National Cyber Security Centre

# Identifying and reporting a suspected phishing email

Micro exercise

# Exercise introduction

This micro exercise is focussed on identifying and reporting a suspected phishing email. It is a short and sharp session that explores this topic using a combination of interactive activities covering the definition of phishing, the impact, and identifying a phishing email. You will have the opportunity to evaluate yourselves as a group against various competencies and at the end of the exercise you will be provided with a report summarising your evaluation.

## Participants and timing

Allow around 15 to 30 minutes, you may choose to tailor this to the time you and your participants have available.

## Required attendees

You can have as many or as few people involved as you like, and no one taking part in this exercise needs to be a cyber security expert. We recommend 3-5 people including a nominated facilitator to run the session and keep the conversation on track.

## What is expected of the participants?

You're here to think, talk and learn about this topic. You don't need to be a cyber security expert; it is not a test. Instead, we aim to enable collaborative discussions that further your knowledge and help you identify areas of improvement.

Your nominated facilitator is here to run the session and keep the conversation on track, in whatever way the group is comfortable with.

## Context

Spotting a phishing email is becoming increasingly difficult and can trick almost anyone into clicking on a link or opening an attachment, potentially infecting your system and those connected to it. Preventing this type of attack from being successful can help to mitigate a large proportion of cyber attacks.

Whilst the majority of this defence is technical, cyber security is everyone's responsibility and we all have a role to play in preventing cyber attacks and minimising the impact when attacks do happen.

This micro exercise focuses on exploring the role users have to play in spotting a phishing email, and the steps they can take to mitigate the damage a breach may cause.

# Questions

## Question 1 of 3

What is Phishing?

## Answer

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

## Question 2 of 3

What is Spear Phishing?

## Answer

This is more of a targeted campaign, where the attacker may use information about your employees or company to make their messages more persuasive and realistic.

## Question 3 of 3

Other than email, what common methods could phishing be conducted by?

## Answer

- SMS / text messages (Smishing) - malicious messages that appear to be from an official source
- Social media - malicious links and attachments
- Phone Call (Vishing) - cold calling to elicit sensitive information such as passwords

## Discussion

Discuss the risks around the following topics, that attackers might exploit to obtain passwords of work and personal accounts. A description of what to consider for each point will follow on the next page of the exercise.

### Discussion point 1

Common or obvious passwords

### Discussion point 2

Password Reuse

### Discussion point 3

Keylogging

### Discussion point 4

Phishing Attacks

## What to consider

### *Response to Discussion point 1*

Attackers are often able to conduct a dictionary or brute force attack against common passwords such as those observed in the quiz. A dictionary attack tries every word in a dictionary or wordlist to guess a password. A brute force attack differs as it uses computational power to enter a huge number of combination of values.

### *Response to Discussion point 2*

If an organisation, website or application you use is compromised, an attacker may be able to access user passwords. This can allow an attacker to gain access to any other internet facing system on which you use the same password for authentication.

### *Response to Discussion point 3*

Keyloggers are a type of malicious software that, once on your system, attempts to log the keystrokes you make — including passwords. Of course, this will compromise any password entered, no matter how complex. The best defence here is keeping your software current and up to date.

### *Response to Discussion point 4*

Attackers will often utilise phishing attacks to send users to fake login pages. Once the user enters their username and password it is passed to the attacker. Further guidance on attacker techniques can be found on the NCSC website.

## Question

What percentage of UK businesses reported a fraudulent email or being directed to fraudulent websites as their most disruptive breach or attack from the list below?

- 29%
- 43%
- 60%
- 95%

*Source: DCMS Cyber Security Breaches Survey 2019*

## Answer

- 43%

43% of UK businesses. However, while some companies experience loss of money or data, not all breaches or attacks lead to this. Direct costs may include staff being prevented from carrying out their work and lost revenue if customers could not access online services.

# Case study

## DDCMS survey

As an example, one high-income charity had suffered a breach after an employee email account was hacked. The email account sent a fake supplier invoice worth around £10,000 to their finance department, which a team leader mistakenly approved.

When considering the cost of this breach, the initial cost considered was the stolen £10,000.

They considered the recovery cost, but felt this was negligible, as securing the hacked email account was relatively straightforward.

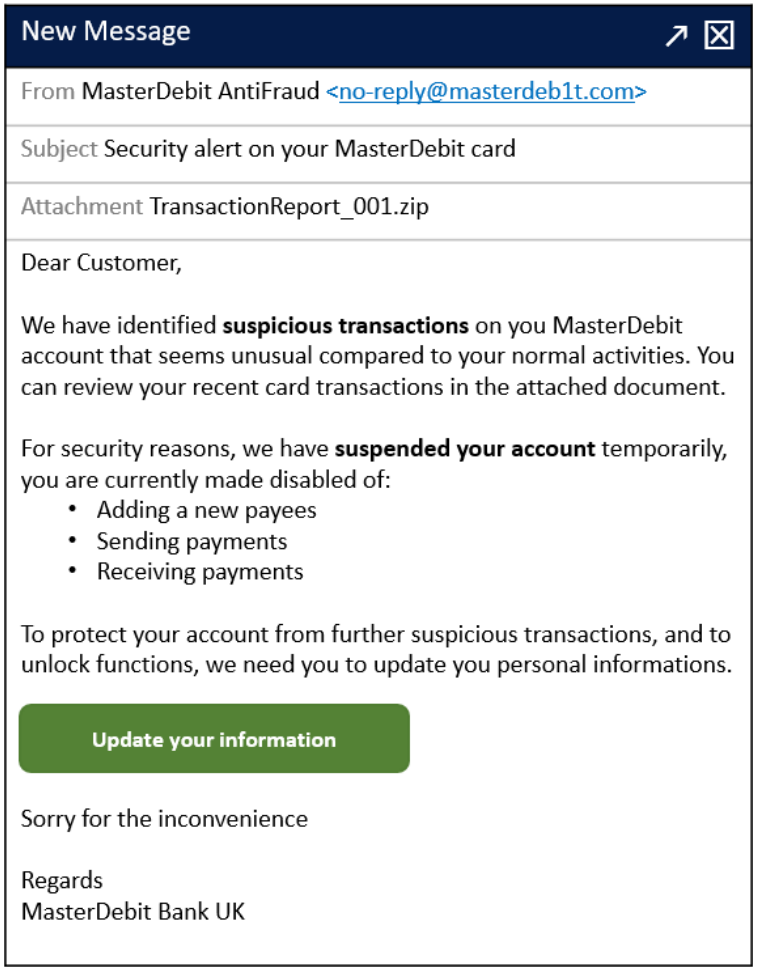
However, they did not initially consider the ongoing cost. As a result of the breach, all new supplier invoices now have to be approved by senior finance staff - an ongoing cost that senior managers had not considered.

*Source: Department for Digital, Culture, Media and Sport - Cyber Security Breaches Survey 2019*

## Identify

Can you identify the suspicious elements of this email?

Key things to look out for when you receive an unusual email:



New Message

From MasterDebit AntiFraud <no-reply@masterdeb1t.com>

Subject Security alert on your MasterDebit card

Attachment TransactionReport_001.zip

Dear Customer,

We have identified **suspicious transactions** on you MasterDebit account that seems unusual compared to your normal activities. You can review your recent card transactions in the attached document.

For security reasons, we have **suspended your account** temporarily, you are currently made disabled of:

- Adding a new payees
- Sending payments
- Receiving payments

To protect your account from further suspicious transactions, and to unlock functions, we need you to update you personal informations.

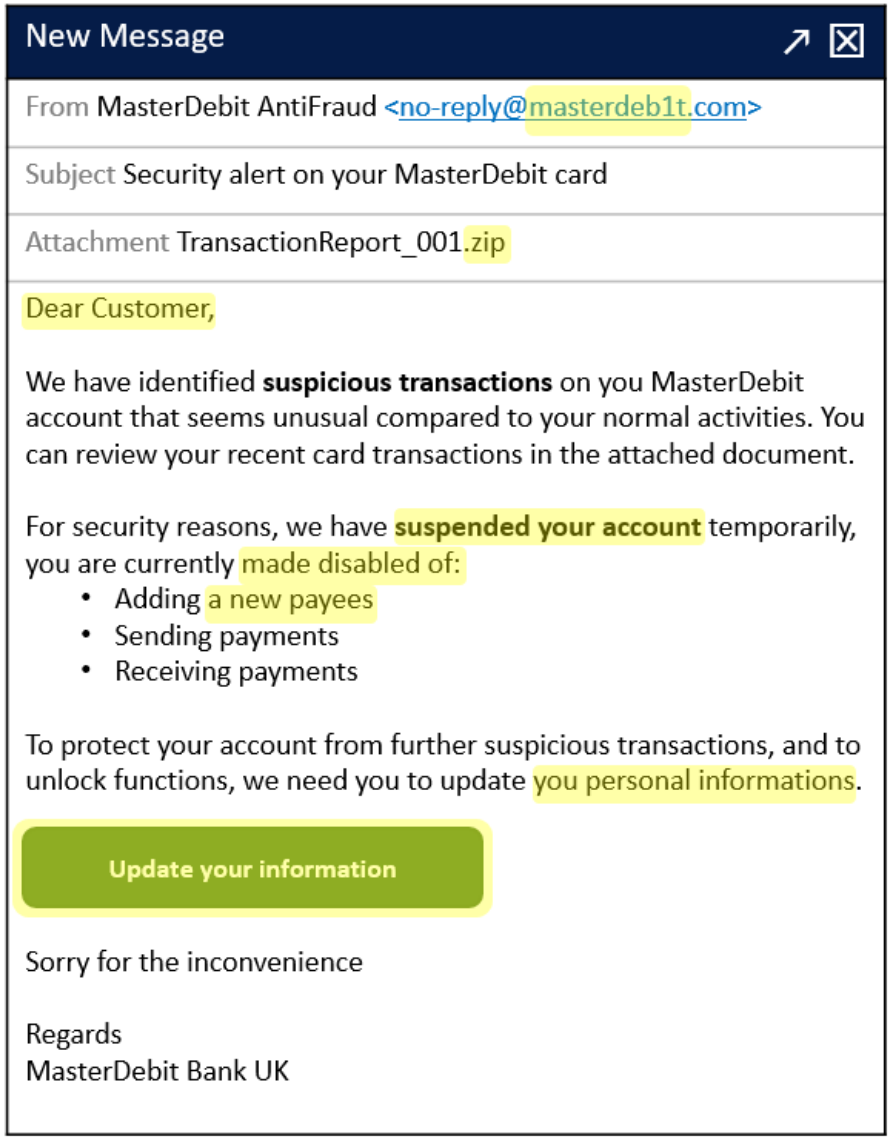
**Update your information**

Sorry for the inconvenience

Regards
MasterDebit Bank UK

## Key things to look out for when you receive an unusual email:

- **Dangerous file extensions in attachments** - These can be concealed within ZIP files
- **Suspicious email domains** - From public domains, nonsensical, misspelled or concealed
- **Poor spelling and grammar** - Especially if allegedly from a reputable company
- **Generic communications** - Using terms like “Dear Customer” to deliver automated, mass attacks
- **Suspicious links** - Where the destination does not match the company or context
- **Sense of urgency** - Attempting to provoke an immediate reaction without thinking



New Message

From MasterDebit AntiFraud <no-reply@masterdeb1t.com>

Subject Security alert on your MasterDebit card

Attachment TransactionReport_001.zip

Dear Customer,

We have identified **suspicious transactions** on you MasterDebit account that seems unusual compared to your normal activities. You can review your recent card transactions in the attached document.

For security reasons, we have **suspended your account** temporarily, you are currently made disabled of:

- Adding a new payees
- Sending payments
- Receiving payments

To protect your account from further suspicious transactions, and to unlock functions, we need you to update you personal informations.

**Update your information**

Sorry for the inconvenience

Regards
MasterDebit Bank UK

## Evaluation

Discuss the following statements and rate them on a scale of:

1. Not at all confident
2. Slightly confident
3. Somewhat confident
4. Fairly confident
5. Completely confident

- We have regular and effective training in using peripheral devices (such as a USB) and how to identify suspicious links and unexpected email attachments.

- The information on our public social media and other online accounts is minimal, private and regularly reviewed to reduce the risk of becoming a target.

- If we spot a phishing or fraudulent email, we have a clear reporting method to seek help and information.

- We have easily accessible policies and procedures in place in the event of a cyber security incident.

## Conclusion

Phishing and spear phishing continue to be a significant method for attackers to infect systems. Mitigating this attack vector can prove critical in helping you or your organisation avoid becoming a victim.

In its first two weeks of operation, NCSC's Suspicious Email Reporting Service (SERS) received 160,000 suspicious emails from the public which resulted in 395 phishing websites being taken offline. Flagging the email as spam in your mail provider and sending it to NCSC's SERS (report@phishing.gov.uk) will help protect others from falling victim to the same scam.

More information can be found at report suspicious emails

**Please note...**

You should not report a crime to the NCSC in this way.

If you think you may have been a victim of fraud or cyber crime, and live in England, Wales or Northern Ireland, you should report this to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2020. If you live in Scotland, you should report to Police Scotland by calling 101.

## Next steps

Make recommendations that will develop confidence in the areas that have been identified as having scope for improvement. Areas for improvement could be where you have given a lower confidence rating in any of the exercise observations. Discuss with and allocate the recommendations to the people in your organisation who can facilitate change and action improvement. Discuss the risks associated with not addressing the recommendations.

Ensure any recommendations are implemented and when ready, run the exercise again to see how those changes have impacted upon your organisation.

Also refer to the Related Guidance, below, which may help you in those areas you have identified as needing improvement.

To run further exercises please go back to Exercise in a box.

## Related guidance from the NCSC

Small Business Guide - How to improve cyber security within your organisation - quickly, easily and at low cost.
Small Business Guide: Response and Recovery - Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.
Mitigating Malware - This guidance describes how organisations of all sizes - and home users - can reduce the likelihood of being infected by malware.