CS2HFS: Human Factors in Security

Design and Evaluation of an Appropriate Cybersecurity Training and Awareness Program

George Hotten (XXXXXX352)

December 11, 2024

Word Count: 2363

Contents

1 Introduction

I have been employed by a local hospital to conduct an in-depth analysis of their security awareness and vulnerability to social engineering attacks. One of the methods I will be using to evaluate the staff at the local hospital will be Social Engineering Penetration Testing. Penetration testing, at its core, is an activity where an authorised professional attempts to find security flaws and vulnerabilities in a system or network. Adding social engineering into the exercise, the authorized professional expands their reach by using the people of the organisation as a method of entry into their systems and networks.

2 Social Engineering Attacks

Lenaerts-Bergmans (2023) explored the most common methods of social engineering that threat actors use to gain access to organisational information and confidential data.

2.1 Phishing

The most used attack is a Phishing attack (Lenaerts-Bergmans, 2023), where an attacker sends a fake email or text message to an employee with the aim to trick them into downloading a malicious file or entering personal credentials into a fake website. Threat actors often choose to pretend being businesses, attempting to lore users into entering their credentials or personal information into a fake form designed to look like the business targeted.

A threat actor could use phishing to evaluate the vulnerabilities of the hospital's employees by sending an email pretending to be a service provider of the hospital, or the management of the hospital. The type of email sent could be fake services such as online payslips or a mandatory password reset to capture login information.

2.2 Whailing

Lenaerts-Bergmans (2023) describes how whaling uses a mix of phishing and direct personal communication, often targeting high-level executives within a business. Whaling often requires extensive background searches and planning to maximise the chances of success. This commonly through information on social media.

This form of attack would not be very suitable for a hospital, as they often have hundreds of staff. This makes this attack not feasible as research into every staff member would be time consuming and impractical.

2.3 Baiting

Baiting is the act of trying to get personal information off a user by giving them false promises. This can be in the forms of 'too good to be true' advertisements or promotions (Lenaerts-Bergmans, 2023). An example of this could require a user to make an account. A poll by Google Haris Poll (2019), showed that 66% of Americans used the same password across multiple online accounts. A threat actor could use the email and password entered from their baiting attack to hack into other online services potentially used by the victim.

This could be useful in the context of the local hospital as staff members could use the same password for the hospital's online services such as emails, patient records, and other sensitive information. A threat actor could attempt to target employees on social media with fake advertisements and promotions to harvest their login information.

2.3.1 Physical Baiting

Another form of baiting is through a physical medium such as USB flash drives (Lenaerts-Bergmans, 2023). At the local hospital a bad actor pretending to a patient could load malware onto a flash drive and attempt to get a member of staff to insert it into a computer stating that it contains photos of an injury, whereas it installs malware into the network.

2.4 Tailgating

Tailgating, as described by Lenaerts-Bergmans (2023) is a physical breach where a threat actor gains access to a restricted area by a nonsuspecting employee holding a door open for them. The threat actor open pretends to be someone else, such as a delivery driver or someone wearing a similar uniform to the site being breached. In the hospital scenario, a threat actor could be dressed in scrubs or in a lab coat. This could allow them to breach a restricted area containing unattended devices or files containing private information about patients.

Compared to the other digital methods, Tailgating has a higher risk involved as hospitals often have site security and CCTV that would expose your identity. For auditing the hospital's staff this would also not be practical as I would have been seen on site and perhaps would have an implicit level of trust within the staff.

2.5 Most Appropriate Attack to Test the Hospital

With technology ever evolving, more organisations will be switching to digital records and removing paper files. Hospitals are no different. With patient records being migrated to a central digital solution, the most appropriate type of social engineering attack to test the hospital's employees would be a phishing attack.

West, et al. (2009) notes just how exploitable humans are: in a study of 512 people who were sent a phising email by a seamingly trusted source, 80% of them fell for the attack and clicked on a malicious link. Data from the Information Commissioner's Office (2023) also shows that 79% of businesses in 2023 had experienced a phishing attack, with 91% of them succeeding.

With 71% of users taking risky action from a phishing attack, and 96% of them knowing that they are being risky (Proofpoint, 2024), it is more important than ever to ensure that the staff at the hospital receive proper and regular training regarding the risks of phishing. It is critical to highlight the importance that the staff are at the front line of security, despite 59% of users being uncertain about if they are (Proofpoint, 2024).

3 Planning the Test Attack

There are many different types of phishing attacks to choose from, such as:

- Spear phishing – attack targeting a single person, often requiring more extensive background research.
- Vishing – "voice phishing", typically done over the phone where a threat actor impersonates someone trusted.
- Email phishing – also known as bulk phishing, where a mass number of emails are sent pretending to be a social media site.
- Evil twin phishing – the act of creating a fake Wi-Fi network in attempt to steal credentials and information.

Data from Proofpoint (2024) shows that in 2023:

- 74% of businesses had an attempted spear phishing attack.
- 67% received an attempted vishing attack.
- 76% received an attempted bulk phishing attack.

Whilst this shows how prevalent these attacks are, the attack that would have the most reach with the least amount of background research would be an email/bulk phishing attack. This attack would allow me to reach most if not all the hospital staff's email inbox and would allow me to fully test the training and awareness of each individual member. 71% of people take risky action online, and with people re-using passwords ranked 2nd of all risky action users take (Proofpoint, 2024), having their password captured could allow a threat actor to easily access other digital services that person uses causing a major risk to information security and confidentiality.

3.1 Information Gathering

Before starting the attack, first we must gather information about the hospital's staff such as their name, email address and position. Corporate websites often provide information such as their staff, job titles, and email contact forms.

3.1.1 Gathering Emails

To figure out staff emails, all you need is to have a single address. This address could be found on the hospital's website, or a web master could be listed in the site's DNS records. For example, we know the email of the director at the hospital: Mark James (mark.james@aston.nhs.uk). From this, we can be certain that the hospital follows the pattern firstname.lastname@aston.nhs.uk. Now we know their email conventions, we can simply search the internet for social media profiles stating that they work at the hospital we are targeting. This could be through LinkedIn, Facebook, Instagram, etc.

We could also find the names of staff to use in the email format by simply observing the hospital. Hospitals often have staff member's names on the doors to their office and names can be said over public-address systems.

In my opinion the easiest and most discreet way to gather names to add to the attack is through social media. LinkedIn allows you to search for people who work at a specific company, and simply searching for that along side common names would quickly yield results. LinkedIn also has privacy features which hides your name from the person you searched for. LinkedIn also states the role you have within the company, so it would be easy to locate high-ranking officials who could have access to more information within the hospital.

3.2 Planning the Attack

As mentioned above, I will be conducting the test via an email phishing attack that I will send to all members of staff who publicly work for the hospital, using the email pattern found and the information from social media.

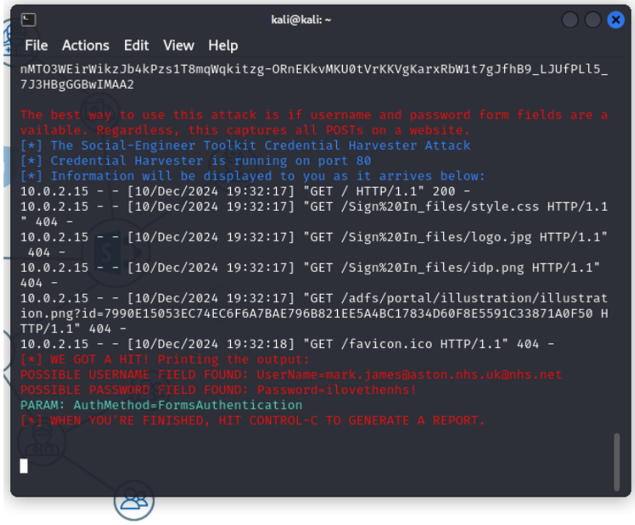
The email format I will use will be in the style of an official NHS email. The email will be regarding an 'urgent action required for your patient' with a link to a fake NHS login screen, where an unsuspecting member of staff would enter their credentials and have them captured.

Watson, et al. (2014) describes how the use of fear and pressure is particularly effective in social engineering. He describes how adding fear into the attack puts the victim into a state of negative emotion. Then the victim should be presented with a way to ease this negative state in a way that would benefit the threat actor.

This research backs up my plan for the contents of my email attack, as the title of ‘urgent action required for your patient’ would put the victim into a fearful and panicked state. With the link to the fake NHS login acting as a way to ease the negative state of emotion. When the victim is in a state of fear, they are less likely to be thinking straight and be paying attention to verify the source of the email. This would then lead to the victim typing in their NHS credentials and having them stolen.

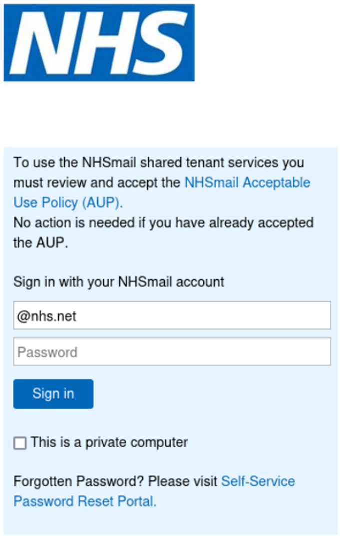
4 Tool Analysis

To execute the attack, I will be using The Social-Engineer Toolkit (SET). SET was a perfect tool for the attack as it provided a simple and easy way to create a fake website that harvests the victim’s credentials. I downloaded the NHS’ webmail login page and imported it into SET, which modified the HTML to send the login POST requests to a local server where the credentials can be extracted. The victim is then redirected to the real NHS webmail site as if nothing happened. SET also exports all found credentials into an XML file, allowing for easy access. The easy access is crucial in a phishing attack as it is important to act fast when credentials are harvested as users or their IT department may start to catch on that a breach has occurred, especially on large scale attacks.



```
nMTO3WEirWikzJb4kPzs1T8mqWqkitzg-ORnEKkvMKU0tVrKKVgKarxRbW1t7gJfhB9_LJUfPLl5_
7J3HBgGGBwIMAA2

The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [10/Dec/2024 19:32:17] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [10/Dec/2024 19:32:17] "GET /Sign%20In_files/style.css HTTP/1.1
" 404 -
10.0.2.15 - - [10/Dec/2024 19:32:17] "GET /Sign%20In_files/logo.jpg HTTP/1.1"
 404 -
10.0.2.15 - - [10/Dec/2024 19:32:17] "GET /Sign%20In_files/idp.png HTTP/1.1"
404 -
10.0.2.15 - - [10/Dec/2024 19:32:17] "GET /adfs/portal/illustration/illustrat
ion.png?id=7990E15053EC74EC6F6A7BAE796B821EE5A4BC17834D60F8E5591C33871A0F50 H
TTP/1.1" 404 -
10.0.2.15 - - [10/Dec/2024 19:32:18] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: UserName=mark.james@aston.nhs.uk@nhs.net
POSSIBLE PASSWORD FIELD FOUND: Password=ilovethenhs!
PARAM: AuthMethod=FormsAuthentication
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



To use the NHSmail shared tenant services you must review and accept the NHSmail Acceptable Use Policy (AUP).
No action is needed if you have already accepted the AUP.

Sign in with your NHSmail account

@nhs.net

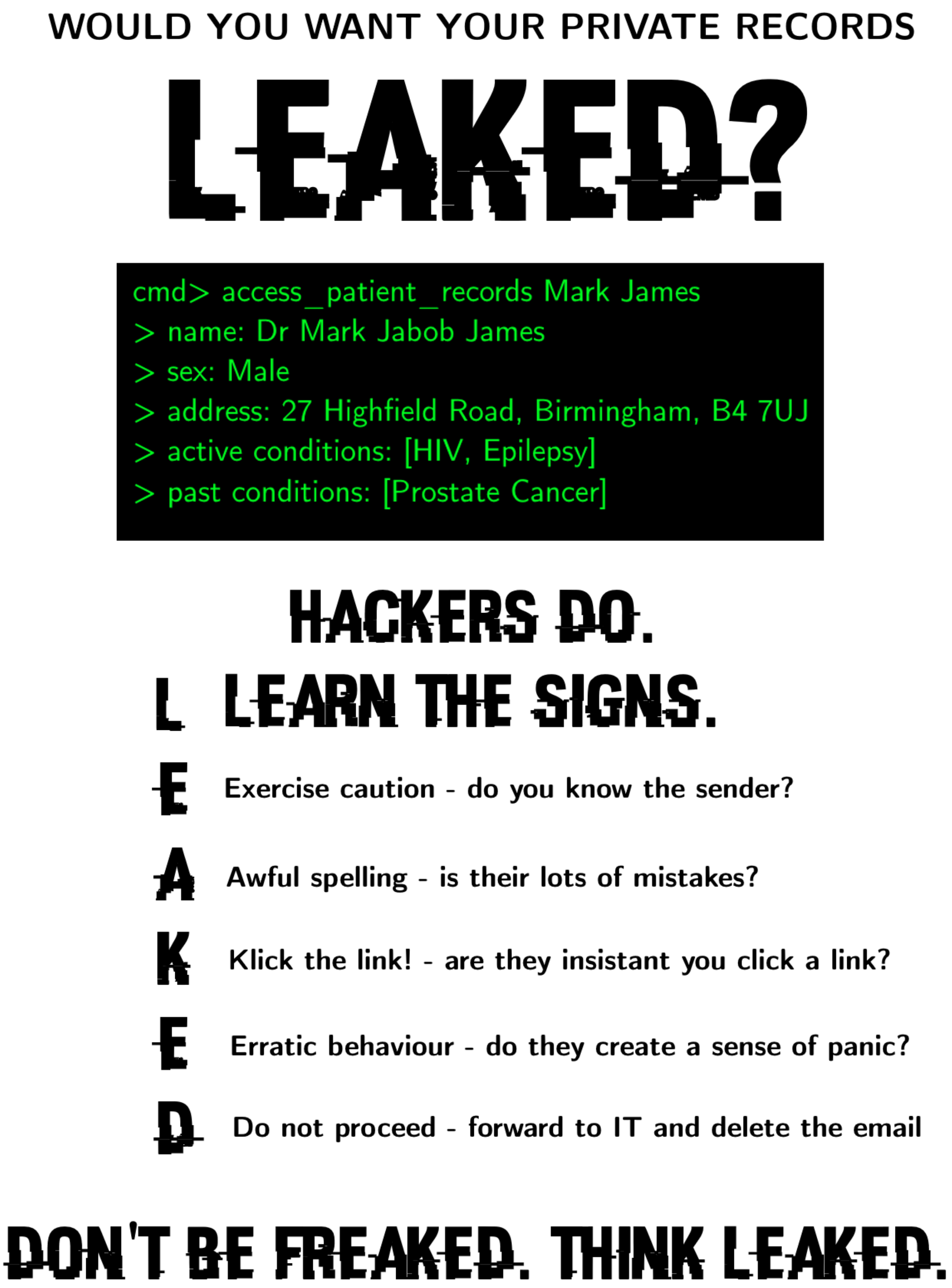
Password

□ This is a private computer

Forgotten Password? Please visit Self-Service Password Reset Portal.

Through SET, I used the following menu options: Social Engineering Attack, Website Attack Vectors, Credentials Harvester Attack Method, and finally Custom Import.

5 Cyber Awareness Strategy



WOULD YOU WANT YOUR PRIVATE RECORDS

LEAKED?

```
cmd> access_patient_records Mark James
> name: Dr Mark Jabob James
> sex: Male
> address: 27 Highfield Road, Birmingham, B4 7UJ
> active conditions: [HIV, Epilepsy]
> past conditions: [Prostate Cancer]
```

HACKERS DO.

L LEARN THE SIGNS.

E Exercise caution - do you know the sender?

A Awful spelling - is their lots of mistakes?

K Klick the link! - are they insistant you click a link?

E Erratic behaviour - do they create a sense of panic?

D Do not proceed - forward to IT and delete the email

DON'T BE FREAKED. THINK LEAKED.

5.1 The Vision

The goal when designing the awareness poster was to make it as simple as possible whilst also keeping it highly effective. Jurkonytė (2024), notes how "Colour contrast is one of the most effective tools for boosting your design and making particular elements stand out." With this knowledge, I designed the poster to be white with a black and green section to standout, grabbing the attention of employees passing by.

The poster also installs fear into employees by making them aware of the risks their actions can have whilst being on the internet. I chose to create an acronym out of the word LEAKED. This acronym highlights the signs of phishing attacks. As explored previously, attackers can use fear or panic as an effective way to phish people, so included in the poster is the slogan "Don't be freaked, think leaked", referring to the acronym of spotting the signs. It also has a subtle spelling mistake on the "Awful spelling", further highlighting the signs of a phishing attack and the importance of carefully reading emails.

6 Best Cyber Hygiene Practice: Access Control

Access Control is a crucial aspect in best cyber practices as it is the often the last line of defence on a network. When access control is breached, an attacker will gain full control of that user account and all data it has access to. This is the aim of a threat actor when they perform attacks such as a phishing attack. In my test attack on the hospital, my aim was to breach their access control and gain access to confidential information, such as patient records.

There are multiple ways to prevent access control related attacks. A study by Meyer, et al. (2023) found that Microsoft Active Directory Users' accounts that used a form of multifactor authentication (MFA) reduced the risk of comprise by 99.22%, and for leaked credentials the risk was reduced by 98.56%. This data clearly shows the huge benefit of using MFA to reduce the effectiveness of a phishing attack. With MFA enabled, even if a threat actor harvests your credentials, they will not be able to access your account, and any confidential information will remain secure. Risk based MFA is also an effective method, which prompts for MFA when suspicious activity is noticed, such as a user attempting to login from a different country despite them not having enough time to get there from their last activity (Microsoft, 2024).

Combined with MFA, another way to prevent access control attacks is to disable password rotations (for example, a user must change their password every month). Microsoft (2024) notes how rotating passwords encourage users to create predictable and repetitive passwords that are all related to each-other. Often a new password can be predicted from an old one. For example, if a leaked password was "January27", you could assume the new password is "January28".

6.1 Cybersecurity Policies for the Hospital

With access control in mind, I have drafted 3 important cybersecurity policies for the hospital:

- Enforce multifactor authentication – all users must use a form of MFA, such as a text message or entering numbers in an app.
- Risk based MFA – enforce extra checks if suspicious activity is detected, such as logging in from another country despite not having enough time to get there.
- Password strength – all users must create a strong password that the user can remember, ideally with a mix of letters numbers and symbols.

7 References

Google & Harris Poll, 2019. *The United States of P@ssw0rd$.* Available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf
(Accessed 02 December 2024).

Information Commissioner's Office, 2023. *Learning from the mistakes of others – A retrospective review.* Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/
(Accessed 03 December).

Jurkonytė, D., 2024. *How Eye-Catching Colors Attract Users' Attention.* Available at: https://attentioninsight.com/eye-catching-colors/
(Accessed 11 December 2024).

Lenaerts-Bergmans, B., 2023. *10 Types of Social Engineering Attacks and How to Prevent Them.* Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/
(Accessed 02 December 2024).

Meyer, L. A. et al., 2023. *How effective is multifactor authentication at deterring cyberattacks?*, s.l.: arXiv preprint arXiv:2305.00945.

Microsoft, 2024. *Password policy recommendations for Microsoft 365 passwords.* Available at: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations
(Accessed 11 December 2024).

Proofpoint, 2024. *2024 State of the Phish.* Available at: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf
(Accessed 03 December 2024).

SafeAeon, 2024. *Exposing the Threat: Understanding Evil Twin Attack.* Available at: https://www.safeaeon.com/security-blog/evil-twin-attack/
(Accessed 04 December 2024).

Watson, G., et al., 2014. The Techniques of Manipulation. In: *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense.* s.l.:Syngress, pp. 39-63.

West, R., Mayhorn, C., Hardee, J. Mendel, J., 2009. The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions. *In: Social and Human Elements of Information Security: Emerging Trends and Countermeasures.* s.l.:IGI Global, pp. 43-60.