NHS
Sherwood Forest Hospitals
NHS Foundation Trust

CYBER SECURITY PHISHING GUIDANCE

Cyber security risks are an ongoing threat across the UK, with the National Cyber Security Centre (NCSC) managing around 60 serious attacks each month.

As an organisation we have solid data security measures in place, but no system is completely impenetrable, as seen by the recent high-profile attacks on major global companies.

It's critical that we all act to minimise the impact on essential front-line services. Data security is everyone's responsibility and we all have a duty to protect public information in a safe and secure manner. Here are a few common security threats to be aware of, to help you remain vigilant against possible attacks.

Phishing

Phishing is a common tactic employed by hackers, requiring little effort and generally preys on the less cyber-aware. Criminals use phishing emails and websites to scam people on a regular basis. They are hoping that you will click on fake links to sites or open attachments so that they can steal data or install malicious software.

The aim of phishing emails is to force users to make a mistake – for example, by imitating a legitimate company's emails or by creating a time-limited or pressurised situation.

Phishing email attachments or websites might ask you to enter personal information or a password, or they could start downloading and installing malware.

It's also the most common way for organisations to be exposed to ransomware (paying to get your computer working again). Although we maintain controls to help protect our networks and computers from cyber threats, we rely on you to be our first line of defence.

What you can do

There's no way to guarantee against falling for a phishing email, but there are many things you can do to try and prevent an attack:

- don't click on links or attachments from senders that you don't recognise
- don't provide sensitive personal information (like usernames and passwords) over email
- watch for email senders that use suspicious or misleading domain names (where the email address originated from). Is the email name and domain name real? Hovering over the 'From' column is a simple way to check if an email is legitimate or not
- inspect hyperlinks carefully to make sure they're legitimate and not directing you to imposter sites. To do this hover over the link to see if it matches the URL that is displayed
- don't try to open any attachments that you're not expecting to receive.

Using your workplace device to access your personal email account

You are reminded not to access your personal email account using an organisational device (computer, laptop or mobile) as this could lead to malware/ransomware from a phishing email contaminating your laptop.

Using your work email address on external websites

You are reminded not to register your work email address on external websites. The more you use your work email address, the more likely you are to see your email address becoming exposed, which can increase the likelihood of phishing attacks.

If you use your work email address to register with, or log into different work related applications or websites you should use a different password for each application. Using a different password for each application/website helps prevent unauthorised people gaining access to your other accounts and data on the other systems if your password is compromised in one application/website.

You can check whether your email address is included in any well-known breaches using https://haveibeenpwned.com/

Using strong passwords

The easiest way to protect yourself from cyber threats is by having a strong password. It's simple – the longer and more complex your password, the more difficult it is to crack.

Traits of a bad password

Hackers have created databases of the most common words, phrases, and number combinations that they can run your password through to find a match. You should try to ensure that your password isn't easy to guess. We all know that passwords protect things that are valuable to us but that doesn't stop the most common passwords consistently including 'password', '123456', 'qwerty', 'football' and so on.

It is important that all passwords are strong. A strong password should:

- Be a minimum of 8 characters long.
- Contain at least two uppercase letters.
- Contain at least two lower case letters.
- Contain at least 2 numbers.
- Contain at least two special characters or non-alphanumeric characters, such as- ! ” £ $ % & * @.

Try to use phrases to help make a complex, secure password: EG. ‘Number 27 bus stops at my Street’ can become ‘N27bs@mS!’ by using the first letter of each word.

Make sure one password is not a derivative of another.

Even if a system allows, avoid reusing a password. Reusing that password could allow someone unauthorized access to your account.

It’s important to remember that you should not use the same password for multiple accounts – no matter how strong it is – because if one account gets compromised, then they’re all compromised.

Thank you for continuing to keep our organisation secure. Patient safety and care relies on strong data security and you are our first line of defence against the majority of the attacks we face. If you have any questions or need further guidance please contact Information Governance sfh-tr.information.governance@nhs.net.