Appendix One A

Simulated Phishing - Training Exercise 2019/20

Allerdale Borough Council

MIAA ASSURANCE

Introduction and Background

- Phishing is a type of social engineering attack that aims to influence users to disclose credentials, sensitive information, or introduce malware to a host device or system by creating a plausible, yet malicious scenario.
- Although social engineering can be conducted via social media, a phone call or text message, phishing is most strongly associated with emails.
- It relies upon human errors and system vulnerabilities to successfully obtain credentials/data and/or to deliver a malicious payload such as ransomware/malware.
- Delivery via email is straightforward, hitting high numbers of non-specifically targeted mailboxes at minimal cost.
- Alternatively and often more successfully, targeted attacks can be focused on particular individuals, organisations or sectors with emails crafted to appear legitimate or internally delivered.
- Often a single success is all that is needed to expose the target organisation to the malicious activity.

Objectives & Scope

The objective was for MIAA to conduct an e-mail phishing exercise to test the technical and human controls around cyber security within the organisation and to:

- Report on results from the recent phishing awareness exercise;
- Identify any wider lessons learnt and / or opportunities for the future; and,
- Provide a benchmark baseline for a potential future Cyber Security Awareness Plan / Campaign.

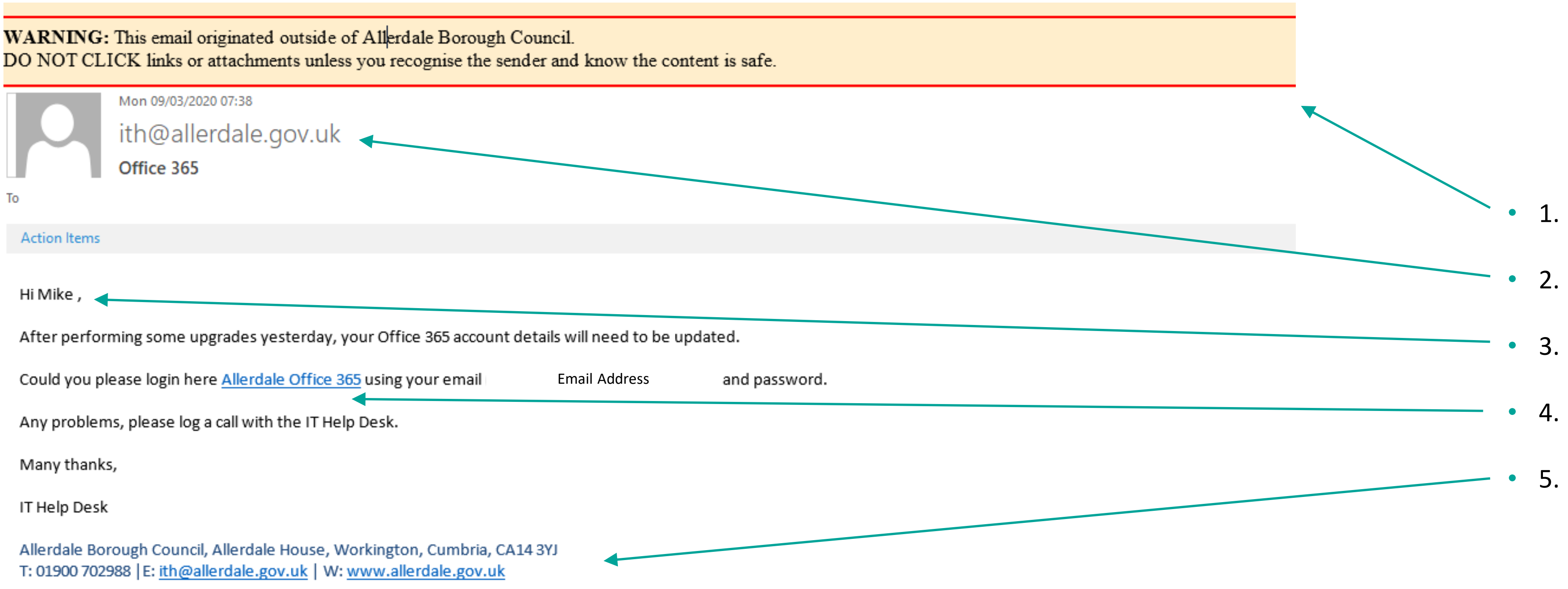
Approach

The approach was to deliver a sophisticated phishing email to all staff (employees and members) requesting them to click on a link and enter their logon credentials. This was approved by and agreed with the knowledge and cooperation of the IT Department and the Assurance, Risk and Audit Manager.

The email was sent from ith@allerdale.gov.uk, and due to a recent upgrade of Office 365, asked users to click on the link to update their account details.

- The URL users were encouraged to click on looked similar to Allerdale council’s e.g. http://www.allerdale-gov.uk/?rid=32c9zrU. If clicked, the link took the user to a copy of Microsoft Office 365’s login page.
- If credentials were entered, the page simply redirected the user to the official Office 365 logon page.
- Only the username/email address was captured as part of the exercise (no passwords were captured as part of the simulation).
- The approach was designed as a sophisticated hoax and had the potential to be used for malicious purposes, such as to harvest credentials or download a malicious payload, etc.

Simulated Phishing Email Example



WARNING: This email originated outside of Allerdale Borough Council.
DO NOT CLICK links or attachments unless you recognise the sender and know the content is safe.

Mon 09/03/2020 07:38
ith@allerdale.gov.uk
Office 365

To

Action Items

Hi Mike ,

After performing some upgrades yesterday, your Office 365 account details will need to be updated.

Could you please login here [Allerdale Office 365]() using your email Email Address and password.

Any problems, please log a call with the IT Help Desk.

Many thanks,

IT Help Desk

Allerdale Borough Council, Allerdale House, Workington, Cumbria, CA14 3YJ
T: 01900 702988 | E: ith@allerdale.gov.uk | W: www.allerdale.gov.uk

There were two aspects of this email that would have indicated that this was a potential phishing email, (4) Hovering over the hyperlink would have displayed a URL similar to http://www.allerdale-gov.uk/?rid=32c9zrU, this differs from the legitimate web address. (1) All incoming emails from external senders arrive into the recipients inbox with a warning on that alerts them to the fact.

There were several aspects of this email that were designed to look as if it was a legitimate email:

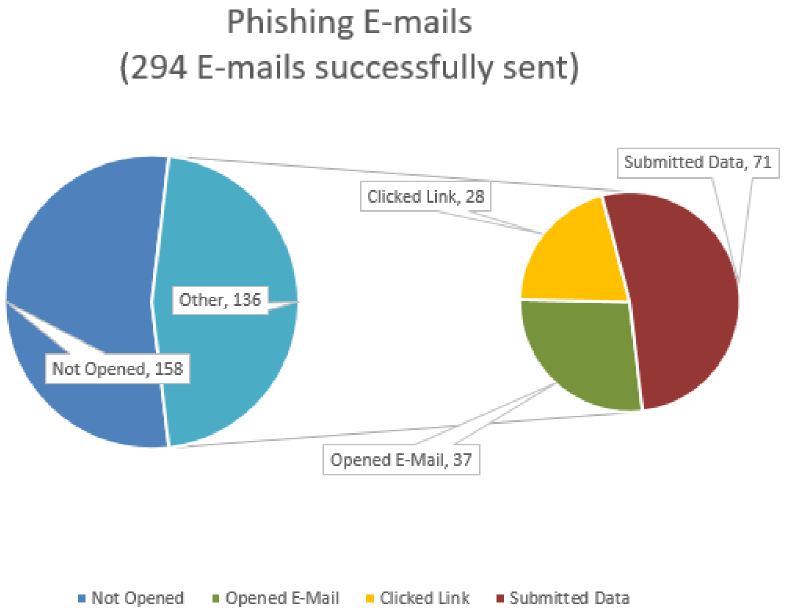
- The email was designed to look as if it was sent from Allerdale Council’s IT Department (2)
- The email was addressed directly to individual members of staff, the email also included their work email address (2)
- The signature within the email was designed to look identical to the format used by the council (5)

Outcome

The exercise began sending phishing emails at 10:02 AM on 12/03/2020 and ran for 7 days with the first staff member clicking on the link within 10 seconds and the first staff member submitting credentials at 10:03:55 AM.

Attack Outcomes

- In total **294** phishing e-mails were sent to the council of which **136** were opened and **37** did not interact any further.
- The total number of individual staff who clicked the link was **99**, representing **73%**. of the **136** who opened the e-mail.
- **71** usernames and passwords were entered into the bogus login page, **28** members of staff followed the link but did not enter any details.
- The total number of users who submitted credentials was **71**, representing **24%** of overall staff or **72%** of staff who clicked the link.
- The last staff member to click the link was recorded at 01:49 PM on 18/03/202 and the last person to submit their credentials did so at 01:50 PM on 19/03/2020.



*For ‘Clicked Link’ the user must have also opened the e-mail

*For ‘Submitted Data’ the user must have also opened the e-mail and clicked the link.

Outcome

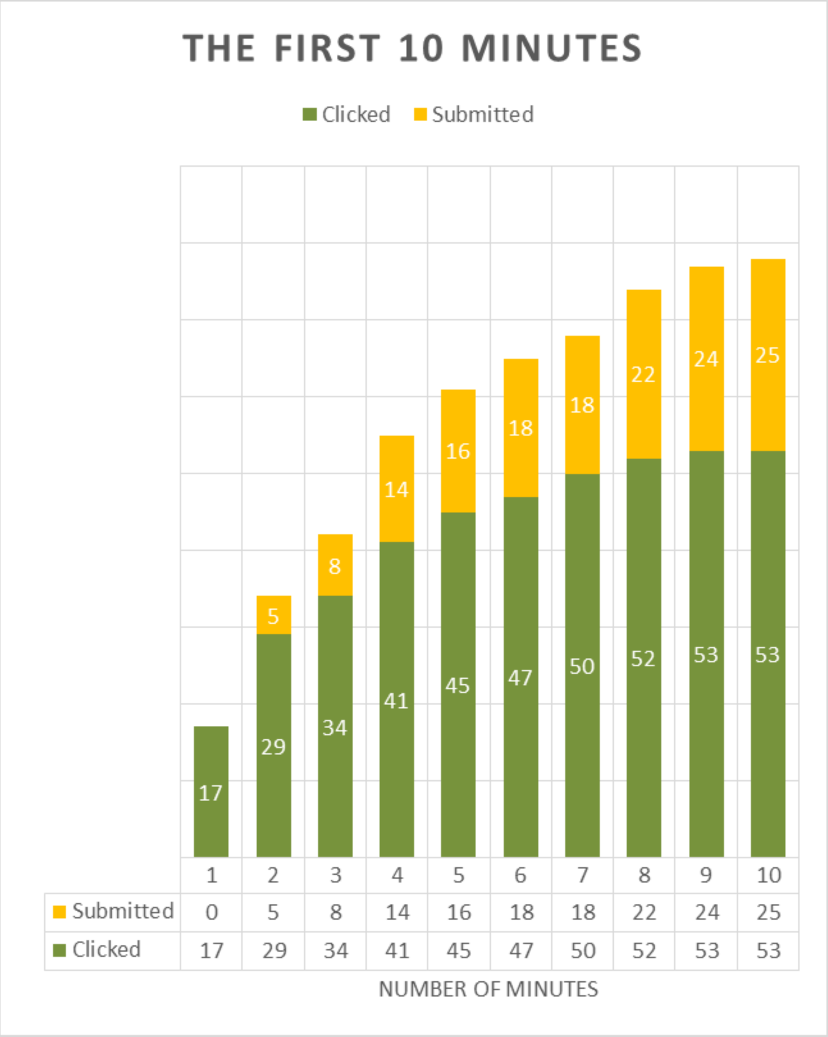
User Interaction

- The majority of staff clicked the link multiple time with several staff members clicking the link five times.
- Several staff members entered their credentials on to the bogus web page multiple time with one member of staff entering their credentials five times.
- The phone number within the phishing email belonged to the Assurance, Risk and Audit Manager. During the course of the exercise they received one phone call.

Mitigation

The campaign ran for seven days, ending on 19/03/2020 at 10:00 AM. Feedback from the organisation revealed that opportunities had arisen to reduce the potential impact of the phishing exercise. As this was a exercise those opportunities where purposely not instigated i.e. communication or blocking the sender/domain.

- IT managers received 20 different notifications from staff about the phishing attack within 13 minutes.
- At 10:30 AM staff were discussing sending a communication to all staff to alert them of the phishing email. Although this did not happen, information that the email may have been malicious may have spread via word of mouth.
- A further five members of staff reported the email to IT over the course of the exercise.
- During testing, controls within the council began to block the emails. IT then reconfigured these controls to allow the phishing emails through.



*For 'Clicked' the user must have also opened the e-mail

*For 'Submitted' the user must have also opened the e-mail and clicked the link.

Conclusion

The number of users who were successfully phished appears significant, if the campaign were to have run for longer, it is likely that even more people would have clicked on the link /submitted credentials as some will have been off-duty during this period.

It should be remembered that it can only take a single success to bring down a network or extract data. Organisations need to ensure, therefore, that they minimise their exposure through effective training so that staff can spot phishing. The outcomes of this exercise should provide a basis for delivering targeted training and awareness raising empowering users to make informed decisions. Example guidance includes:- *https://www.ncsc.gov.uk/phishing*

Specific training may include, for example:-

- Technical controls, such as passwords, safe ways to send emails, categories of phishing attacks, social media vulnerabilities, etc.;
- Legislation, such as EU General Data Protection Regulations (GDPR);
- Use of social media / online behaviour;
- Physical controls, such as clear desk policy;
- Threats / example scenarios, such as tailgating / targeted attacks using specific types of technology;
- Checklists for top tips / steps a user should take within the organisation; and
- Common terminology.

Management should also consider:-

- Follow up training exercise(s) to embed learning, taking into account targeted learning, where applicable;
- Carry out a lessons learned from both a technical and user perspective;
- Regularly review the processes, especially around incident response planning; and
- Review the supply chain for potential vulnerabilities, for instance, if an attacker masquerades as you / them in order to perpetuate a fraud.

Name	Mike Bennett
Title	Technology Risk Assurance Auditor
☎	0151 285 4607
✉	Michael.Bennett@miaa.nhs.uk

One trusted business. Two different services

MIAA ASSURANCE

MIAA SOLUTIONS