Penetration Testing - Phishing

Benchmarking Exercise

www.360assurance.co.uk
enquiries@360assurance.co.uk

www.audityorkshire.nhs.uk
audityorkshire@york.nhs.uk

Introduction

NHS organisations have a legal responsibility to protect the Confidentiality, Integrity and Accessibility of personal and sensitive data entrusted to them.

The consequences of a data breach can be significant – fines can be levied by the Information Commissioner's Office, and have increased significantly following the implementation of the General Data Protection Regulation in May 2018. The most serious consequence is to the data subjects; those patients or employees who might be put at risk if their information is compromised, is inaccurate or is inaccessible, potentially resulting in harm.

Organisations protect their systems and data using technological controls, underpinned by robust policies and procedures that set out what their staff should and shouldn't do. Systems and data can also be at risk from an organisation's own workforce. Staff unwittingly cause data breaches by not following proper processes, or not knowing how to identify a phishing email. Cyber-criminals target staff, for example using phishing campaigns, in an attempt to spread a virus or to obtain personal details.

Phishing emails

Phishing emails are increasingly sophisticated, and despite delivering mandatory training to staff, the risk remains that staff are susceptible to clicking a link or providing personal details in response to a phishing email. One way to assess the level of susceptibility is to issue mock-phishing emails, and to measure the response from staff. Findings from our mock-phishing attacks generally highlight an inherent level of susceptibility that organisations should be aware of.

Headline Messages

- Over 560 out of 6,000 individuals targeted in a range of mock phishing campaigns clicked on a link in a phishing email;
- In total, 1,213 "clicks" were registered over the course of the exercises, indicating that a number of recipients had responded multiple times;
- Approximately 200 responses were within 20 minutes of the email being sent, highlighting that IT staff have very little time to identify and respond in the event of a concerted attack against an organisation;
- Half of the individuals targeted (3,000 staff) were invited to provide their login credentials into a fake website. 156 individuals entered their login details;
- Staff are more susceptible to an email with 'personal consequences' – ie more people responded to an email indicating that money would be deducted from their pay, compared to an email purporting to be from IT.
- We conducted the campaigns at four Trusts and noted varying levels of susceptibility. This implies that the risk of exposure to phishing can be influenced by Trusts with appropriate mitigating actions.

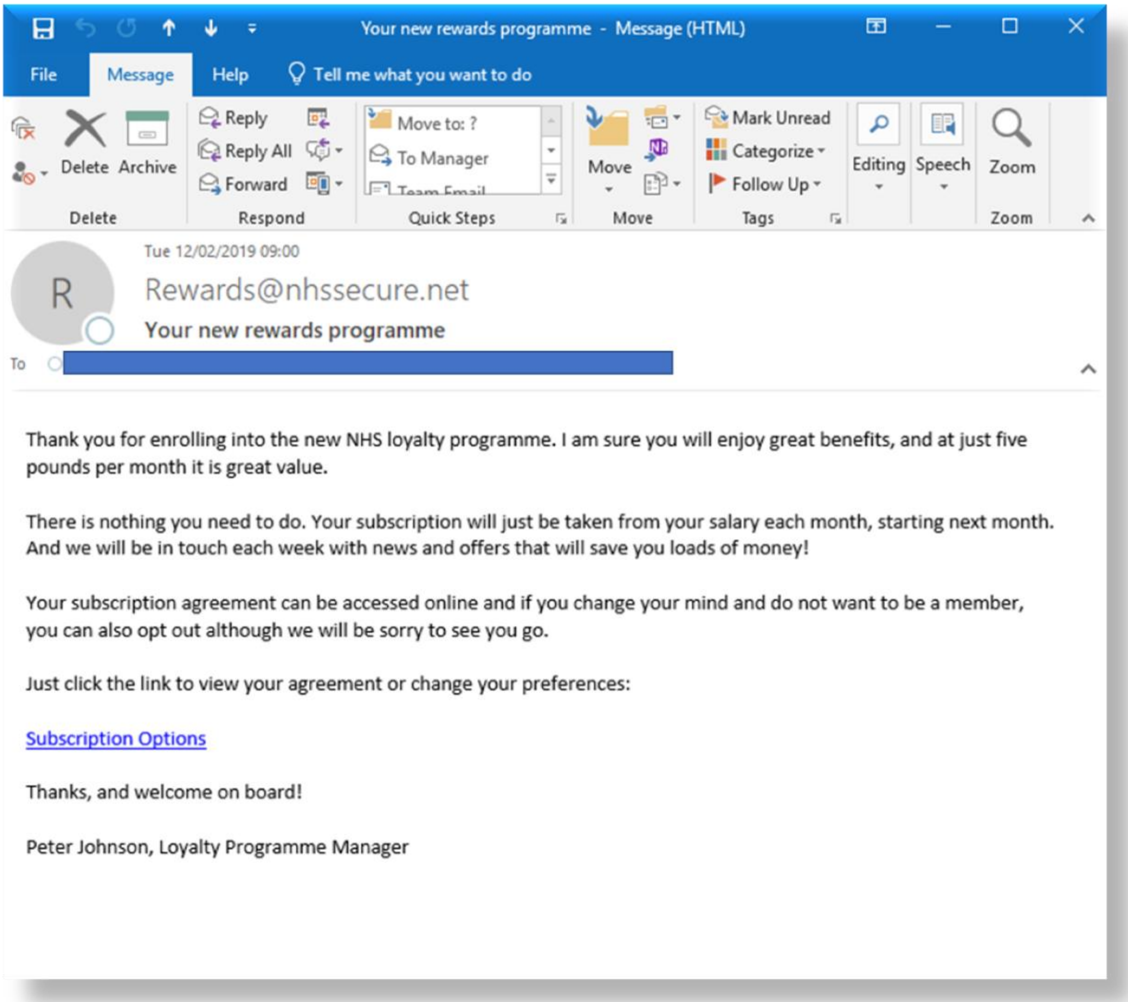
Our Phishing Approach

This paper summarises recent phishing campaigns at four Trusts, each campaign targeting 1,500 staff. Each campaign used two different types of phishing email (each type sent to 750 staff). In total, we targeted 6,000 individual staff members.

We used different campaigns to assess if the level of susceptibility among staff varied depending on the nature of the email. One email indicated that money was to be taken from the recipients' pay, whereas the other was simply an instruction to enable software on their computer.

Hackers will often prey on human emotions such as fear, curiosity and greed, so the suggestion that money could be taken from salary payments was a more personal attack, whereas the instruction to activate software was much more innocuous.

Campaign 1: NHS Rewards Scheme



Tue 12/02/2019 09:00

Rewards@nhssecure.net

Your new rewards programme

To [redacted]

Thank you for enrolling into the new NHS loyalty programme. I am sure you will enjoy great benefits, and at just five pounds per month it is great value.

There is nothing you need to do. Your subscription will just be taken from your salary each month, starting next month. And we will be in touch each week with news and offers that will save you loads of money!

Your subscription agreement can be accessed online and if you change your mind and do not want to be a member, you can also opt out although we will be sorry to see you go.

Just click the link to view your agreement or change your preferences:

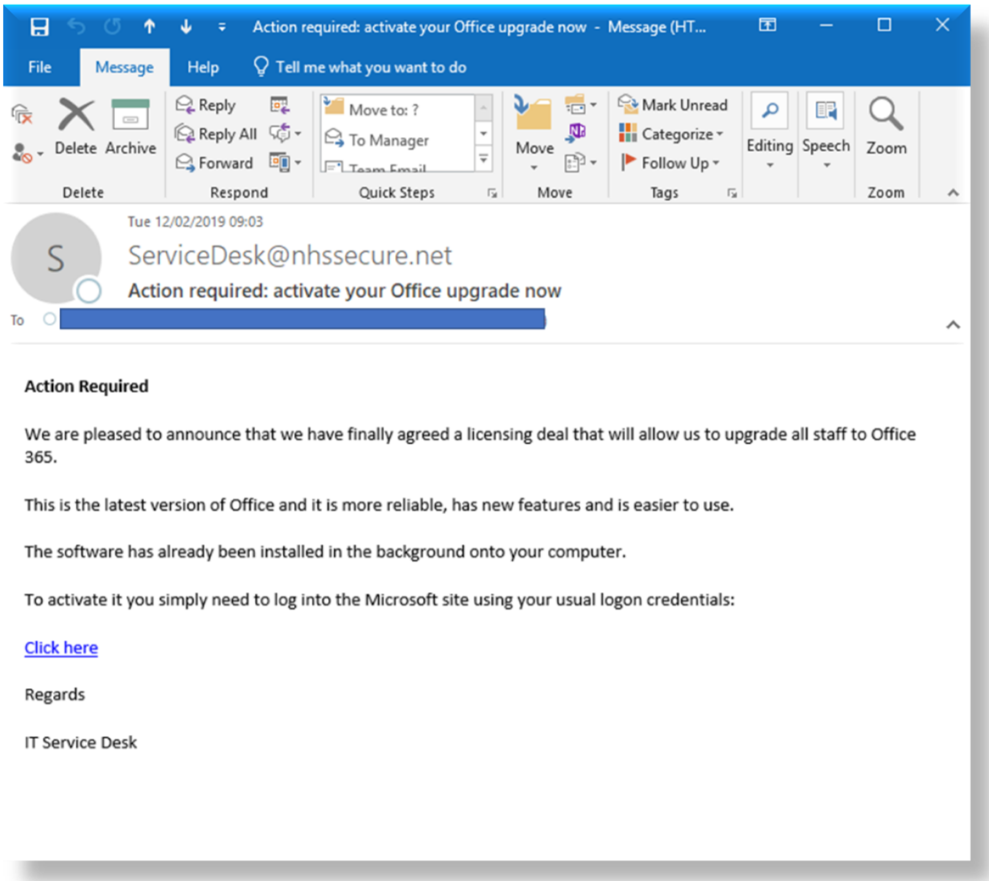
Subscription Options

Thanks, and welcome on board!

Peter Johnson, Loyalty Programme Manager

All Campaign 1 emails were sent out between 08:20 and 09:05.

Campaign 2: Office 365 Upgrade



Tue 12/02/2019 09:03

ServiceDesk@nhssecure.net

Action required: activate your Office upgrade now

To [redacted]

Action Required

We are pleased to announce that we have finally agreed a licensing deal that will allow us to upgrade all staff to Office 365.

This is the latest version of Office and it is more reliable, has new features and is easier to use.

The software has already been installed in the background onto your computer.

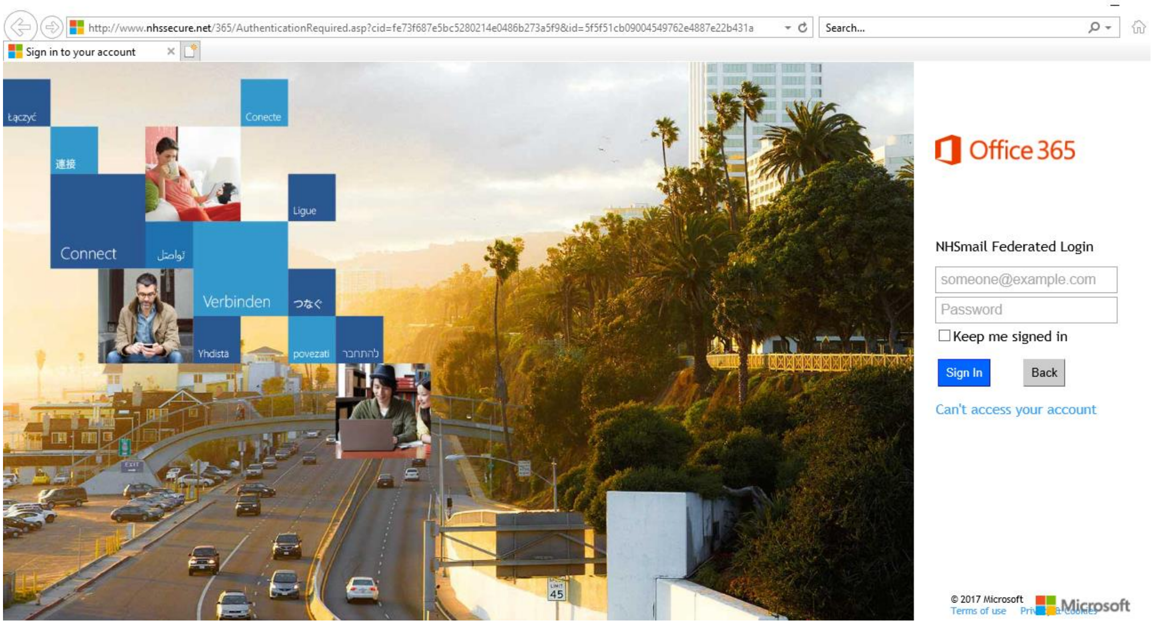
To activate it you simply need to log into the Microsoft site using your usual logon credentials:

Click here

Regards

IT Service Desk

This campaign differed from the first, as not only did it ask staff to click a link, but it then tested whether they were susceptible to disclosing personal details, by asking them to enter a username and password, as indicated in the screenshot below:


http://www.nhssecure.net/365/AuthenticationRequired.asp?cid=fe73f687e5bc5280214e0486b273a5f9&id=5f5f51cb09004549762e4887e22b431a
Search...
Sign in to your account
Łączyć
Conecte
連接
Ligue
Connect
تواصل
Verbinden
つなぐ
Yhdista
povezati
להתחבר
Office 365

NHSmail Federated Login

someone@example.com

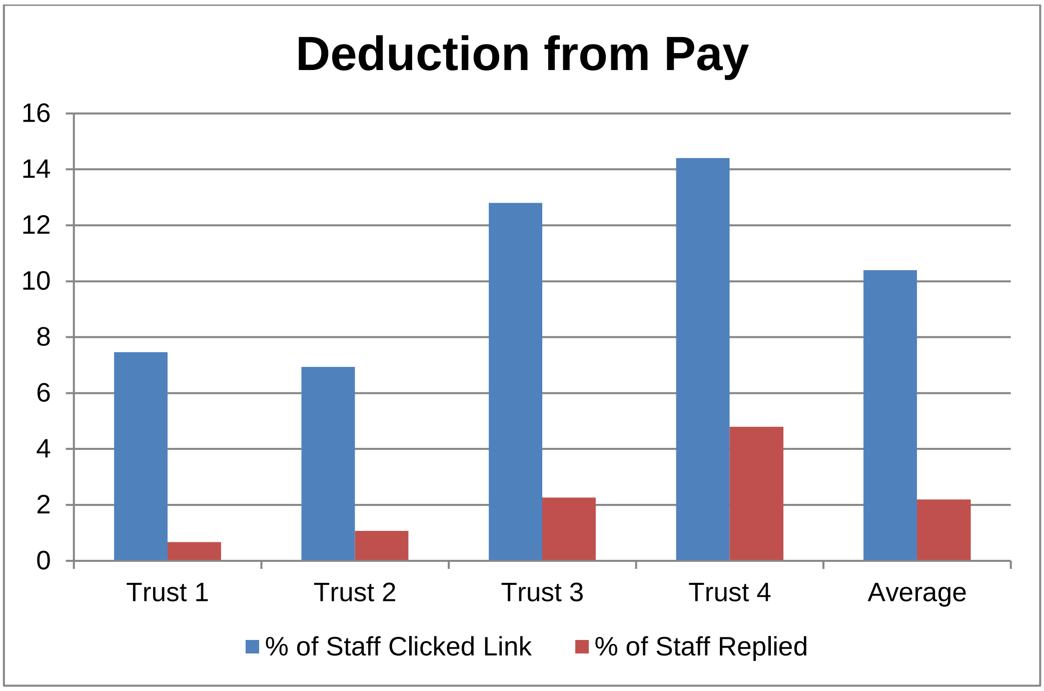
Password

□ Keep me signed in

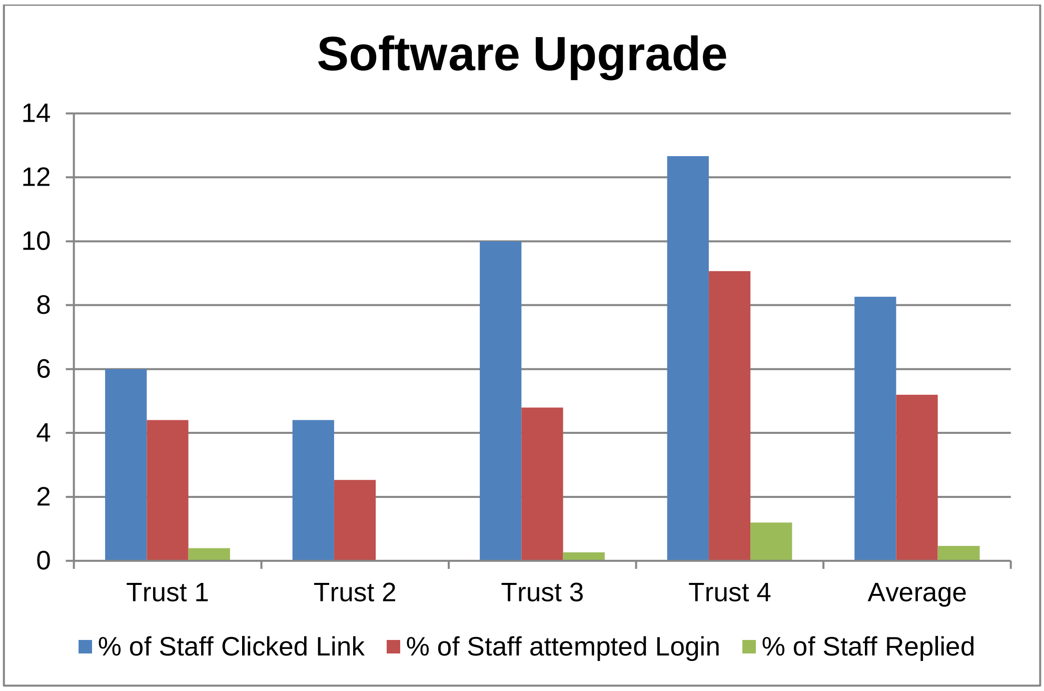
Three of these campaigns took place between 8:20 and 09:05 with a further campaign launched at 15:06.

Results

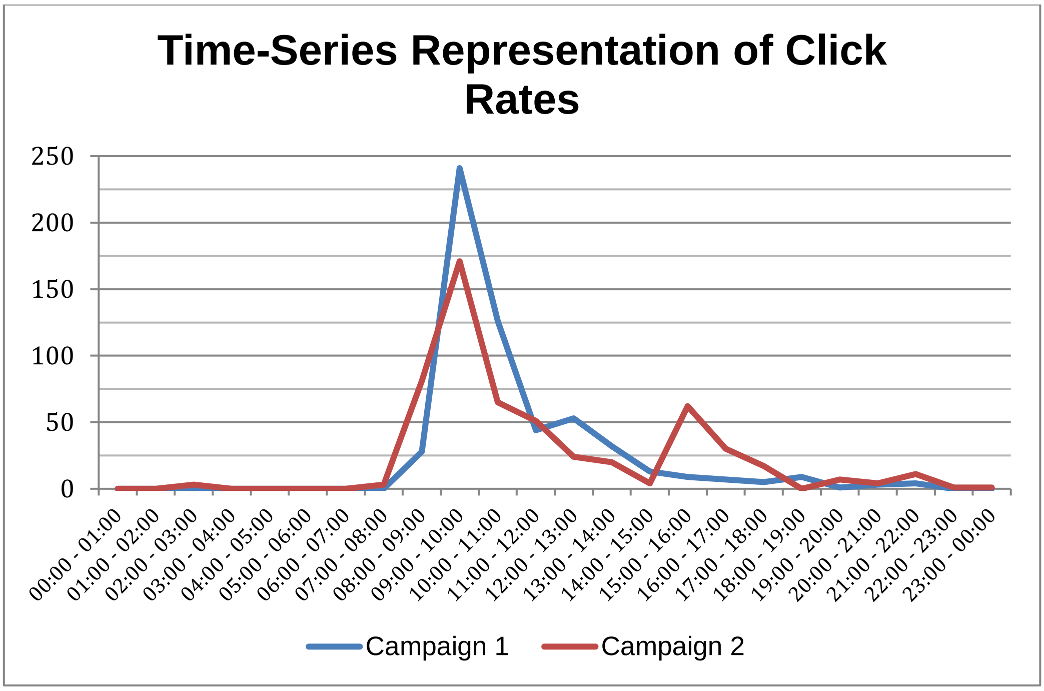
The results of the exercises showed that there a significant proportion of staff who were willing to follow links provided in an email, and even reply.



Campaign 1, focused on NHS pay generated an average response rate of 10.4%.

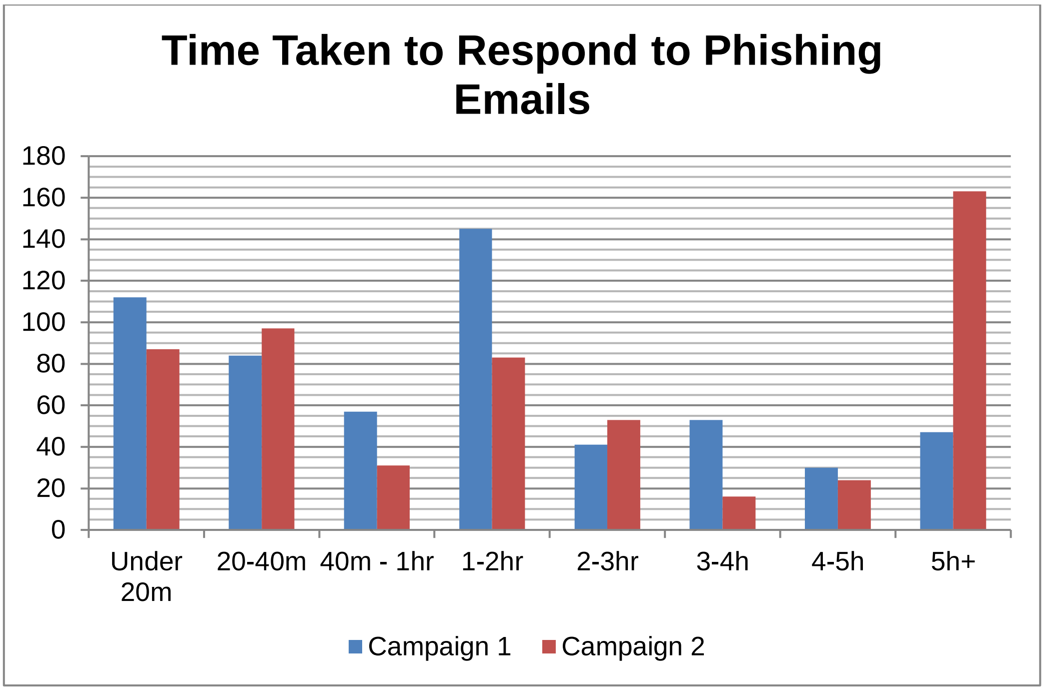


Campaign 2 generated an average response rate of 8.3%. 5.2% of emails resulted in an individual attempting to login to the linked webpage and providing their username and password.



Most responses to the phishing emails are within the first hour of receiving the email, with a small spike corresponding with most lunch breaks.

This is also indicated in the chart below, which shows the time elapsed from the emails being sent, to the point that the user engaged.



The time taken to respond to the phishing emails highlights that a cyber-criminal could quickly gain access to an organisation’s systems. It took less than two minutes for the first user to respond to our campaigns. The number of people responding indicates that, despite the provision of mandatory Information Governance training, there remains an inherent level of susceptibility that could be exploited by cyber-criminals to gain access to systems and data.

Implications and risk exposure

It is helpful to understand the implications for an individual and the organisation when a phishing attack is successful. We have set out some examples, but there are many reasons why hackers might wish to send phishing emails.

Financial gain: a common attack (Wannacry being perhaps the most famous example) is to encrypt a user’s data, demanding a ransom for the encryption to be reversed. Payment is usually demanded using non-traceable crypto currencies. Even where there are robust backups in place, there is a cost associated with the downtime and distress when a user falls victim to such an attack.

Access privileged information: organisations hold sensitive data, including financial records and highly sensitive medical records. A sophisticated hacker might seek to gain access to this information, perhaps by taking control of a user’s computer, or simply recording spyware that captures the user’s actions or what is displayed on their screen. This information, once compromised, has a currency in that it might be used for blackmail, identity theft or other criminal purposes.

Harvest credentials: if a hacker can trick a user into disclosing their username and password, they can use this to access networks, systems and services by masquerading as that user. Many users will use the same password for a number of different systems, so once a password is captured, the hacker might be able to use a user’s email address and password to attempt to gain access to other sites and systems.

If a hacker managed, for example, to obtain the logon details for a senior officer’s NHS.NET account, they could then log onto their email service and send emails from that individual’s account. Such emails might instruct operational staff to raise payments or change bank payment details, and they are less likely to be questioned because they are being sent from the officer’s genuine account.

Hackers might also use compromised accounts to contact a payroll department, asking that a person’s pay is paid to a new bank account. The change would be enacted in good faith, in response to the email from the user’s valid email account.

Revenge: a hacker might not seek personal financial gain, but could simply wish to damage an organisation’s reputation. A disgruntled employee or patient might target Communications staff to trick them into disclosing the credentials for the organisation’s website. This could then be accessed and defaced, causing reputational damage.

In many instances, even where an employee falls for a phishing email, the risk should be mitigated by the firewalls and anti-virus solutions in place. However, if an employee is directed to a fake website and unwittingly gives away their credentials, this is more difficult for an organisation to identify and prevent through technical controls.

Recommended actions for the Audit Committee

What does this mean for the Audit Committee? The Treasury's Audit and Risk Assurance Committee Handbook makes clear that cyber security arrangements should be scrutinised by audit committees:

"*Audit and risk assurance committees' role is to provide assurance to the Board that the organisation is properly managing its cyber risk including appropriate risk mitigation strategies*".

National Audit Office guidance for audit committees sets out three key questions:

- Has the organisation implemented a formal regime or structured approach to cyber security which guides its activities and expenditure?
- How has management decided what risk it will tolerate and how it manages that risk?
- Has the organisation identified and deployed the capability it needs in this area?

Audit Committees should ensure that they have asked – and that they can answer – these three questions. In doing so, we suggest that audit committees also consider:

- The extent of the risk? Following the Wannacry attack, many organisations concluded they had responded well because no data was actually breached. Data subjects' confidentiality was preserved. But if data cannot be accessed when it is needed, this can have serious consequences. Your assessment of risk should consider the confidentiality, integrity and availability of data.
- Is your assurance robust? Historically many organisations have taken assurance that workforce risks are mitigated through mandatory training. The organisations where we ran these campaigns had delivered mandatory Information Governance training to at least 95% of the workforce, yet staff remained susceptible. Whilst mandatory training remains important, it must be accompanied by other training, guidance and communications.

Conclusion and next steps

Our results are consistent with the findings from similar exercises carried out by other NHS Audit organisations. There is a need for ongoing training, advice and communications to ensure that staff can identify and respond appropriately to phishing emails.

One suggested approach is for regular campaigns throughout the year, with the user directed to an eLearning page if they engage with the campaign. This approach provides ongoing information and assurance to the organisation, and ensures that those staff who need further training and support receive it.

We are able to work with you to develop a tailored solution, combining phishing campaigns, awareness training and other tools (surveys and training materials) to support you in driving down the level of susceptibility across your workforce.

If you would like further information or advice relating to the Data Security and Protection Standards, and the assurance services that we can provide, please contact Andy Mellor, Assistant Director, 360 Assurance (andy.mellor@nhs.net), or Tom Watson Internal Audit Manager, Audit Yorkshire (tom.watson@hdft.nhs.uk).