Alert: Scams

We are continuing to see an increase in scams exploiting remote working arrangements and urgent need for goods and services as a result of Covid-19.

Examples of some of the fraudulent contact recently received:

A blank email is received by the NHS employee with the subject 'FW: Audio: Message Received on X July 2020'. A HTML file, with the recipient's name and a telephone symbol included in the name, is attached.

Fraudsters are contacting NHS employees purporting to be a genuine senior member of staff.

The fraudsters may make initial contact by email and ask for the individual's phone number to continue the discussion by text message.

The fraudster then requests that the staff member urgently purchase an Amazon gift card and provide the code and a photo of the card or receipt to the requestor, stating that the individual will be reimbursed.

Fraudsters are contacting external organisations purporting to be selling digital advertising space within NHS premises.

The fraudsters target organisations offering services which may be of benefit to patients about to be discharged, such as transport or home cleaning services.

Although the intention is to defraud the external organisation, there is a reputational risk if the organisation believes it has entered into an agreement with the NHS organisation.

A chain of emails between a credit controller and the organisation's Director of Finance is sent to a member of the Finance team.

The chain of emails, which has been created by the fraudster, suggest that the credit controller is chasing an outstanding invoice and that the Director of Finance has approved the payment for issue.

When challenged, the fraudster responds as the Director of Finance attaching the outstanding invoice.

A high importance email is received by the NHS employee stating that they are required to confirm their access to Office365 by clicking on a verification link within the email, otherwise they will be unable to login.

The email includes multiple authentication codes and reference numbers, and states that the email has been encrypted by Office365, in order to make the request seem legitimate.

Individuals are receiving telephone calls threatening them with arrest and the seizure of property if they do not make an immediate payment to settle a government debt.

Some calls use a recorded message and request the caller select an option from a switchboard menu to speak with the lawyer in their case.

Fake emails often (but not always) display some of the following characteristics:

- The email contains spelling and grammatical errors.
- The sender's email address doesn't tally with the trusted organisation's website address.
- The email does not use your proper name, but uses a non-specific greeting like "Dear customer", "Hi friend"
- A sense of urgency; for example the threat that unless you act immediately your account may be closed or patient safety may be compromised.
- A prominent website link. These can be forged or seem very similar to the proper address of the known company, but even a single character difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the company that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format.
- The image contains an embedded hyperlink which if clicked would divert to a bogus site.

What should you do if you have received a scam email?

- Exercise **caution** when dealing with any unsolicited emails.
- Check the **sender's email domain** by hovering your mouse over the sender's name.
- **Do not click on any links** in the scam email.
- **Do not reply to the email** or contact the senders in any way.
- **Do not open any attachments** or download content or images if you are prompted to do so.
- Permanently **delete the email**.
- **Report** any concerns to IT security and/or your Local Counter Fraud Specialist team.

Be aware that scams and phishing attempts are not always in the form of an email, but can be a text message, phone call or social media contact. You can report suspicious contacts by emails or other methods to Action Fraud.

For more information please contact:

Kate Harrington Stillwell
Senior Consultant
LCFS
07778 862 713
kate.harrington-stillwell@rsmuk.com

Matt Wilson
Manager
LCFS
07484 040 691
matt.wilson@rsmuk.com

rsmuk.com