cw audit
audit and assurance services

NHS

Counter Fraud Team CCG Update

July 2018

CYBER CRIME

Many health organisations within the United Kingdom have been targeted by cyber criminals, mainly last May 2017 by a virus called ransomware. Do we however fully understand what all the different terms used really mean and know how to protect ourselves against potential scams?

This is a brief guide to help you understand some unfamiliar terms:

COMMON EXPRESSIONS

Phishing:
Emails usually contain malicious software, designed to entice or scare you into clicking on a link or opening an attachment, and then provide personal information such as usernames, passwords and credit card details.

Impersonation:
Information online through social media help criminals be very convincing when sending emails impersonating management, staff, customers and suppliers.

Keystroke Logger:
A program or device that captures every key depression on the computer. Cybercriminals install them on computers to clandestinely record the computer user password.

DO NOT CLICK ON THE LINK
If the offer looks too good to be true, or it is time sensitive putting you under pressure to act quickly, it could well be a scam.

Hacker:
Someone who users skills to gain access to a computer or network without authorisation.

Pharming:
A technique used by hackers to redirect users to false websites without their knowledge.

SUSPECT AN EMAIL IS ILLEGITIMATE?
If an email looks dodgy, check the email address look for characters added or removed. Hover over the email address to see if it changes.

Produced on behalf of:
NHS Redditch and Bromsgrove Clinical Commissioning Group
NHS South Worcestershire Clinical Commissioning Group
NHS Wyre Forest Clinical Commissioning Group

SO WHAT CAN YOU DO?

How can you reduce the threat?

- Be alert to unsolicited emails and avoid clicking on links or attachments from unknown sources.
- Consider ethical phishing campaigns to see how good staff are at spotting them
- Have regular fraud and cyber-crime awareness training and refreshers for all staff
- Have a strong password to log on to your computer.

Password Guidance

Always use a different password for each website, this will help prevent unauthorised people gaining access to your other accounts and data should your password be compromised to one website.

A strong password should:

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

Try using phrases to help make a complex secure password e.g "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 passwords can make it easier for someone to gain unauthorised access to all of your accounts.

If you suspect an act of possible cyber crime please do not hesitate to contact the CCGs Local Counter Fraud Team.

Your dedicated Counter Fraud Lead is Fiona Dwyer:

Mobile: 07552 290964 or 02476 536880
Email: fiona.dwyer@cwaudit.org.uk
FDwyer@nhs.net (secure email)

Please feel free to contact Fiona should you have any concerns or suspect that fraud is being committed against the CCGs.

Thank you for taking the time to read this and remember:

You can report any concerns you have directly to the CCG's Anti-Fraud team via the details contained in this newsletter or to the NHS Counter Fraud Authority via:

NHS National Fraud and Corruption Reporting Line: **0800 028 40 60**
Online: **www.cfa.nhs.uk**