Micro Exercises

Master Class

Scottish Government
Riaghaltas na h-Alba
gov.scot

Scottish Business
Resilience Centre

OUR **VISION**

Our vision is to make Scotland one of the safest and most resilient places to live, work and do business both on and offline.

Scottish Business Resilience Centre

Background

Scottish Business
Resilience Centre

Exercise in a Box

Using Passwords

Scottish Business Resilience Centre

Question

What is the most hacked password worldwide?

- Password
- 1111111
- 123456
- Qwerty

The answer is: 123456

Scottish Business Resilience Centre

Question

Which is the most hacked fictional name password?

- Pokemon
- Batman
- Tigger
- Superman

The answer is: Superman

Scottish Business Resilience Centre

Discussion

Common or obvious passwords

Why do we think common passwords are a bad thing?

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.

Password reuse

Why is password reuse a bad thing?

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.

Scottish Business Resilience Centre

Discussion

Keylogging

What are keyloggers?

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.

Phishing attacks

What is a phishing attack?

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.

Scottish Business Resilience Centre

Question

Choose the best password from the list below:

- Pa55word
- Password1
- Manutd1977
- 3redhousemonkeys27

The answer is: 3redhousemonkeys27

Scottish Business Resilience Centre

Scenario

You have logged into your laptop, and you cannot access your work email account due to an 'Incorrect password'. You have checked and confirmed that the password you are entering is correct. You have the ability to change your own password. Some colleagues mention that they will respond to your urgent emails as soon as possible.

- Have you ever experienced being locked out of an account before?
- What immediate steps would you take?
- Who would be your contact in your organisation?
- Why might colleagues be commenting on an urgent email from you?

You successfully reset your password and you have managed to logon to your work email account. Would you inform your organisation that your email may have been compromised? Yes, or no?

Scottish Business Resilience Centre

Advice

1. Create a strong and memorable password
2. Use Two Factor Authentication (2FA)
3. Use different passwords for your work account and personal accounts
4. Use stronger passwords for email accounts
5. Store passwords in a secure manner
6. Never reveal your full password to anyone

Scottish Business Resilience Centre

Responding to a ransomware attack

Scottish Business Resilience Centre

Question

What is ransomware?

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network.

How can Ransomware get onto your work computer?

Not all attack methods rely on user error or mistakes. Ransomware can reach your computer in a range of different ways, including:

- Spam/phishing emails
- Infected portable devices (e.g., USB)
- Phone
- Compromised/exploited websites (hacked by ransomware creators)

Scottish Business Resilience Centre

Case Study (WannaCry)

In May 2017, Telefonica reported its systems were encrypted by a previously unreported ransomware strain, demanding $300 worth of Bitcoin to unencrypt systems. Within hours the ransomware began to spread globally.

WannaCry was a worm, or a self-propagating piece of malicious code, that when deployed took advantage of unpatched systems that once infected would start looking for other systems to infect.

It is estimated that 200,000 - 300,000 computers were affected globally with billions of pounds of damage reported. The NHS was hit with an estimated 19,000 operations and appointments cancelled. Internationally, Government departments, car manufacturers and banks were also high profile victims of the attack.

Scottish Business Resilience Centre

Scenario

You log in one morning to find your computer infected with Ransomware. Your data is encrypted, and the malware has demanded £300 in bitcoin to release it.

- *What immediate steps would you take following an incident like this?*
- *Who would you contact in your organisation?*
- *Have you experienced a ransomware attack before?*

If you could not restore your data, would you consider paying the ransom? Yes or no?

Scottish Business Resilience Centre

Advice

The National Crime Agency (NCA) encourages industry and the public not to pay the ransom.

If you do:

- There is no guarantee that you will get access to your data.
- Your computer will still be infected unless you complete extensive clean-up activities.
- You will be paying criminal groups.

It is recommended that you report any ransom incident to PoliceScotland on 101. It is a matter for the victim whether to pay the ransom.

Scottish Business Resilience Centre

Identifying and reporting a suspected phishing email

Scottish Business Resilience Centre

Question

What is Phishing?

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.

What is Spear Phishing?

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.

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

- *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*

Scottish Business Resilience Centre

Question

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

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

The answer is: 43%

Scottish Business Resilience Centre

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*

Scottish Business Resilience Centre

Identifying and Reporting a suspected Phishing email

Can you identify the suspicious elements of this 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

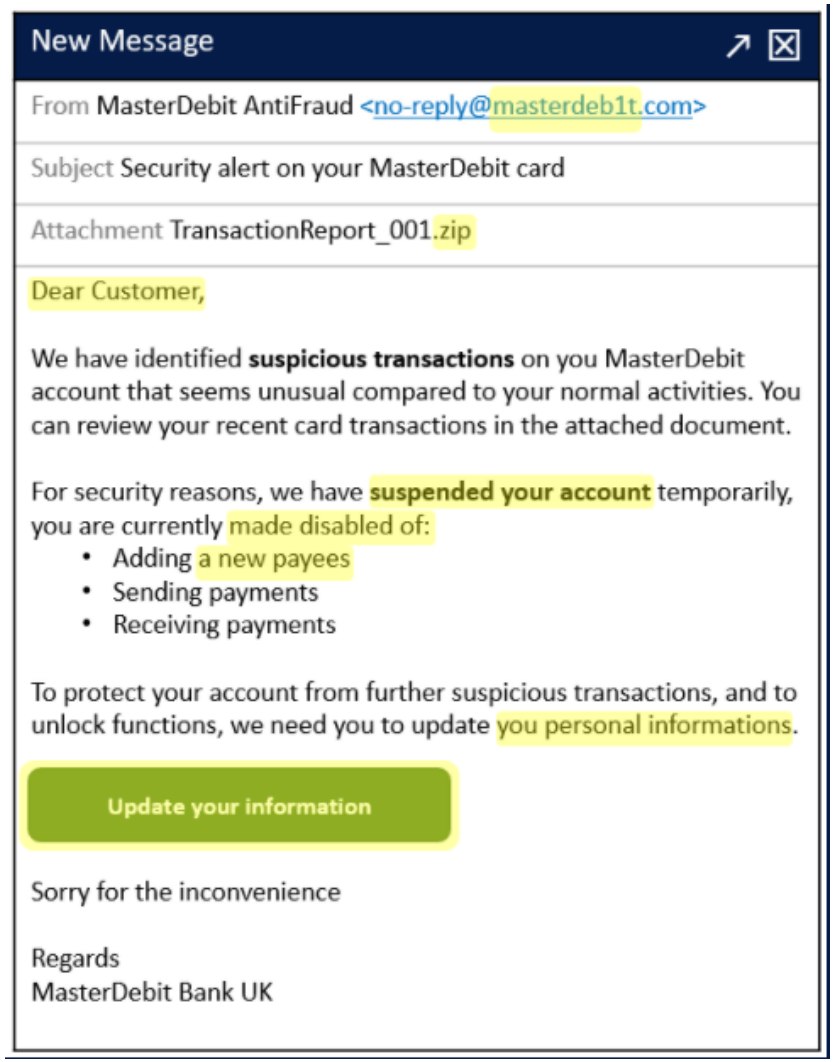
Sorry for the inconvenience

Regards
MasterDebit Bank UK

Scottish Business Resilience Centre

Identifying and Reporting a suspected Phishing 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

Scottish Business Resilience Centre

Wrap Up

Scottish Business
Resilience Centre

Scottish Business Resilience Centre

Q&A