CMP417 - Engineering Resilient Systems 1
Human-Centred Security

Jack Bowker - 1803838

May 2021

ABSTRACT

This report is a short look into different Security Awareness measures that could be adopted by a small company, whose IT infrastructure and employees are being targeted with phishing emails by a hacktivist group. The background covers a dive into literature regarding how phishing can be a security risk to the company, as well as showing real life examples and how awareness can be raised. The Recommendations section will cover the suggestion of implementing automated email filtering and fake phishing being used as a training method. As well as this, security keys will be recommended to enhance the existing password system. The Experiment section will go over evaluating these new systems, and Challenges will cover the possible issues these solutions may present.

1. Background

This paper will provide security recommendations for a small company, who after experiencing threats of a cyber-attack from a hacktivist group are looking to improve their overall security posture. This follows on from a review carried out on possible machine learning solutions that could help the company monitor their network traffic. This report will review literature regarding phishing and its impact, as well as recommending mitigations to improve the company's security.

The following literature was reviewed to evaluate the security implications of phishing attacks and explore how untrained and irresponsible employees can present a risk to the company.

The term "Insider threat" can refer to both malicious actors inside an organization as well as well-intentioned employees that, due to a lack of education or care, end up helping malicious external actors. CERT Insider Threat Team, (2014) refers to these actors as an Unintentional Insider Threat (UIT). It finds that UITs are often exploited in order to carry out credential theft of usernames & passwords to sensitive systems. It also finds that in the majority of cases phishing is used as part of a multi-stage attack, where after gaining access attackers will "gather intelligence about the compromised systems or networks, and use the information to cause harm or develop subsequent spear phishing messages", as shown in Figure 1.

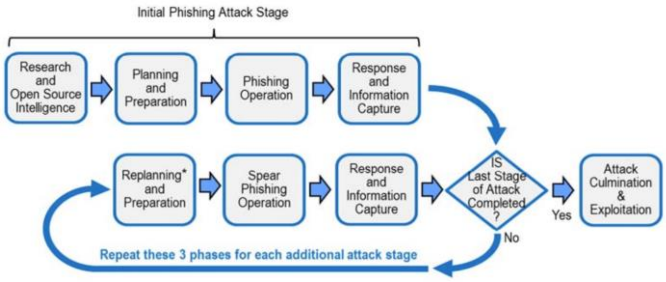
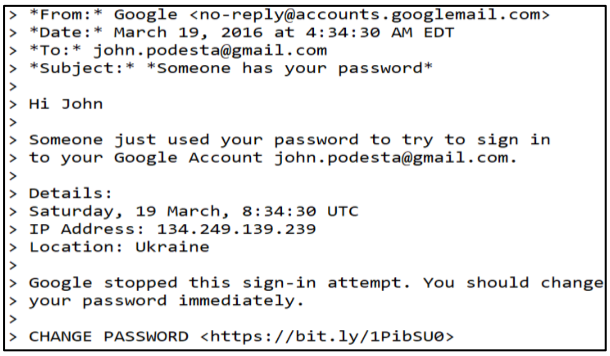

Initial Phishing Attack Stage
Research and Open Source Intelligence
Planning and Preparation
Phishing Operation
Response and Information Capture
Replanning* and Preparation
Spear Phishing Operation
Response and Information Capture
IS Last Stage of Attack Completed ?
Yes
No
Attack Culmination & Exploitation
Repeat these 3 phases for each additional attack stage

Figure 1 - Workflow diagram for multi-stage attack (CERT Insider Threat Team, 2014)

Verizon, (2020)'s Data Breach Investigations Report analysed over 150,000 security incidents to build a collection of statistics that can inform businesses of current threat trends. It details that phishing is the most popular of many "threat actions", used as part of a wider attack strategy with 94% of malware delivered via the opening of an untrusted email attachment. As well as this, it was found that 80% of hacking-related breaches took advantage of compromised or weak passwords. This issue is made worse by the fact that according to a 2019 study by Google, 52% of people reuse their passwords across multiple accounts, with 13% of people using the same password across all their accounts (Google, 2019). This reality enables malicious actors to use "credential stuffing", a technique involving attackers using lists of previously compromised login credentials to breach into a system (OWASP Foundation, 2021).

In 2016, the Democratic Party of the USA was targeted by a successful phishing campaign. This involved John Podesta being forwarded a "Password reset" email as shown in Figure 2 (Lipton, Sanger and Shane, 2016) to his private Gmail account, which was not protected by Multi-Factor Authentication (MFA). This slip-up resulted in Russian hackers gaining access to over 60,000 sensitive emails for almost 7 months.



```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* john.podesta@gmail.com
> *Subject:* *Someone has your password*
>
> Hi John
>
> Someone just used your password to try to sign in
> to your Google Account john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change
> your password immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
```

Figure 2 - Illegitimate password reset email

This incident demonstrates the importance of having multiple factors of authentication in place.

Abhishek *et al.*, (2013) goes over different methods used in Multi-Factor Authentication in a literature study, including different implementations of “Something you know”, “Something you have”, “Something you are” and “Somewhere you are/Someone you know”. The paper references Table 1, where One Time Passwords are measured for their effectiveness against different attacks and overall usability.

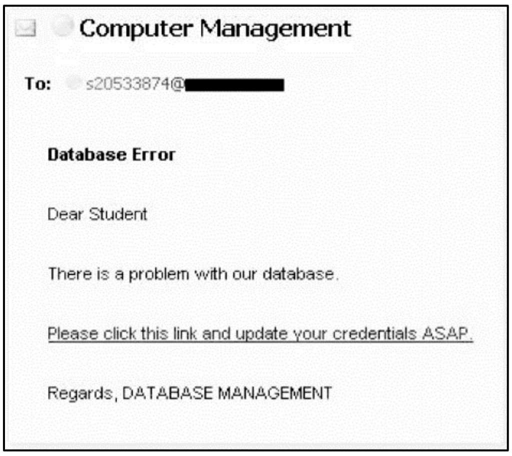
Table 1 - Different aspects of OTP (GPayments, 2006)

Protection against Passive Attacks	HIGH
Protection against Active Attacks	LOW to MEDIUM
Initial Cost Involved	MEDIUM
Support and Usage Costs	LOW to NONE
Ease of Use	MEDIUM
Portability	HIGH
Special Software for client required	MOSTLY NO

It’s concluded that multiple factors are essential for use in any application that wishes to achieve strong authentication.

Security keys are another form of MFA, where a physical USB device is plugged in to the system being accessed, sometimes as well as a traditional password. In early 2017, Google rolled out security keys to more than 85,000 of their employees, with not a single instance of phishing reported since they were implemented (KrebsOnSecurity, 2018).

In a case study of an institution in South Africa, Jansson and Solms, (2013) designed a campaign of simulated phishing emails and embedded training in order to raise awareness of the dangers of clicking unknown links. Emails were crafted and sent out to students, with a red warning presented to users that clicked the link notifying them of their insecure behaviour. These warning screens also linked to a voluntary awareness training programme as shown in Figure 3.



Computer Management

To: s20533874@[redacted]

Database Error

Dear Student

There is a problem with our database.

Please click this link and update your credentials ASAP.

Regards, DATABASE MANAGEMENT

Figure 3 - Database Crash phishing email

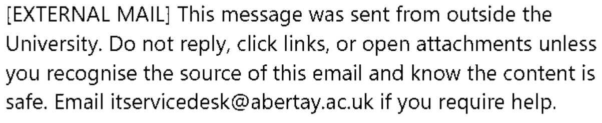
Although at first the emails had a high clickthrough rate, after two weeks, the emails received 42% less reactions than at first. It was concluded that the simulated attacks when integrated with training was an effective way to cultivate resistance to phishing campaigns.

Scholefield and Shepherd, (2019) of the University of Abertay investigate another method of raising security awareness. Security gamification was investigated - a method of learning through play. Users played through a role-playing quiz, answering questions related to password security in order to progress through the game, using the game elements of HP (health points) and time limits. After this, they were surveyed on their feedback, and it was found that overall participants enjoyed the exercise, with a majority Agreeing with the statement

“The password security game helped increase your knowledge on password security”.

2. Recommendations

There are many existing automated solutions that can assist with preventing phishing attacks reaching employee inboxes. Using heuristic methods, the source of the email (domain, TLS status, WHOIS information etc.) can be analysed and a decision can be made based on a trust factor. As well as this, solutions involving Machine Learning that analyse the language and wording used in previous phishing emails. This involves the fact they’re often misspelled, or intended to incentivise fast action without thinking by using harsh language (SSLStore, 2017) as shown in Figure 2 and Figure 3 with the words “imminently” and “ASAP”. These methods both improve resilience against phishing attacks as they reduce the likelihood of malicious emails reaching the end user. Appending external emails to notify users, as shown in Figure 4 can also be a useful way to make users more apprehensive of opening links, however if the majority of email the employee deals with is external, it may quickly fade into the background.

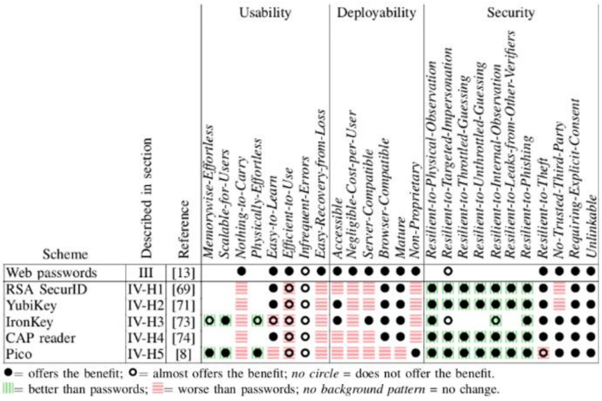


[EXTERNAL MAIL] This message was sent from outside the University. Do not reply, click links, or open attachments unless you recognise the source of this email and know the content is safe. Email itservicedesk@abertay.ac.uk if you require help.

Figure 4 - University of Abertay external notice

Although automated solutions are valuable for reducing the number of attacks employees will have to deal with, employees must be educated on the dangers of phishing and the methods used to detect and report them. A valuable method that can be used both to raise and track employee awareness is to use phishing attack simulation, where fake phishing emails are sent to employees that can be catered to the company. As described in the previous literature review, it was found to be effective after only two weeks. Open source solutions such as GoPhish (*Gophish*, no date) can be integrated with existing email systems, so campaigns can be rolled out based on the level and types of phishing campaigns the company is experiencing. It’s also important to integrate learning material here so employees don’t feel as if they’re punished for clicking these links, instead providing learning materials taking advantage of techniques such as gamification, as explained in the literature review.

As shown throughout this review, password-based authentication has the flaw of being a single point of failure, as well as employees often reusing passwords that have been previously compromised. A solution to this would be for the company to integrate a Multi-Factor Authentication system. Recent protocol standardization under the FIDO U2F standard (FIDO Alliance, no date) as well as support inside Windows and most web browsers has reduced the complexity of implementing physical security in the company’s infrastructure. The implementation of this would differ slightly based on the company’s specific infrastructure but would involve giving employees a small USB device that employees would be prompted to plug in after entering their traditional password. As shown in the abbreviated Figure 5, compared to passwords physical keys score very highly with regards to Security, but fall behind in terms of Usability and Deployability. It’s important however that compared to other methods included in this matrix, keys are most often used as a second authentication method and include methods for backing up and resetting in case of lost or theft.

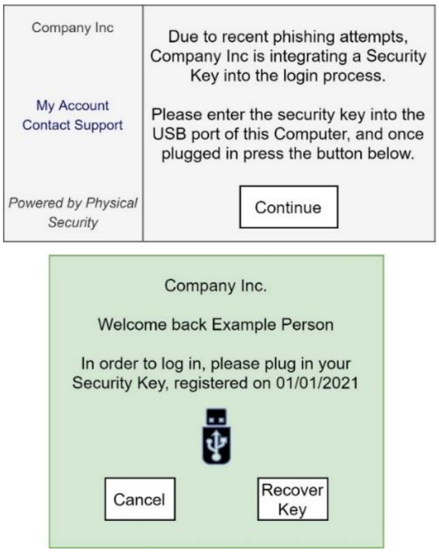


			Usability								Deployability						Security										
Scheme	Described in section	Reference	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Resilient-to-Physical-Observation	Resilient-to-Targeted-Impersonation	Resilient-to-Throttled-Guessing	Resilient-to-Unthrottled-Guessing	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
RSA SecurID	IV-H1	[69]			🟥		●	🟥○	○	🟥	🟥	🟥	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	🟥	●	●
YubiKey	IV-H2	[71]			🟥		●	🟥○	○	🟥	●	🟥	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	🟥	●	●
IronKey	IV-H3	[73]	🟩○	🟩●	🟥	🟩○	🟥○	🟥○	○	🟥	●	🟥	●	●	●	🟥	🟩●	○			🟩○		🟩●	●	●	●	●
CAP reader	IV-H4	[74]			🟥		●	🟥○	○	🟥	🟥	🟥	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	●	●	●
Pico	IV-H5	[8]	🟩●	🟩●	🟥	🟩●	🟥	🟥○	○	🟥	🟥	🟥	🟥	🟥	🟥	●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟥○	●	●	●

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
🟩= better than passwords; 🟥= worse than passwords; *no background pattern* = no change.

Figure 5 - Usability matrix (Bonneau et al., 2012)

Figure 6 demonstrates a proof of concept interface for employees once they receive a security key, as well as the process after login where the key is presented.



Company Inc

My Account
Contact Support

Powered by Physical Security

Due to recent phishing attempts, Company Inc is integrating a Security Key into the login process.

Please enter the security key into the USB port of this Computer, and once plugged in press the button below.

Continue

Company Inc.

Welcome back Example Person

In order to log in, please plug in your Security Key, registered on 01/01/2021

Cancel

Recover Key

Figure 6 - Proof of concept design of security key enrolment and authentication ceremony

3. Experiment

It's important that the recommended solutions are evaluated to ensure that they are effective and are working as intended.

Automated spam detection could be evaluated by finding the accuracy rate, measuring emails incorrectly marked as phishing or non-phishing. In order to evaluate this, the company should measure any spam/discarded message folders, taking note of any legitimate messages that were incorrectly marked. In order to find phishing emails that still got through, employees should be encouraged to forward suspicious messages to a dedicated company address, where the email could be investigated and either added to the false negative count or marked as innocent.

Similar evaluation could be carried out on the security awareness training, by tracking the percentage of employees falling for the training exercises. Importantly however, interaction rate with training material should also be measured to ensure that employees aren't just clicking off once they've realised they've fallen for it. Training can be incentivised by making challenges more fun and offering, for example, prizes for employees that finish X number of levels.

Although technically secure, the efficacy of a Multi-Factor security key depends on users being able to understand and operate it effectively. The usability of such as a solution could be carried out via interviewing users, by giving them a realistic scenario that allows them to evaluate the system as they would use it every day. A specific goal should be given, for example "Set up this security key and log in", and verbal feedback from test participants should be noted, to act as qualitative feedback. After this, a System Usability Scale (Affairs, 2013) could be given for participants to gather a bigger picture in quantitative form. Depending on how many employees are available, 5 at a minimum should be used as it's been studied by Virzi, (1992) that 80% of usability issues are detected with 4-5 participants.

4. Challenges

Although the company could greatly increase their security posture by implementing these steps, the changes need to be embraced by employees in order to make a difference.

Phishing email challenges can be a useful tool to train employees on what to look out for, however this material would need to be maintained and updated regularly so employees wouldn't just learn which ones the company sent out. On the other hand, employees shouldn't be punished for failing to detect that the email wasn't legitimate, as NCSC explains "Training should aim to improve your users' confidence and willingness to report future incidents" (NCSC, 2018).

An obvious challenge involving security keys is that they are small and easy to lose, therefore a robust backup and replacement solution would need to be implemented alongside this method. As well as this, checks would need to be carried out that employees use devices that support the physical key, with legacy Operating Systems often unsupported.

References

Abhishek, K. *et al.* (2013) 'A Comprehensive Study on Multifactor Authentication Schemes', in Meghanathan, N., Nagamalai, D., and Chaki, N. (eds) *Advances in Computing and Information Technology*. Berlin, Heidelberg: Springer (Advances in Intelligent Systems and Computing), pp. 561–568. doi: 10.1007/978-3-642-31552-7_57.

Affairs, A. S. for P. (2013) *System Usability Scale (SUS)*. Department of Health and Human Services. Available at: system-usability-scale.html (Accessed: 26 April 2021).

Bonneau, J. *et al.* (2012) 'The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes', *IEEE Symp. on Security and Privacy*, pp. 553–567. doi: 10.1109/SP.2012.44.

CERT Insider Threat Team (2014) *Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector*. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=297771 (Accessed: 10 May 2021).

FIDO Alliance (no date) 'FIDO Alliance Specifications Overview', *FIDO Alliance*. Available at: https://fidoalliance.org/specifications/ (Accessed: 11 May 2021).

Google (2019) *Online Security Survey*. Available at: https://services.google.com/fh/files/blogs/google_security_infographic.pdf (Accessed: 11 May 2021).

Gophish (no date) *Open Source Phishing Framework*. Available at: https://getgophish.com/ (Accessed: 11 May 2021).

GPayments (2006) *Two-Factor Authentication: An essential guide in the fight against Internet fraud*. Available at: https://www.gpayments.com/Portals/0/pdfs/WHITEPAPER_2FA-Fighting_Internet_Fraud.pdf (Accessed: 11 May 2021).

Jansson, K. and Solms, R. von (2013) 'Phishing for phishing awareness', *Behaviour & Information Technology*, 32(6), pp. 584–593. doi: 10.1080/0144929X.2011.632650.

KrebsOnSecurity (2018) 'Google: Security Keys Neutralized Employee Phishing – Krebs on Security'. Available at: https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/ (Accessed: 11 May 2021).

Lipton, E., Sanger, D. E. and Shane, S. (2016) 'The Perfect Weapon: How Russian Cyberpower Invaded the U.S.', *The New York Times*, 13 December. Available at: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html (Accessed: 10 May 2021).

NCSC (2018) *Phishing attacks: defending your organisation*. Available at: https://www.ncsc.gov.uk/guidance/phishing (Accessed: 11 May 2021).

OWASP Foundation (2021) *Credential stuffing Software Attack | OWASP Foundation*. Available at: https://owasp.org/www-community/attacks/Credential_stuffing (Accessed: 11 May 2021).

Scholefield, S. and Shepherd, L. A. (2019) 'Gamification Techniques for Raising Cyber Security Awareness', in Moallem, A. (ed.) *HCI for Cybersecurity, Privacy and Trust*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 191–203. doi: 10.1007/978-3-030-22351-9_13.

SSLStore (2017) 'Study: The most effective phishing emails create a sense of urgency', *Hashed Out by The SSL Store^{TM}*, 12 October. Available at: https://www.thesslstore.com/blog/study-effective-phishing-emails-create-sense-urgency/ (Accessed: 11 May 2021).

Verizon (2020) *2020 Data Breach Investigations Report, Verizon Enterprise*. Available at: https://enterprise.verizon.com/en-gb/resources/reports/dbir/ (Accessed: 9 May 2021).

Virzi, R. A. (1992) 'Refining the Test Phase of Usability Evaluation: How Many Subjects Is Enough?', *Human Factors*, 34(4), pp. 457–468. doi: 10.1177/001872089203400407.