Fraud Counts Newsletter

April 2021

SOCIAL ENGINEERING



This Photo by Unknown Author is licensed under CC BY-NC-ND

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions, using manipulation to trick users into making security mistakes or giving away sensitive information.

The growth of social media is an obvious target for criminals, it is a place where people share and debate their views, play a variety of online games and tell either their friends, or, potentially, the whole world about themselves and what they have done.

Striking examples of this are games where you answer (seemingly innocuous) questions and the game will give you an alternative name, such as your “elf name”, “Pirate Name”, your “Soap Opera name” or tell you what type of personality you have.

There are at least as many variations on this theme as there are cyber criminals. Perfectly innocent questions may be interspersed with more sinister questions such as, “Where did you grow up?”, “What was your first pet’s name”, “Where did you first go to school?”, “Who was your favourite teacher?”. These are typical security questions to reset passwords used on online accounts. Not only might the answers to these questions enable criminals to access your accounts and lock you out of them, but they are also snippets of information that can lead on to other crimes such as identity theft.

When a cyber hacker has even a small quantity of information about their potential victim, those little nuggets of information are used to find more and more information about an individual they are targeting, very much like following a trail or breadcrumbs. It can be a matter of minutes for an experienced hacker to find out your address, family members, where you live, whether you own or rent your home and, if you own, how much you paid for your house. It is very simple to find out if your property is mortgaged, who your mortgage is with and even how much you owe.

Whilst social media can be a great place to have fun, provided you take the right precautions such as heavily restricting who can see your information and thinking carefully before you answer any questions posed, social media can also be a safe place.

Thinking more widely, we strongly encourage people to be very careful of any unsolicited approach, whether online, in person (such as someone undertaking a survey in the street), by traditional mail or in any other form. Information is a valuable asset in this day and age and whilst most people will be honest in their intentions when they approach you, a significant minority will have very different thoughts in mind.

Criminals want to convince you to do something which they can use to their advantage



This Photo by Unknown Author is licensed under CC BY-NC-ND

The most common form of social engineering is phishing. In a scam email or text message, the criminal's goal is often to convince you that they represent the organisation they claim to be from so that it is safe for you to click a link within the communication. Once clicked, you may be sent to a fake/replica website which could download viruses onto your computer or steal your passwords and personal information.

Over the phone, the approach may be more direct, asking you for sensitive information, such as banking details. Sometimes, criminals pretend to be calling form your bank's fraud department or the police and tell you there has been suspicious activity on your account. They will try to panic you into either disclosing your security details or to move your money into a "safe account" which is really the criminal's own bank account.

Alternatively, they may pretend to be someone you trust, or a trusted organisation. This could be your Internet Service Provider (ISP), local council, employer, supplier or even a friend in need. And they may contact you by phone call, email or text message. Most fraud cases affecting the UK involve the use of the internet to unlawfully obtain victims' personal information, such as names, dates of birth, bank details and National Insurance numbers. Social engineering is one of the primary mechanisms for eliciting this information.

A successful phishing attack will result in the victim entering their log in details which will immediately be revealed to criminals. The consequences are, sadly, very predictable.

Employees have an important role to play in keeping themselves and their organisations secure by remembering that **most cyber fraud attacks depend entirely on human interactions**.



If you have any suspicions or concerns,
You can call us anonymously on

0800 028 40 60

POWERED BY **CRIMESTOPPERS**

Or search 'NHS Fraud' online for more information
The NHS Counter Fraud Authority leads on fighting fraud, bribery and corruption in the NHS and the wider health group

NHS
Counter Fraud Authority

Department of Health & Social Care

The techniques cyber criminals will use

To avoid being tricked and to protect yourself and your organisation from cyber criminals, it is important to understand the different techniques cyber criminals will use. Some common warning signs in the communication from fraudsters, include the following:

Spelling errors

Spelling errors in email addresses and email addresses which closely match a legitimate address but vary by only one or two characters. For example, the letter "I" could be swapped for the number 1 or "O" for 0.

Poor grammar

Poor grammar and spelling in email correspondence and letters sent by fraudsters (this is often done deliberately, don't be fooled into thinking the fraudster is being stupid!)

Incorrect job titles

Incorrect job titles in email signatures.

Specific information

Communications specifying that replies should be made to specific individuals and specific email addresses only.

Always report cyber incidents immediately



For work related cyber-crime such as suspicious emails via NHS Mail or work phone calls, contact your local IT departments. For cyber-crime incidents outside of work you can report to:

Email - if you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk.

Text message - suspicious text messages should be forwarded to 7726 (spells SPAM on a standard phone keypad). This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.

If you would like a cyber awareness presentation, please contact your organisation's Local Counter Fraud Specialist -contact details are at the back of this newsletter.

NHSCFA Copyright 2020 - This information is licensed under the terms of the Open Government Licence.

Some common tactics fraudsters are using include:

	Emails or letters accompanied by pressuring phone calls requesting that a particular change or payment be actioned straight away.
	Letters purportedly from suppliers / third parties including company logos but which do not appear to be on the company's official headed paper or appear "cut & pasted" – logos are often readily available on the internet.
	Letters containing contact details for a known supplier which differ to the ones usually used. This means that if a company tries to call or email to confirm payments / bank details they will contact the fraudsters rather than the genuine intended recipient of the funds.
	Payee bank accounts in locations or jurisdictions which have no apparent connection with the payee. It is possible that a UK company might want you to pay into an offshore account but if this is a new arrangement it should warrant further checks. It is worth remembering that fraudsters can hack email accounts meaning that they can include genuine historic email correspondence in their communications.
	Increasingly fraudsters are playing the long game where they inform the organisation of their change in contact details (such as a new phone number or email address). Then after a period of time they will request to change the bank details. The organisation may then use the contact details on file (which were previously changed by the fraudster) to confirm the request is legitimate. This form of calculated fraud is on the increase and organisations must be extremely diligent about any change and independently verify them.

Suspicions of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence - 0800 028 40 60 or www.reportnhsfraud.nhs.uk



©ASW Assurance

OUR LOCAL COUNTER FRAUD TEAM

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact your Local Counter Fraud Specialist (LCFS) below.



Gareth Cottrell – Counter Fraud Manager

gareth.cottrell@nhs.net ☎ 01872 258057/07814 002364

LCFS for Royal Cornwall Hospitals NHS Trust, Cornwall Partnership NHS Foundation Trust and Cornwall Care



Tracy Wheeler – LCFS

tracy.wheeler2@nhs.net ☎ 01752 431378/07789 868568

LCFS for University Hospitals Plymouth NHS Trust, Devon Partnership NHS Trust, and Livewell Southwest



Adele Rilstone – LCFS

a.rilstone@nhs.net ☎ 07775 417508

LCFS for Torbay and South Devon NHS Foundation Trust



Alice Lee – LCFS

alicelee1@nhs.net ☎ 07813 540022

LCFS for Devon CCG and Out of Hours Service Providers



Eli Hayes – LCFS

elias.hayes@nhs.net ☎ 07920 284239

LCFS for University Hospitals Bristol and Weston NHS Foundation Trust and Bristol, North Somerset and South Gloucestershire CCG



Mo Jackson – LCFS

mo.jackson@nhs.net ☎ 07824 606899

LCFS for Northern Devon Healthcare NHS Trust and Royal Devon & Exeter NHS Foundation Trust

©ASW Assurance