYJAX.COM OR VISIT OUR WEBSITE AT CYJAX.COM

CYJAX

A guide to cyber security in the workplace

CYJAX.COM

SOCIAL ENGINEERING

Be aware that attackers will seek to utilise publicly available information about your company in their attempts to make their phishing emails look more legitimate and convincing.

They will also target employees. Seemingly innocuous posts made on Facebook, Instagram or LinkedIn can provide a rich source of data for cybercriminals.

Encourage awareness among staff about the type of information they are revealing.

The online presence of business partners and suppliers should also be analysed. Are they giving away information about your own organisation that could be harvested by cyber criminals?

Check your organisation's digital footprint and encourage staff to do the same. See what is out there on social media sites such as Facebook or LinkedIn.

SMISHING

Smishing (short for SMS Phishing) is a type of attack that involves a text message. Much like malicious links in emails, these attacks target victims by using elements of social engineering to obtain personal information. Examples include messages claiming the recipient will be charged for a service they have not requested.

PHISHING ATTACKS

This is a common technique used by cyber criminals to gain access to confidential data, such as names, passwords and credit card information that can be used to carry out fraudulent activities against your organisation.

What to look out for: Emails laced with malicious links or attachments will be disguised and appear to come from a legitimate source. The attackers rely on the unsuspecting victim being fooled into clicking links or otherwise keying in information. For example, one typical scam could involve an email purporting to come from your bank and claiming that your account has been compromised. Or you may be sent an 'invoice' detailing a payment for something you have supposedly purchased. In both cases, you will be asked to key in certain information, thereby allowing the fraudsters access to the data they are targeting.

BUSINESS EMAIL COMPROMISE

Business Email Compromise is a common scam that can result in very severe financial losses. These emails will purport to come from a senior person in your company and will request payments of invoices to a particular bank account. Ensure your staff know how to spot suspect emails, and implement safeguards across the organisation that include simple security measures. For example, requests for financial transfers should not be sent over email, and where possible employees should be required to confirm all details face-to-face.

RANSOMWARE

Ransomware is one of the greatest threats currently facing organisations of all sizes. An attack typically starts when someone clicks on an attachment in emails, leading to the encryption of all documents on the PC or the network. Cyber criminals will then demand a sum of money for the release of the data.

In many cases, companies will be faced with the choice of paying the ransom, or losing the extremely valuable files.

Ensure that well-defined security policies are in place, with clear lines of responsibility within your organisation. And back up your data frequently!

PATCHING & SOFTWARE

All software must be kept up to date. When patches are released, make sure they are implemented quickly, if possible by allowing automatic updates on computers and mobile devices.

Obsolete software should be replaced with the latest version available.