Fraud Counts Newsletter
Cyber Crime

Autumn 2020

How secure is your password?

Cyber crime is a high risk to the NHS and NHS Providers, especially during the current climate where many members of staff are working from home. Whilst the NHS has very good technical measures in place that successfully fends off most cyber crimes, a small percentage still get past these defences. The last line of defence against cyber-crime is **PEOPLE**.

Whilst organisations need to be successful at defeating criminals all of the time, the criminals themselves only need to succeed once.

When criminals use IT to "guess" passwords, they use computer programs that initially try commonly used passwords and then move to trying every possible combination of characters. The longer and more complex the password, the more time it takes for a hacker to "crack it".

Here's some sample passwords with the estimated time for a computer to successfully guess it:

- "Password" / "Pa$$w0rd" - 0 seconds.
- "qwertyuiopasdfghjkl" (the top two rows of letters on a keyboard) - 2.01 minutes.
- "TreeSnookerAmbulance" (three random unrelated words that are easy to remember) - 2 months.
- "I'm not giving you my password" – (i.e. a memorable phrase of many characters) - 56 million years.
- "Fs&kg&se&t&c&uk" (the first letters of someone's home address separated by "&") - 14 thousand trillion years!

It's important to use passwords that you can remember but very difficult for anyone else to guess!

Protect yourself both in work and in your personal life by creating strong and memorable passwords by using three random words. Avoid using predictable passwords such as dates, family and pet names. Use a separate password for your work account.

The National Cyber Security Centre has seen a growing number of cyber criminals and other malicious groups online are exploiting the COVID-19 outbreak for their own personal gain with a range of ransomware and malware. Cyber criminals have also been scanning for vulnerabilities in software and remote working tools as more people work from home during the pandemic.

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

What is cyber crime and social engineering?

Cyber crime is a global threat. Criminals will seek to exploit security or human vulnerabilities by hacking into computers or networks in order to steal data, passwords or to simply disrupt business.

Social Engineering is the manipulation of people into performing actions or divulging confidential information. It is therefore easier to trick people into opening an infected email than it is to hack into a computer system. Additionally, hackers build up a level of rapport with their victims and over a period of time, con them into revealing pieces of information which they can then use to commit their crime. For example, quizzes on social media often ask some question which will give password security reset answers; "What was your first car" and "what was your Mum called before she got married" are quite common.

During COVID-19, a cyber attack on an NHS Trust in the South of England resulted in it being infected with a virus known as Hama. The NHS organisation's IT security team was alerted to monitor the network for any unusual activity. Other social engineering attacks have also been uncovered during COVID19, which are:

- **Phishing** is when cyber criminals will send an email pretending to be from someone else, such as your bank. The email will often contain a link, which when pressed, can install malware or obtain login credentials. The cyber criminals will make the email appear to be from a legitimate source by using the same bank logo. By doing this the receiver is more likely to reply or take the action requested in the email.

- **Smishing** is the text message (SMS) equivalent to phishing. The text message will appear on your phone. Criminals can disguise their mobile phone number to make it look like it is from a reputable source and will try to convince you to click on the attached link. When the text message is received, these messages can appear in the same text threat as genuine messages.

- **Spear phishing** is a direct form of phishing as the email will target a specific person. The sender is often shown as a person the receiver will know, such as work colleague or senior employee. The email may contain information about the receiver which has been obtained from the internet such as LinkedIn or other social platforms and can make the email seem more genuine.

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

Bogus NHS Test and Trace emails

NHS Test and Trace phishing emails are being sent by scammers, the fake email refers to the service as 'track and trace'. The email advises the recipient that they have been exposed to someone who has tested positive for coronavirus. They are instructed to click on a link in order to find out who that person is and are warned that if they fail to do so within 24 hours, legal action may be taken and their benefits suspended.

Bereavement Services

Fraudsters are contacting families claiming to be from the Local Authority's bereavement services team. They will ask families to provide card details and say funerals will be cancelled if not paid.

TV Licensing

TV Licensing phishing emails continue to circulate, asking users to update direct debit details, or offering a COVID-19 six-month free TV Licence offer.

HMRC

HMRC phishing emails continue to circulate. A recent Financial Times investigation found that the number of emails reported to HMRC had increased to 42,575 in March, an increase of 74% since January.

Cyber crime

In the meantime, below are some useful tips on what you should and shouldn't do:

DO

- Use your organisation's security tools.
- Enable multi factor authentication where possible i.e. text security code as well as password.
- Remain vigilant against phishing attacks.
- Create stronger passwords.
- Keep work passwords different to personal ones.
- Install latest software and app updates.

DON'T

- Leave work equipment unattended/unlocked.
- Let others use your work equipment.
- Leave equipment visible in public including downstairs windows at home.
- Connect to untrusted Wi-Fi hotspots.

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:

- **Action Fraud**—0300 123 2040
- **Phishing emails** – report@phishing.gov.uk
- **Spam texts** – 7726 (standard phone key pad – spells SPAM)

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 – Interim Counter Fraud Manager
01872 258057 or 07814 002364
gareth.cottrell@nhs.net

LCFS for:

- Royal Cornwall Hospitals NHS Trust
- Cornwall Partnership NHS Foundation Trust
- Cornwall Care

Tracy Wheeler - LCFS
01752 431378 / 07789 868568
tracy.wheeler2@nhs.net

LCFS for:

- University Hospitals Plymouth NHS Trust
- Devon Partnership NHS Trust
- Livewell Southwest

Shamaila Asghar - LCFS (maternity cover for Adele Rilstone)
07775 417508
shamaila.asghar@nhs.net

LCFS for:

- Torbay and South Devon NHS Foundation Trust

Alice Lee - LCFS
07813 540022
alicelee1@nhs.net

LCFS for:

- Devon CCG
- Out of Hours Service Providers

Eli Hayes – LCFS
07920 284239
elias.hayes@nhs.net

LCFS for:

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

Mo Jackson - LCFS
07824 606899
mo.jackson@nhs.net

LCFS for:

- Northern Devon Healthcare NHS Trust
- Royal Devon & Exeter NHS Foundation Trust