2022 - 2023

Business Email Compromise Course - Research Document

NAME: BEN NAGLE

STUDENT NUMBER: C00247271

SUPERVISOR: PAUL BARRY

South East Technological University

Abstract

This document records the research undertaken into the topic of Business Email Compromise (BEC) in preparation for developing electronic teaching materials to educate users on the subject. The aim of this project **D**evelop a collection of electronic teaching materials which can be used to educate emails users on BEC (business email compromise), concentrating on how to identify a compromised email, as well as strategies for dealing with same. The resulting “course” should be no more than one hour induration, and needs to be graded (i.e., activities test how well the material is understood by the user).

Table of Contents

Introduction 3
1 – How Does Internet Email Work? 4
2 – What is Business Email Compromise? 5
2.1 – What is Social Engineering? 7
2.2– What is Phishing? 8
2.2.1 – Five Types of Phishing Attacks 9
2.2- How does Business Email Compromise Work? 13
2.3- The Five Major Types of Business Email Compromise Scams 14
2.4- Business Email Compromise in 2022 16
3 – Famous Examples of Business Email Compromise Attacks 17
3.1- Facebook and Google BEC Attack 17
3.2- Save The Children BEC Attack 18
3.3- Puerto Rico Government BEC Attack 18
4 – Business Email Compromise Courses & Training Materials 19
4.1- 'Would you know what to do if you were a victim of business email compromise?' 19
4.2- 'Phishing Staff Awareness Training Programme' 20
4.3- 'Business Email Compromise by Tyler Hudak and Aaron Rosenmund'. 20
4.4- IT Security: Business E-mail Compromise 20
4.5- Nano Self Study: What is Business Email Compromise? 21
4.6 - Business Email Compromise Readiness Assessment 21
4.7- MetaCompliance Phishing and Ransomware: 'MetaPhish' 22
4.8– Articles and online materials 22
5 – Online quiz recourses 24
5.1 – PHP/MYSQL 24
5.2 – Google Forms Quiz 24
5.3 – Microsoft Forms Quiz 25
5.4 – Moodle 25
References 27

Introduction

This document records the research undertaken into the topic of Business Email Compromise (BEC) in preparation for developing electronic teaching materials to educate users on the subject.

The aim of this document is to provide the reader with a broad introduction to this final year project, beginning with how BEC became one of the top threats identified by the FBI in their 2021 Internet Crime Report [21]. This will be explored by examining the technology behind internet email which provides the groundwork for the emergence of threats such as BEC due to vulnerabilities that can be exploited for malicious intent, to the history of scamming and social engineering which has become more sophisticated and adapted to newer technologies (such as email and video conferencing).

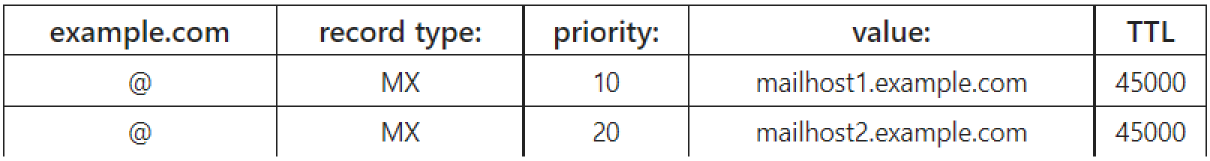
Business Email Compromise is a type of Phishing attack, how BEC compares to other forms of phishing and the growth in such attacks over recent years will be examined. Having established this groundwork, the document will explain Business Email Compromise in more detail and expand on the types of attacks that are commonly undertaken by threat actors. To aid in explaining the severe impact successful BEC attacks can have on organisations, famous examples of BEC are outlined along with the financial impact experienced by the victim organisation(s).

Finally, electronic teaching materials and courses which cover Business Email Compromise that are currently available will be detailed. The topics covered, relative price and duration of these courses will provide an understanding of the material that currently exists for those wishing to educate themselves about BEC in 2022.

1 – How Does Internet Email Work?

Business Email Compromise Attacks rely on the dependency organisations have on email for communication. The standard communication protocol for email transmission is SMTP (simple mail transfer protocol), which is used to both send and receive emails over the internet.

When a user sends an email, the email client (ex. Gmail or Microsoft Outlook) sends it to an SMTP server. The SMTP server processes the email and checks for the recipients address/domain in the email envelope. It’s possible for an attacker to input a spoofed email address in the ‘mail from’ field of the email envelope which “opens the door” for BEC type attacks [1]. The SMTP server communicates with a DNS (Domain Name System) server to translate the domain name to an IP Address. SMTP searchers for a mail exchange server that is associated with the recipient’s domain, according to CloudFlare [2] *“A DNS 'mail exchange' (MX) record directs email to a mail server. The MX record indicates how email messages should be routed in accordance with the Simple Mail Transfer Protocol”.*

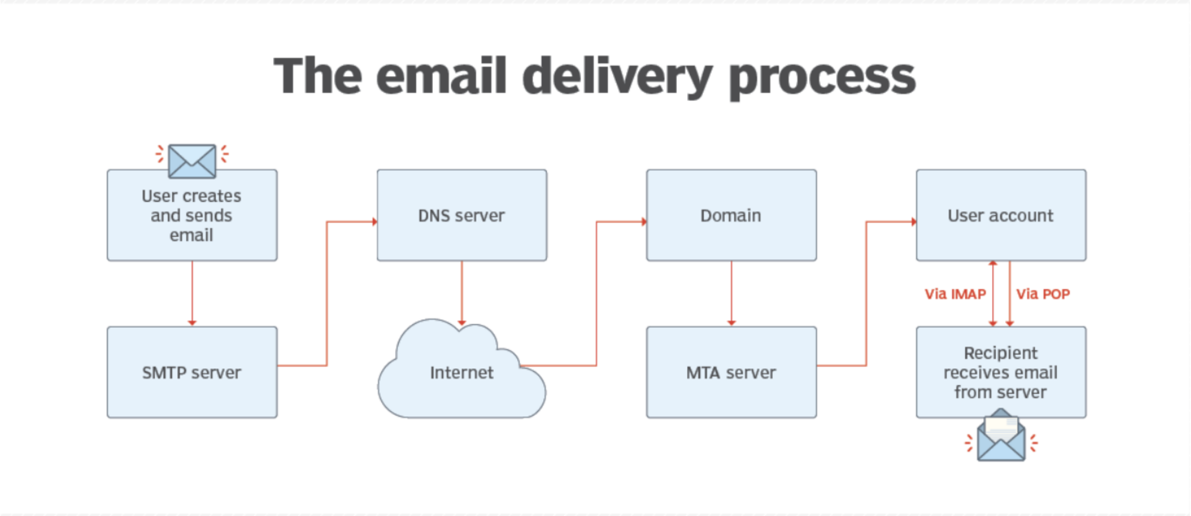


example.com	record type:	priority:	value:	TTL
@	MX	10	mailhost1.example.com	45000
@	MX	20	mailhost2.example.com	45000

Figure 1: Example of a MX Record [2]

Above is an example of a MX record, in this case preference is given to ‘mailhost1’ as its priority is set to ‘10’. If there is a failure, the server will automatically default to ‘mailhost2’.

The email is then forwarded to the recipient’s mail server, it may be retrieved by either the POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) protocols. POP will download the email to the recipient’s local device while IMAP only downloads the message from the server when the receiver interacts with it, otherwise it remains stored on the server and not on a local device. [3]



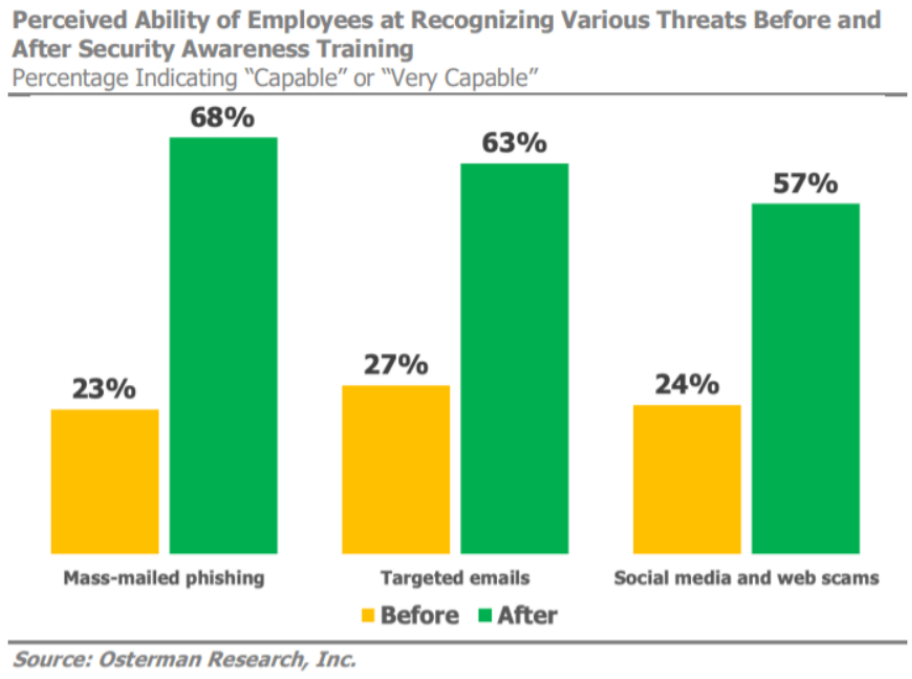
The email delivery process
User creates and sends email
SMTP server
DNS server
Internet
Domain
MTA server
User account
Via IMAP
Via POP
Recipient receives email from server

Figure 2: The Email Delivery Process [3]

2 – What is Business Email Compromise?

In their H2 2022 Email Threat Report, Abnormal Security identified a 48% increase in email attacks over the previous six-month period [4]. In 2020, it was reported that a staggering 65% of businesses world-wide faced Business Email Compromise (BEC) attacks [5] and concerningly in a 2020 survey conducted by Canadian researchers, 25% of participants were fooled by phishing emails [6]. Just taking some of the above statistics gathered in recent years, it's clear that email related attacks and social engineering are of great threat to organisations globally. As such, its of vital importance that employees have increased awareness of these attacks and the dangers associated with having sensitive data compromised.

Training and cyber security awareness is key to providing employees across all departments in an organisation with the knowledge and skill set to identify suspicious activity, such as phishing or BEC. Research shows that employees are far more likely to identify threats having received the appropriate awareness training:



Source: Osterman Research, Inc.

Figure 3: Perceived Ability of Employees at Recognizing Various Threats before and after Security Awareness Training. [7]

Business Email Compromise (BEC) is a sophisticated scam in which fraudsters target organisations, often by posing as a high-level executive (likely someone who can authorise a transaction) in order to trick a victim into sending money to an account controlled by the fraudster or divulge confidential information.

In their '2021 Internet Crime Report', the FBI revealed that they received 19,954 complaints related to BEC scams with an adjusted loss of nearly $2.4 Billion [8]. BEC, along with Ransomware and the Criminal Use of Cryptocurrency, were among the top incidents reported to the FBI in 2021.

BEC attacks can have huge financial implications for an organisation and can go undetected due to their targeted and advanced nature. Fraudsters carefully and thoroughly research their victims/organisations, crafting emails that appear more legitimate and trustworthy when compared to mass mail phishing. These scams often don't include any malicious links or attachments which can make it difficult for the victim to identify as suspicious, which leads to a higher success rate.

Greathorns 2021 Business Email Compromise Report found that 35% of organisations stated that BEC/phishing attacks accounted for more than 50% of the incidents they suffered [9]. Training and increased awareness can help employees identify this type of scam.

2.1 – What is Social Engineering?

BEC attacks rely not only on vulnerabilities that exists in email communication (such as changing the 'mail from' value to a spoofed email address) but also on people's trusting nature. Cisco's description of Social Engineering best captures this:

"(Social Engineering) *targets the mind like your old school grifter or con man. The aim is to gain the trust of targets, so they lower their guard, and then encourage them into taking unsafe actions such as divulging personal information or clicking on web links or opening attachments that may be malicious".* [10]

The term 'social engineering' appears to date back to the 1890's [11] and has evolved ever since. In the 1990's, threat actors would call victims to trick them into divulging credentials. Nowadays, attackers commonly use email as a method of social engineering to trick victims into sending large sums of money to offshore accounts.

Social engineering emails often involve the use of a spoofed email address (attacker will register a domain similar to the target organisations), urgent language (which may influence the victim to act quickly) and malicious attachments or links.

According to Proofpoint, Social engineering is responsible for 98% of cyber attacks [12]. Which would suggest that humans are the weakest link in any organisation's security, partly due to our trustworthy nature and belief that people have our best interests at heart. Con men and criminals have been exploiting this trustworthiness for centuries, it's only the means in which they trick people that have changed. During the increasing popularity of the telegram, scammers would send out messages about fake goods and services to wealthy businessmen, like mass-mail phishing that is commonplace today.

BEC scams are no different than scams from centuries past in their aim – fool unsuspecting victims into sending money to the scammer. In BEC, the attacker often impersonates a high-ranking executive and may take advantage of trust that exists between the executive and other employees in the organisation (such as those in the finance department). The attacker will craft a personalised email in an attempt to trick the victim into wiring funds to an attacker-controlled account (more on this in **section 2**).

BEC is just part of the evolution and ever-growing sophistication of scams, particularly over more recent decades with the growth in popularity of email as a form of communication in organisations and the use of the internet to conduct business (sending wire transfers).

2.2 – What is Phishing?

According to Proofpoint, Phishing is *"when attackers send malicious emails designed to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials or other sensitive data."* [13]. Business Email Compromise is considered a form of Phishing attack.

Phishing Attacks have varying levels of sophistication and anyone from large organisations to individuals can be targeted. According to APWG's 'PHISHING ACTIVITY TRENDS REPORT Q4 2021', phishing hit an all-time high in 2021, with attacks tripling since early 2020 [14].

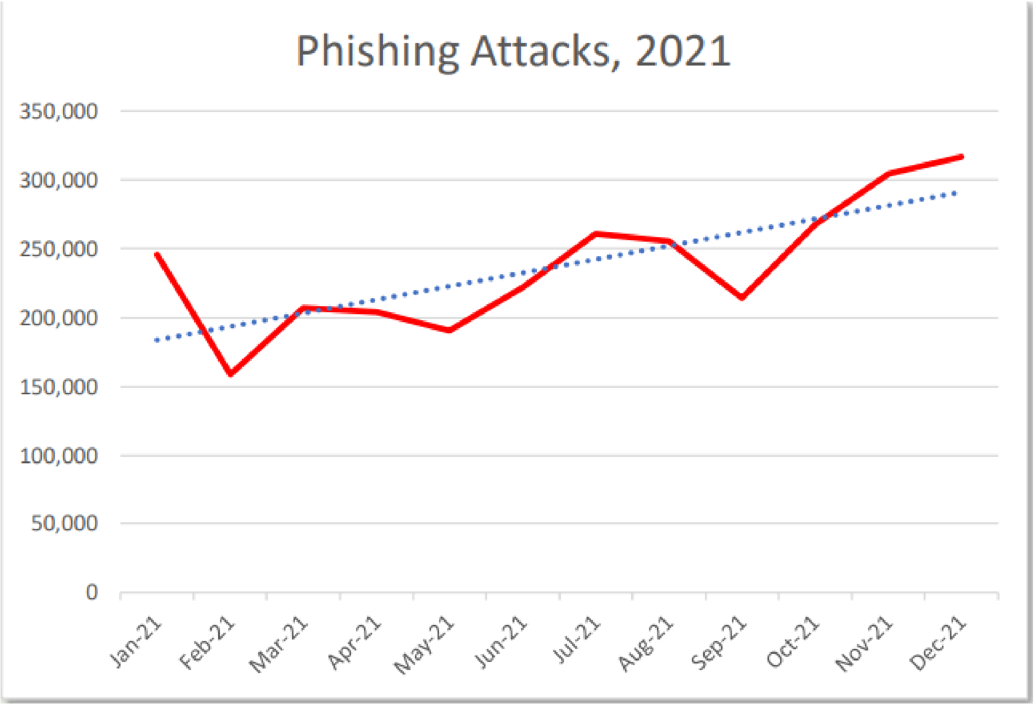


Figure 4: Phishing Attacks, 2021 [13].

With more than 300,000 incidents recorded in December 2021, Phishing attacks are becoming increasingly common. Checkpoint have identified five frequent types of Phishing attacks, outlined below [15].

2.2.1 – Five Types of Phishing Attacks

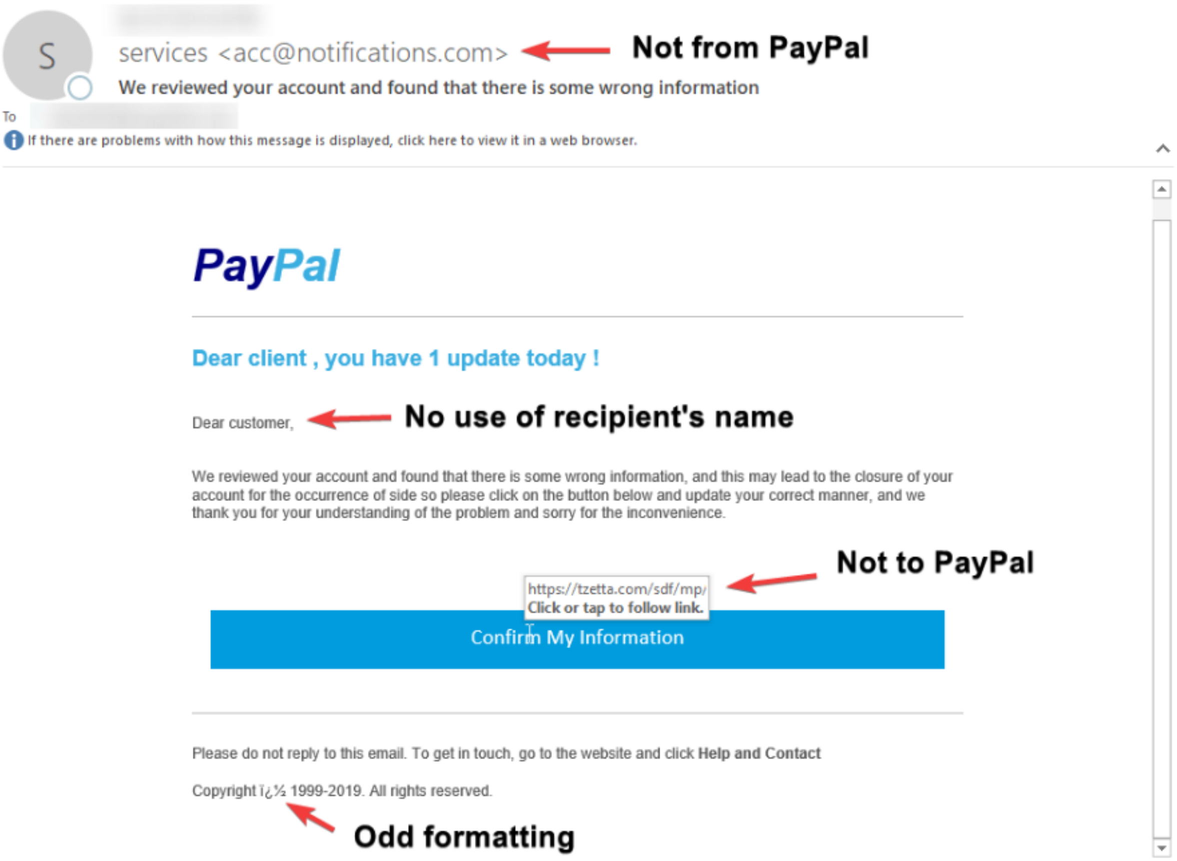
<u>1 - Email Phish</u>

Most phishing campaigns are conducted over email, the attacker will often pose themselves as a legitimate organisation and send fraudulent emails with generic requests to thousands of potential victims.

The attacker will register a fake domain like that of the organisation they are impersonating. Alternatively, the fraudster may create a domain with the organisations name in it, such as 'john@bankofirelandhelp[.]com'. The victim may be fooled if they see the legitimate organisations name in the address.

The fraudulent emails will often include a link to a malicious site to either deploy malware or have the user submit personal information such as credentials. Phishing emails may use a sense of urgency to panic the victim into complying with the fraudulent requests before checking the authenticity of the email.

Below is a real example of a Phishing email [16], claiming that there is something wrong with the users PayPal account and it will be shut down unless they click a link to update their information. PayPal is one of the words largest payment systems and therefore is a popular choice by scammers to be spoofed in order to steal a victim's credentials.



[redacted]

services <acc@notifications.com>

Not from PayPal

We reviewed your account and found that there is some wrong information

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

PayPal

Dear client , you have 1 update today !

Dear customer,

No use of recipient's name

We reviewed your account and found that there is some wrong information, and this may lead to the closure of your account for the occurrence of side so please click on the button below and update your correct manner, and we thank you for your understanding of the problem and sorry for the inconvenience.

Not to PayPal

https://tzetta.com/sdf/mp/
Click or tap to follow link.

Confirm My Information

Please do not reply to this email. To get in touch, go to the website and click **Help and Contact**

Copyright ï¿½ 1999-2019. All rights reserved.

Odd formatting

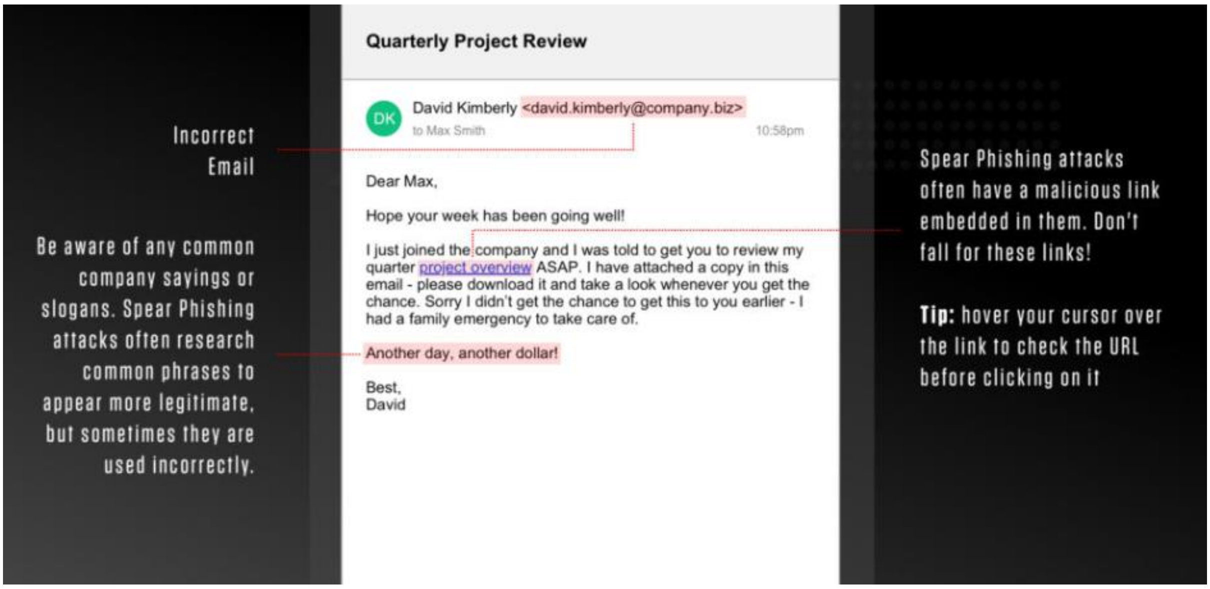
Figure 5: PayPal Phishing Email [16]

This email was intercepted by AddRiver and they claim the clink brings the victim to a convincing looking PayPal login page. However, any information entered will be given to the attackers allowing them to steal funds from the account.

2 – Spear Phishing

Unlike the previous example, Spear Phishing is targeted to a specific individual or group. Typical Spear Phishing attacks include personal information about the target (name, job title, trusted colleagues) that can be sourced online and a malicious attachment or link. As these emails are more personalised and can appear to come from a trusted source, victims are more likely to fall for it.

The goal of these attacks is to obtain credentials or other confidential information from the victim. Below is an example of a Spear Phishing email provided by Crowdstrike [17]:



Incorrect Email

Be aware of any common company sayings or slogans. Spear Phishing attacks often research common phrases to appear more legitimate, but sometimes they are used incorrectly.

Quarterly Project Review

David Kimberly <david.kimberly@company.biz>
to Max Smith
10:58pm

Dear Max,

Hope your week has been going well!

I just joined the company and I was told to get you to review my quarter project overview ASAP. I have attached a copy in this email - please download it and take a look whenever you get the chance. Sorry I didn't get the chance to get this to you earlier - I had a family emergency to take care of.

Another day, another dollar!

Best,
David

Spear Phishing attacks often have a malicious link embedded in them. Don't fall for these links!

Tip: hover your cursor over the link to check the URL before clicking on it

Figure 6: Spear Phishing Email [17]

The language used in these emails can portray a sense of urgency so that the victim will comply with the request quickly and will be less likely to realise the email is fraudulent. In this example, the attacker poses themselves as a new employee who has been instructed to have their project reviewed. However, the link is malicious and could lead to the installation of malware or the exposure of the victims' credentials. According to DataPort [18], 50% of people who open spear phishing emails click on malicious links within an hour of receiving. BEC is a from of spear phishing.

3 – Whaling Attack

According to Mimecast, a whaling attack *"is a type of spear-phishing attack directed at high-level executives where attackers masquerade as legitimate, known and trusted entities and encourage a victim to share highly sensitive information or to send a wire transfer to a fraudulent account."* [19]

Whaling attacks are similar to Business Email Compromise, however in BEC the attacker poses themselves as a high-ranking executive while whaling attacks target them. These attacks typically don't include malicious attachments and links, instead they aim to fool the victim into divulging personal information, customer information, employee data or bank account data. This makes Whaling more difficult to identify compared to other types of Phishing attacks.

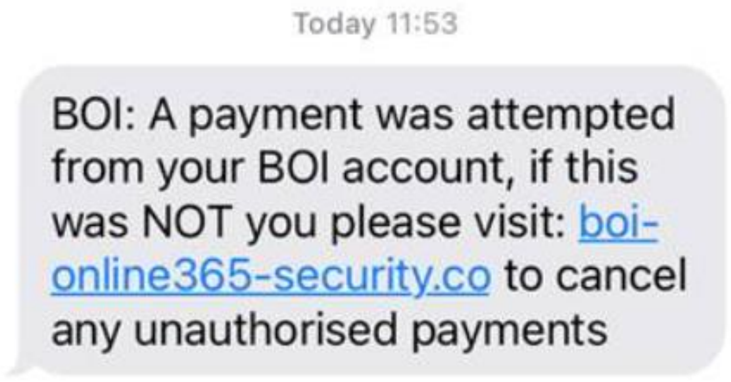
Much can be discovered about high-ranking executives in the public domain, allowing attackers to form highly personalised emails and increase their success rate.

4 – Smishing

Smishing is a type of Phishing, in which the attacker sends fraudulent SMS messages as opposed to emails. Proofpoint claims that users are much more trusting of text messages and are less aware of the dangers associated with clicking malicious links in them [20].

'Smishers' may use personalised information or location-based information to make the message seem more believable, with the goal being like other phishing types (obtain credentials, personal information, financial data). Smishers may pose themselves as a legitimate organisation such as a courier service or bank. Having clicked on the malicious link, users may be prompted to provide personal info or malware may be installed on their device.

Below is an example of smishing provided by Bank of Ireland in a campaign to warn and educate their customers [21]:



Today 11:53

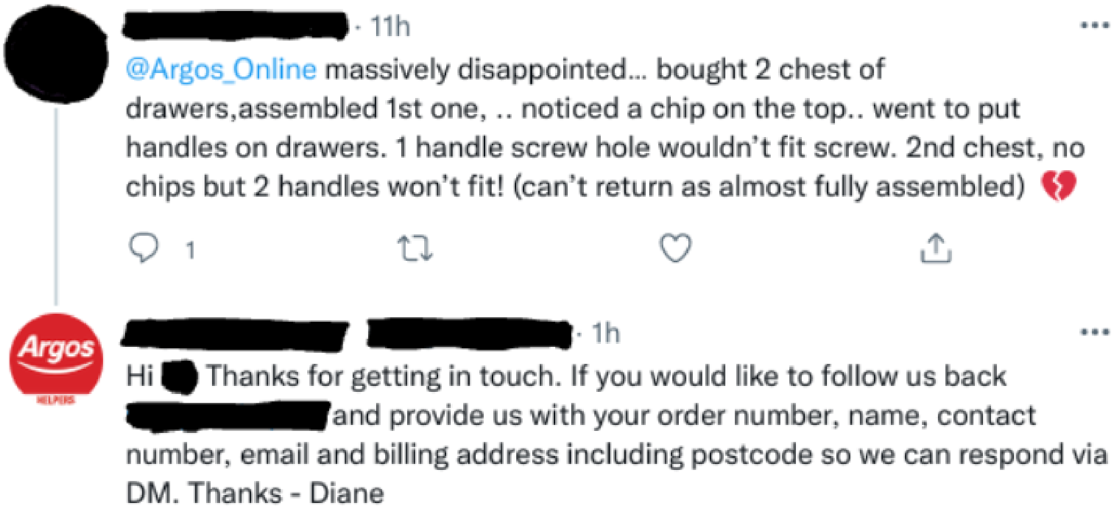
BOI: A payment was attempted from your BOI account, if this was NOT you please visit: boi-online365-security.co to cancel any unauthorised payments

Figure 7: Bank of Ireland Smishing [21]

5 – Angler Phishing

In Angler Phishing, fraudsters use fake social media account impersonating legitimate organisations to trick users. Users often use social media platforms (such as Twitter) to complain or attempt to get in contact with legitimate companies, attackers will use fake accounts to contact customers and trick them into sending sensitive information to them.

Users who may be impatient or desperate for assistance could fall victim to this type of Phishing and may not check that the account they are communicating with is official. Below is an example of Angler Phishing on Twitter.



[redacted] · 11h

@Argos_Online massively disappointed... bought 2 chest of drawers,assembled 1st one, .. noticed a chip on the top.. went to put handles on drawers. 1 handle screw hole wouldn't fit screw. 2nd chest, no chips but 2 handles won't fit! (can't return as almost fully assembled) 💔

1

[redacted] [redacted] · 1h

Hi [redacted] Thanks for getting in touch. If you would like to follow us back [redacted] and provide us with your order number, name, contact number, email and billing address including postcode so we can respond via DM. Thanks - Diane

Figure 8: Angler Phishing [22]

Phishing attacks can vary from more generic email campaigns that target a large group to more sophisticated schemes that are targeted at an individual/specific organisation. More sophisticated examples including whaling, spear phishing and business email comprise which can be more difficult to detect and appear more legitimate to the victim.

2.2- How does Business Email Compromise Work?

Business Email Compromise attacks often begin with the attacker identifying their target and gathering information through open-source intelligence. The attackers aim may be to impersonate a high-ranking executive, in which case they will use resources such as the company website and social media during their reconnaissance. The attacker builds a profile of their target organisation and victims.

According to Microsoft [23], the specific roles that are more likely to be targets of BEC scams include, but are not limited to; Executives and leaders, finance employees, HR managers and entry level employees. Entry level employees make for an appealing target as they may be less likely to question a request that appears to be from a manager or higher-ranking team member.

Once the target has been identified, an attacker will attempt to compromise a high-ranking executive's email account in order to fake their identity, methods to achieve this can include using a keylogger, malware or phishing. They may also create a fake/spoofed domain or register a company with the same name as the targets in another country. The fraudster might create a spoofed email address to pose as the high-ranking executive or trick the victim into giving away credentials. The attacker may take advantage of common workflows to get the victim to click a link, such as fake password reset emails.

Having compromised the email account, the attacker will monitor the mailbox to learn more about the inner workings of the organisation. Specifically, they will be interested in discovering who initiates and receives transactions so they can create a more legitimate appearing scam. In order to convincingly impersonate the high-ranking executive, the attacker may read through their 'sent' mailbox to learn how they typically write and construct emails.

When they initiate the attack, the attacker will use language that creates a sense of urgency and authority to achieve the victims trust, the attacker may avail of terms such as:

- Request
- Overdue
- Payment
- Immediate Action Required
- Important
- Urgent

Depending on the type of BEC attack, the perpetrator may attach fake invoices or attorney/legal firm letters to trick the victim. Regardless of the method or execution, the attackers end goal is to convince the victim to send a wire transfer to an account controlled by them.

2.3 - The Five Major Types of Business Email Compromise Scams

The FBI defines the five major types of Business Email Compromise Scams [24] [25]:

1: The Bogus Invoice Scheme:

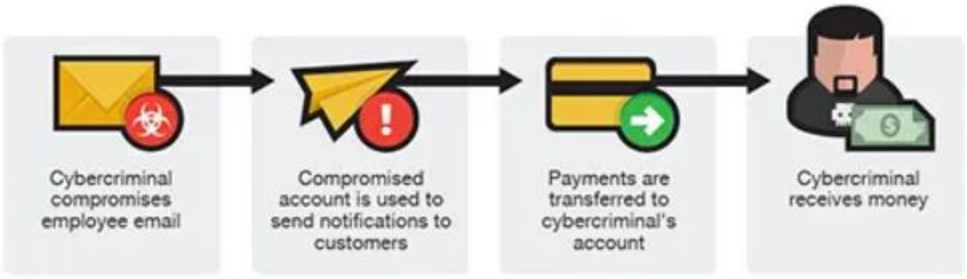

Cybercriminal compromises employee email
Compromised account is used to send notifications to customers
Payments are transferred to cybercriminal's account
Cybercriminal receives money

Figure 9: The Bogus Invoice Scheme [24]

This scheme (also known as ‘The Supplier Swindle’ and ‘Invoice Modification Scheme’) usually targets a business with an established relationship with a vendor, in which the fraudster uses a fake invoice requesting the business to wire funds to an alternate, fraudulent account.

2: CEO Fraud

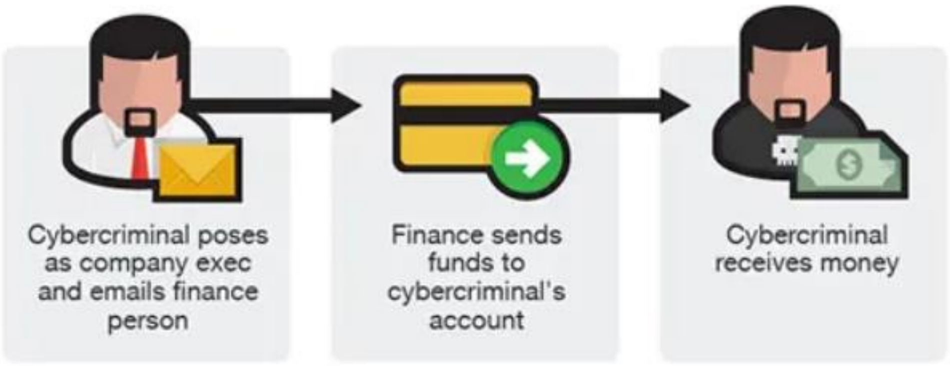

Cybercriminal poses as company exec and emails finance person
Finance sends funds to cybercriminal's account
Cybercriminal receives money

Figure 10: CEO Fraud [24]

In this instance, the email account of a high-level executive (CEO, CFO, CTO etc.) is compromised (spoofed or hacked). A wire transfer request to a fraudulent account is sent from the compromised email to an employee in the organisation (such as within the finance department). In other cases, a fraudulent wire transfer is sent directly to the financial institution with instructions to urgently send funds to a bank. This scenario is also known as ‘Business Executive Scam’, ‘Masquerading’ and ‘Financial Industry Wire Frauds’.

3: Account Compromise

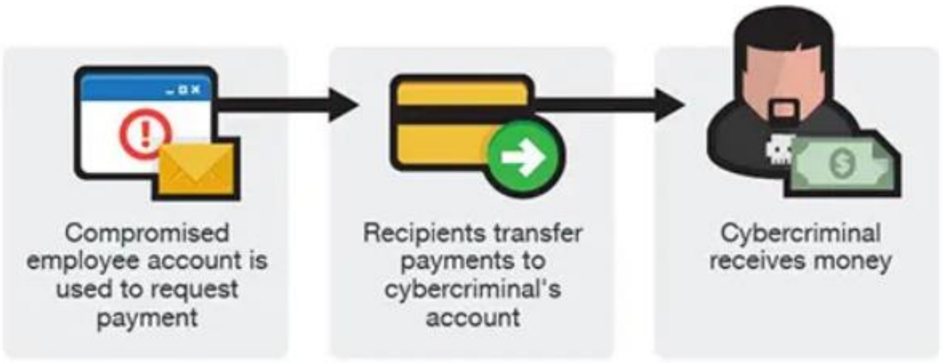

Compromised employee account is used to request payment
Recipients transfer payments to cybercriminal's account
Cybercriminal receives money

Figure 11: Account Compromise [24]

The email account of a business employee is compromised, the attacker identifies multiple vendor contacts from the hacked account. Requests for invoice payments to a fraudster-controlled account are sent to the vendors from the compromised email. The business may not become aware of the scam until vendors request follow ups on the invoice status.

4: Attorney Impersonation

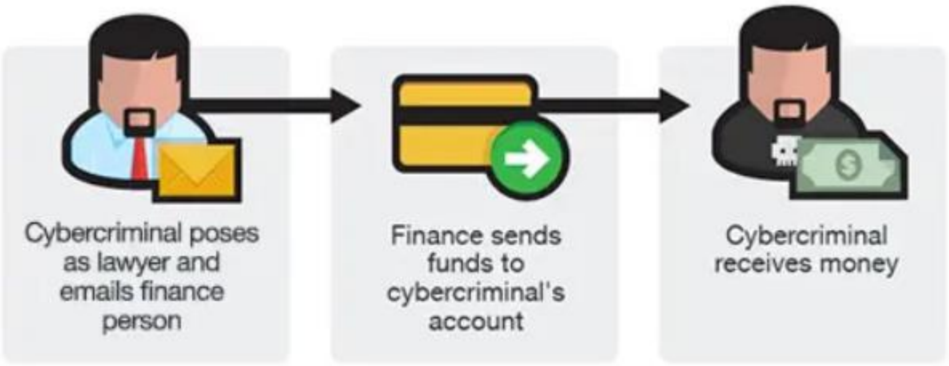

Cybercriminal poses as lawyer and emails finance person
Finance sends funds to cybercriminal's account
Cybercriminal receives money

Figure 12: Attorney Impersonation [24]

In this scheme, the attacker will pose as an attorney or law firm representative claiming to be handlining time sensitive or confidential matters. The victim could be either an employee or CEO, who will be pressured by the attacker into acting quickly on the request to transfer funds. This scheme may even occur towards the end of the working week so to increase potential panic.

5: Data Theft

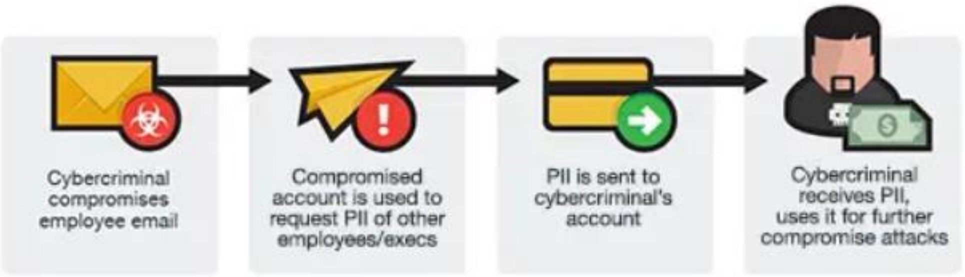

Cybercriminal compromises employee email
Compromised account is used to request PII of other employees/execs
PII is sent to cybercriminal's account
Cybercriminal receives PII, uses it for further compromise attacks

Figure 13: Data Theft [24]

Unlike previous schemes outlined above, in this scenario the attackers aim is to obtain PII from a person in an organisation responsible for handling such information (Human Resources Department). This scheme is more reliant on social engineering and can serve as the beginning of more damaging BEC attack against the organisation or as an isolated incident.

2.4 - Business Email Compromise in 2022

In the 'FBI 2021 Internet Crime Report' [8], coverage was given to the evolving nature of BEC attacks – particularly following the COVID-19 pandemic. The report points out that the scheme has evolved from the simple spoofing/hacking of email accounts and requests to send wire payments or confidential information.

Since the COVID-19 pandemic and associated lockdowns, there has been a significant shift to remote and hybrid working. In the Central Statistics Office 'Pulse Survey - Our Lives Online - Remote Work November 2021' report, 23% of respondents said they worked remotely at some point before the pandemic but 80% have worked remotely at some time since [26]. More recent statistics from September 2022 show that 28% of Irish workers usually work from home [27].

This is relevant as newer BEC schemes exploit the reliance on virtual meetings to instruct victims to send fraudulent wire transfers. This scheme usually begins with the attacker compromising the email account of a high-level executive in order to invite the victim to a virtual meeting. More advanced than traditional BEC schemes, the attacker would either use a still picture of the high-level executive with no audio or use a 'deep fake' audio, through which they will claim their video/audio connection is unstable. The attackers will then directly provide instructions to the victim using the video conferencing platform to initiate the wire transfer.

3 – Famous Examples of Business Email Compromise Attacks

3.1 - Facebook and Google BEC Attack

Between 2013 and 2015 – a Lithuanian man, Evaldas Rimasauskas, scammed over $100 million dollars from two of the world's biggest tech giants (Google and Facebook) through an elaborate BEC scheme. It was alleged that Rimasauskas established a company to pose as another in order to trick employees at Facebook and Google into wiring funds to various accounts that he controlled. He would ultimately plead guilty in 2019 and was sentenced to 5 years in prison and order to forfeit $49 million by a New York Judge [28].

In 2013, Rimasauskas established a company in Lativia called 'Quanta Computer'. 'Quanta Computer' happens to be a Taiwan based computer manufacturer that Facebook and Google routinely do legitimate business with. According to the allegations outlined in the Indictment [29], Rimasauskas sent phishing emails to employees in both companies with fake invoices that appeared to have been sent from actual Quanta employees and agents - while in reality they were not authorized or sent from Quanta. Rimasauskas was successful at deceiving both Google and Facebook into complying with the fraudulent wiring instructions.

Having illegitimately received the funds, Rimasauskas organised that they be wired to bank accounts in various locations around the world including Latvia, Cyprus, Slovakia, Lithuania, Hungary, and Hong Kong. This BEC scheme was elaborate, Rimasauskas is alleged to have created fraudulent letters and contracts with the forged signatures of Quantra executives, which were sent to Banks to 'legitimise' the large sums of money being transferred.

According to the US Attorney's Office [29], the victim companies wired a combined total of $120 million to the fake Quanta bank account. This real-world example shows that even the largest tech giants on the planet can fall victim to these elaborate schemes.

3.2 - Save The Children BEC Attack

In 2017, the US non-profit organization 'Save The Children' was hit by a $1 million BEC Scheme. This scheme demonstrates how attackers are willing to target charitable organisations for their own financial gain.

According to the organisations 2017 income tax returns report [30], an attacker posed themselves as a Save The Children employee and falsely claimed funds were needed for solar panels at Pakistan health centres. Further online research shows that Save the Children has had operations in Pakistan since 1979, specifically in relation to "health and nutrition programs" [31]. The attacker well researched their target organisation to make the scheme believable.

The attacker successfully tricked the organisation into sending $997,400 to an entity in Japan. Unfortunately, this scheme was not discovered until May 2017 by which time it was not possible to recover the funds. Save The Children reported that through insurance carriers they were able to receive $885,784, which recovers much of the financial loss.

Save The Children claims to have worked towards strengthening their internal cybersecurity following this incident.

3.3 - Puerto Rico Government BEC Attack

In 2020, it was reported that the Puerto Rico government had lost $2.6 million due to a successful BEC scheme [32].

Puerto Rico's Industrial Development Company (a government agency) received an email which claimed there was a change in bank accounts tied to remittance payments. The email originated from an account which belonged to an employee working for the Puerto Rico Employment Retirement System, it was later discovered the account had been hacked. This resulted in an employee wiring $2.6 million to a fraudulent account in the US mainland. A further $1.5 million was reportedly sent from Puerto Rico's Tourism Company.

The attack was first noticed by Government Officials when an employee at the retirement agency enquired into funds which had not yet been received, despite being sent. The incident was then reported to the FBI.

The Associated Press [32] reported that the payments sent to the fraudulent account involved public pension funds. An executive director of PRIDC claimed that procedures were not followed and that three employees had been fired as a result [33].

This attack shows that even the government of a US territory can fall victim to BEC, not just enterprise organisations.

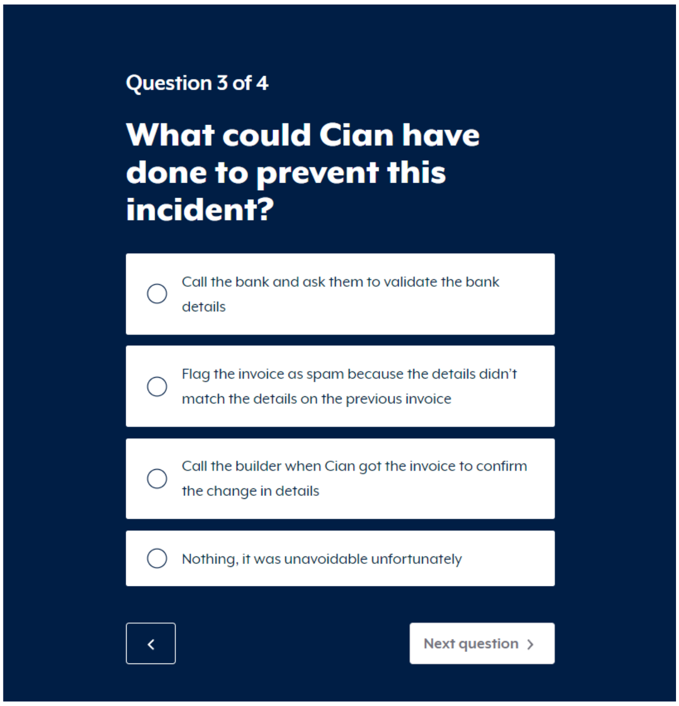
4 – Business Email Compromise Courses & Training Materials

In this section, online courses and teaching materials that cover or claim to help increase awareness around Business Email Compromise are outlined.

4.1 - 'Would you know what to do if you were a victim of business email compromise?'

'Would you know what to do if you were a victim of business email compromise?' [34] is a short quiz testing the user's knowledge around identifying Business Email Compromise provided by the Australian Cyber Security Centre.

A high-level definition of BEC and steps to follow if targeted are provided prior to the quiz, which is free and available to anyone. The quiz takes the participant through one scenario and tests their knowledge with multiple choice questions. In the scenario, 'Cian' had hired a builder to preform renovations. Cian received an invoice from what appeared to be the builders account and paid it; however, he received a phone call from the builder a month later claiming no payment had been sent. It turns out that the builder had been the victim of a BEC attack, and the money had been sent to a fraudulent account.



Question 3 of 4

What could Cian have done to prevent this incident?

○ Call the bank and ask them to validate the bank details

○ Flag the invoice as spam because the details didn't match the details on the previous invoice

○ Call the builder when Cian got the invoice to confirm the change in details

○ Nothing, it was unavoidable unfortunately

Figure 14: Question 3, 'Would you know what to do if you were a victim of business email compromise?' [34]

Upon completing the short quiz, the participant is provided with their results and a breakdown of each question.

4.2 - ‘Phishing Staff Awareness Training Programme’

‘Phishing Staff Awareness Training Programme’ [35] is a paid course provided by ‘IT Governance UK’ which is targeted for both individual (1-2 users) and corporate (1-1000 users) use. The annual subscription for this course is adjusted per quantity of licenses required, starting at £20 (approx. €22) per licence for 1-50 users.

According to the course description it covers social engineering, how phishing attacks work, how to identify phishing emails, tactics used by cyber criminals, what to do if targeted and tests employee understanding. The course is advertised as having short duration (45 minutes) and can be retaken multiple times. Tracked participation is provided for compliance and that the course is updated quarterly to stay on top of the latest trends.

Additionally, a monthly newsletter is provided to staff with the most recent developments and threats related to phishing.

IT Governance UK advertises this course as a way to protect against business email compromise [36].

4.3 - ‘Business Email Compromise by Tyler Hudak and Aaron Rosenmund’.

This course is available on the online learning platform ‘Puralsite’ which requires a subscription (starting at €26 per month). The course description claims that *“This course will teach you to prevent, detect, and when you must, respond to Business Email Compromise cyber attacks”*. [37]

The high-level description further elaborates that the course will cover how BEC attacks work, who they target, and techniques used by attackers. The participant will have acquired the skills to prevent, detect and respond to a BEC attack upon completing the course, which has an advertised duration of 114 minutes and appears to be in a video format.

4.4 - IT Security: Business E-mail Compromise

This paid BEC course is provided by ‘vubiz’ (an e-learning company) and appears to be targeted towards organisations, priced at $30 (approx. €30) per person for 100+ users and $20 (approx. €20) per person for 500+ users.

The course overview claims that users will learn how attackers spoof email accounts, common BEC schemes, characteristics of BEC emails and how to prevent having their email account compromised. The course is specifically designed for employees in HR and finance and has an advertised length of 30 minutes. [38]

4.5 - Nano Self Study: What is Business Email Compromise?

The ‘Nano Self Study: What is Business Email Compromise?’ course was developed by the Association of Certified Fraud Examiners and is available for individual use for $11 (approx. €11). This course claims to teach the user how business email compromise works and ways to prevent and respond to them.

According to the ACFE, “Nano self-study courses are 10-minute explorations of specific anti-fraud topics.”. [39]

4.6 - Business Email Compromise Readiness Assessment

Provided by Palo Alto Networks, the Unit 42 ‘Business Email Compromise Readiness Assessment’ helps prepare organisations through targeted risk assessments with the aim to best defend the organisation against BEC. It is available in three different tiers which matches the needs of specific organisations.

Unit 42 provides cyber awareness training enhancements which aims to educate employees on how to identify, report and prevent email-based attacks. Additionally, Unit 42 focuses on an organisation’s security controls and its effectiveness in responding to and recovering from a Business Email Compromise Incident.

Palo Alto Networks claim that this assessment delivers:

- Security Configuration Assessment
- BEC Threat Briefing
- BEC Incident Response Tabletop Exercise
- Email Compromise Assessment
- Readiness Benchmark
- BEC Incident Response Playbook
- Purple Team Exercise
- Cyber Awareness Training

The ‘Unit 42 ‘Business Email Compromise Readiness Assessment’ goes beyond employee awareness training and provides the security controls required to help defend organisations against BEC attacks by planning, assessing, and testing. [40]

4.7 - MetaCompliance Phishing and Ransomware: 'MetaPhish'

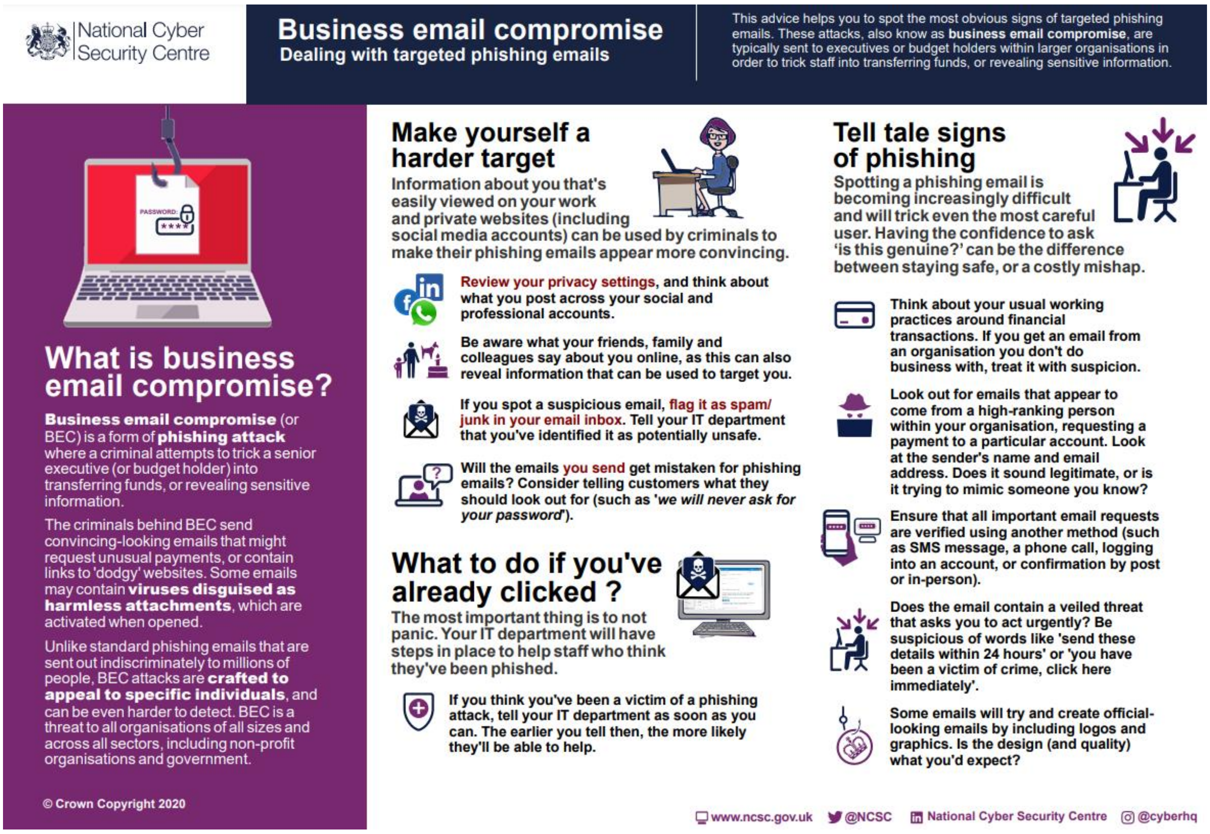
In their 'How Business Email Compromise Works?' [41] article, MetaCompliance suggests that phishing simulation exercises help in educating employees about BEC. MetaPhish provides phishing exercises which tests the level of awareness amongst employees and has been used by Irish local government organizations, such as Cork County Council.

'Metaphish' is fully customizable providing a range of templates and allows for the creation of an internal phishing drill in an organisation. [42]

4.8 – Articles and online materials

In addition to the courses outlined in this section, many articles and other online materials that educate users about Business Email Compromise are available. Many such resources can be found in the references section of this document.

An example of an online resource that can be used to provide awareness around BEC, is an infographic from the UK National Cyber Security Centre. This graphic provides some key information around BEC in a digestible format and could be used to remind employees of their awareness training. It clearly outlines what BEC is, how to prevent yourself becoming a target, steps to take if you believe you've been targeted and the signs of a phishing email.



National Cyber Security Centre

Business email compromise

Dealing with targeted phishing emails

This advice helps you to spot the most obvious signs of targeted phishing emails. These attacks, also know as **business email compromise**, are typically sent to executives or budget holders within larger organisations in order to trick staff into transferring funds, or revealing sensitive information.

What is business email compromise?

Business email compromise (or BEC) is a form of **phishing attack** where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain **viruses disguised as harmless attachments**, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are **crafted to appeal to specific individuals**, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

© Crown Copyright 2020

Make yourself a harder target

Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing.

Review your privacy settings, and think about what you post across your social and professional accounts.

Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.

If you spot a suspicious email, flag it as spam/ junk in your email inbox. Tell your IT department that you've identified it as potentially unsafe.

Will the emails you send get mistaken for phishing emails? Consider telling customers what they should look out for (such as '*we will never ask for your password*').

What to do if you've already clicked ?

The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished.

If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The earlier you tell then, the more likely they'll be able to help.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

Think about your usual working practices around financial transactions. If you get an email from an organisation you don't do business with, treat it with suspicion.

Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

Ensure that all important email requests are verified using another method (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person).

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

Some emails will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Figure 15: UK National Cyber Security Centre Business Email Compromise Infographic [43]

Useful online resources that educate on BEC include an article from Microsoft [13] which covers the types of BEC attacks, how the schemes typically work, email examples and tips to prevent BEC. This article is well formatted, easy to follow and concise which would make it more accessible to those who may not work in the IT industry, such as finance and HR employees who are common targets of BEC.

Alternatively, Trend Micro have an extensive article covering many of the same topics in greater detail [14]. This article was published in 2016 making it somewhat outdated, however a 3-minute video which cover the basics of BEC could be a useful resource for increasing general awareness.

5– Online quiz recourses

The purpose of this project is to develop electronic teaching materials in ordered to teach people about Business Email Compromise. This course will ideally be taken online and should be easily deployed by organisations wishing to enrol employees. In this section, several resources and methods which could be used to build the quiz elements of the online course are outlined.

5.1 – PHP/MYSQL

PHP and MySQL could be used to develop a custom quiz within a web application, using a MySQL database to store questions, choices, track user progression and results. PHP is a "is a widely used open-source general-purpose scripting language that is especially suited for web development and can be embedded into HTML." [44]. MySQL is a "relational database management system (RDBMS)" which is based on SQL (structured query language). According to Orcale (the developers of MySQL) it is the world's second most popular database and powers popular applications such as Twitter and Netflix [45].

PHP and MySQL would allow for the implementation of operations such as user creation, user login/logout functionality, storing credentials, storing questions/choices and grades.

5.2 – Google Forms Quiz

In addition to building a custom quiz, several existing online resources are available that provided pre-existing tools to implement many of the operations and features outlined in section 5.1.

Google Forms provides inbuilt functionality that allows users to create and grade quizzes. According to online documentation provided by Google [46], users can create a variety of question types (including multiple choice, checkboxes and dropdown), assign point values per question, allow participants to see missed questions/correct answers, and grade quizzes/provide induvial feedback. Additionally, users can decide to collect emails of participants in order to track progress, completion and release grades.

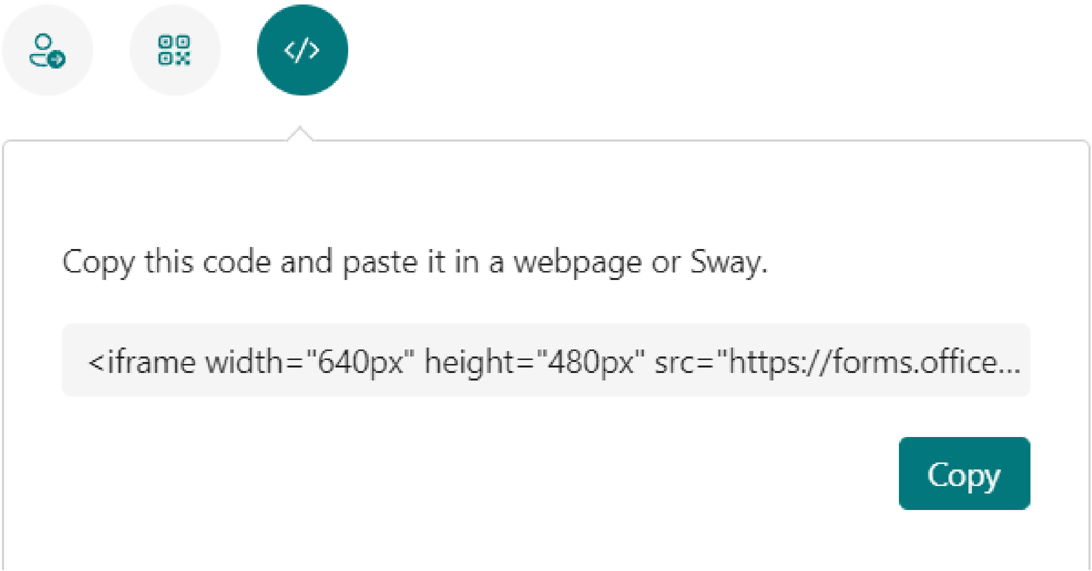
A link to the Google Forms quiz could be presented after each module of the course is completed.

5.3 – Microsoft Forms Quiz

Like Googles offering, Microsoft provide a quiz functionality within their own ‘Forms’ software.

According to online support documentation from Microsoft, forms can be used to add questions, select question type (multiple choice, shuffle options, drop down etc.), select choices/correct answer and assign points to questions. Forms provides a review responses tab with real-time information about your quiz including average score. As Forms is a Microsoft service it is well integrated with other Microsoft applications, for example a user can choose to review all response data in Excel [47].

Microsoft forms allows for quizzes to be embedded in websites and automatically generates a HTML inline frame code to load the quiz into a HTML page. This would allow course content and quizzes to be self-contained within one web application.



Copy this code and paste it in a webpage or Sway.

```
<iframe width="640px" height="480px" src="https://forms.office...
```

Figure 16: Automatically generated code to embed Microsoft forms quiz in a HTML page

5.4 – Moodle

Moodle is an open-source learning platform that is “designed to provide educators, administrators and learners with a single robust, secure and integrated system to create personalised learning environments.” [48]

Moodle can be installed onto a user’s web server, providing a highly customisable ‘all in one’ style platform. The advantage of Moodle is that it allows for users to create electronic teaching materials through an easy to navigate user interface. Unlike the three previous resources mentioned already, Moodle would allow for the creation of course content and multiple-choice quizzes all within one platform. It provides the functionality required to create a course that can be used to teach users about Business Email Compromise.

Operations such as account creation, user progress tacking and log in/log out are all handled by Moodle and do not require extensive PHP and MySQL knowledge. Another advantage of Moodle is that it's a well-established platform used by learners and educators around the world.

References

[1] “My Blue Linux,” 03 March 2019. [Online]. Available: https://www.mybluelinux.com/what-is-email-envelope-and-email-header/. [Accessed 29 October 2022].

[2] CloudFlare , “Cloudflare,” [Online]. Available: https://www.cloudflare.com/learning/dns/dns-records/dns-mx-record/. [Accessed 29 October 2022].

[3] R. Awati, “Tech Target,” [Online]. Available: https://www.techtarget.com/whatis/definition/IMAP-Internet-Message-Access-Protocol. [Accessed 29 October 2022].

[4] “H2 2022 Report Brand Impersonation Phising,” [Online]. Available: https://abnormalsecurity.com/resources/h2-2022-report-brand-impersonation-phishing [Accessed 18 October 2022].

[5] D. Higgins, “Info Security Magazine,” 01 04 2021. [Online]. Available: https://www.infosecurity-magazine.com/opinions/cyber-criminals-fool-april-fools/. [Accessed 21 October 2022].

[6] J. Bouwmeester, “Techaeris,” 8 December 2020. [Online]. Available: https://techaeris.com/2020/12/08/more-employees-clicking-phishing-emails/. [Accessed 21 October 2022].

[7] J. Daly, “USECURE.IO,” [Online]. Available: https://blog.usecure.io/does-security-awareness-training-work. [Accessed 21 October 2022].

[8] “IC3.gov,” 2021. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. [Accessed 22 October 2022].

[9] “Greathorn,” 2021. [Online]. Available: https://info.greathorn.com/hubfs/Reports /2021-Business-Email-Compromise-Report-GreatHorn.pdf. [Accessed 22 October 2022].

[10] Cisco , “Cisco,” [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html. [Accessed 29 October 2022].

[11] J. MCCLYMER, The emergence of social engineering in America, 1890-1925 : an essay in the history of the new middle class, 1974.

[12] Proofpoint , “Proofpoint,” [Online]. Available: https://www.proofpoint.com/us/threat-reference/social-engineering. [Accessed 29 October 2022].

[13] “Proofpoint, Whait is Phishing,” [Online]. Available: https://www.proofpoint.com/us/threat-reference/phishing. [Accessed 11 November 2022].

[14] “APWG, Phishing Activity Trends Report,” 23 February 2022. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf. [Accessed 12 November 2022].

[15] “Checkpoint, What is Phising,” [Online]. [Accessed 11 November 2022].

[16] B. Huddleston, “AppRiver, In Progress Phishing with a sense of urgency,” [Online]. Available: https://appriver.com/blog/in-progress-phishing-with-a-sense-of-urgency. [Accessed 12 November 2022].

[17] “Crowdstrike, Spear Phishing,” [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/. [Accessed 14 November 2022].

[18] N. Cveticanin, “DataPort, Phishing Statistics,” 26 September 3033. [Online]. Available: https://dataprot.net/statistics/phishing-statistics/#:~:text=Phishing%20scam%20statistics%20reveal%20that,within%20an%20hour%20of%20receipt.. [Accessed 13 November 2022].

[19] “Mimecast, Whaling Phishing Attack,” [Online]. Available: https://www.mimecast.com/content/whaling-phishing-attack/. [Accessed 14 Novemeber 2022].

[20] “Proofpoint, What is Smishing,” [Online]. Available: https://www.proofpoint.com/uk/threat-reference/smishing. [Accessed 14 November 2022].

[21] “Bank of Ireland, Phishing and Smishing examples,” [Online]. Available: https://www.bankofireland.com/security-zone/gallery-of-phishing-and-smishing-examples/. [Accessed 14 November 2022].

[22] M. Ahola, “USecure, Types of Phishing Attack,” [Online]. Available: https://blog.usecure.io/types-of-phishing-attack. [Accessed 15 November 2022].

[23] “Microsoft,” [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec. [Accessed 22 October 2022].

[24] “TrendMicro,” 11 January 2016. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes. [Accessed 22 October 2022].

[25] FBI, “Business E-mail Compromise: The 3.1 Billion Dollar Scam,” FBI, 2016.

[26] Central Statistics Office , “CSO,” November 2021. [Online]. Available: https://www.cso.ie/en/releasesandpublications/fp/fp-psolo/pulsesurvey-ourlivesonline-remoteworknovember2021/workingremotely/. [Accessed 23 October 2022].

[27] “RTE,” Brian O'Donovan, 8 September 2022. [Online]. Available: https://www.rte.ie/news/2022/0908/1321379-working-from-home-survey/#:~:text=It%20shows%20that%20nationally%20in,home%20is%20Dublin%20at%2039%25.. [Accessed 23 October 2022].

[28] “Bleeping Computer, Lithuanian Jailed for Stealing $120 Million From Google, Facebook,” Sergiu Gatlan, 19 December 2019. [Online].

Available: https://www.bleepingcomputer.com/news/security/lithuanian-jailed-for-stealing-120-million-from-google-facebook/. [Accessed 30 October 2022].

[29] “Department of Justice (United States),” 19 December 2019. [Online]. Available: https://www.justice.gov/usao-sdny/pr/lithuanian-man-pleads-guilty-wire-fraud-theft-over-100-million-fraudulent-business. [Accessed 30 October 2022].

[30] “Save The Children, STC-990-2017 (Income Tax Returns),” 2017. [Online]. Available: https://www.savethechildren.org/content/dam/usa/reports/advocacy/stc-990-2017.pdf. [Accessed 30 October 2022].

[31] “Save The Children Pakistan,” [Online]. Available: https://pakistan.savethechildren.net/about-us/our-history. [Accessed 30 October 2022].

[32] D. COTO, “Assoaciated Press - Official: Puerto Rico govt loses $2.6M in phishing scam,” 13 February 2020. [Online]. Available: https://apnews.com/article/puerto-rico-caribbean-ap-top-news-us-news-latin-america-e03bea7e491b9c95350887880376562f. [Accessed 01 November 2022].

[33] A. Press, “Security Week, 3 Employees Suspended in $4M Puerto Rico Online Scam,” 14 February 2020. [Online]. Available: https://www.securityweek.com/3-employees-suspended-4m-puerto-rico-online-scam. [Accessed 01 November 2022].

[34] “Australian Cyber Security Centre,” [Online]. Available: https://www.cyber.gov.au/learn/threats/business-email-compromise. [Accessed 05 November 2022].

[35] “IT Goverance, Phising Staff Awareness Training Program,” [Online]. Available: https://www.itgovernance.co.uk/shop/product/phishing-staff-awareness-training-programme. [Accessed 5 November 2022].

[36] “IT Governance, What is BEC,” [Online]. Available: https://www.itgovernance.co.uk/blog/what-is-bec-business-email-compromise-definition-and-prevention. [Accessed 5 November 2022].

[37] “Puralsite, Malware Buisness Email Compromise,” [Online]. Available: https://www.pluralsight.com/courses/malware-business-email-compromise?exp=2. [Accessed 5 November 2022].

[38] “Vubiz, IT Secrutiy: Buisness E-mail Compromise,” 5 November 2022. [Online]. Available: https://vubiz.com/home/it-security-business-e-mail-compromise. [Accessed 5 November 2022].

[39] “ACFE, What is Business Email Conpromise,” [Online]. Available: https://www.acfe.com/training-events-and-products/all-products/product-detail-page?s=What-is-Business-Email-Compromise. [Accessed 5 November 2022].

[40] “Palo Alto Networks,” [Online]. Available: https://www.paloaltonetworks.com/unit42/assess/business-email-compromise. [Accessed 5 November 2022].

[41] J. MacKay, “MetaCompliance, How Business Email Compromise Works,” 15 February 2022. [Online]. Available: https://www.metacompliance.com/blog/cyber-security-awareness/how-business-email-compromise-works. [Accessed 5 November 2022].

[42] “MetaCompliance, Phising and Ransomware,” [Online]. Available: https://go.metacompliance.com/capterra/metaphish?utm_source=Capterra&utm_campaign=capterra+-+metaphish [Accessed 5 November 2022].

[43] “NCSC, Buisness Email Compromise Infographic,” 2020. [Online]. Available: https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf. [Accessed 5 November 2022].

[44] PHP.net, “What is PHP,” [Online]. Available: https://www.php.net/manual/en/intro-whatis.php. [Accessed 03 February 2023].

[45] Oracle, “What is MySql?,” [Online]. Available: https://www.oracle.com/mysql/what-is-mysql/. [Accessed 03 February 2023].

[46] Google Support, “Create & grade quizzes with Google Forms,” [Online]. Available: https://support.google.com/docs/answer/7032287?hl=en#zippy=%2Cmake-an-answer-key-assign-points-add-automatic-feedback%2Cchoose-what-people-see-during-and-after-the-quiz%2Csend-your-quiz-to-people-outside-of-your-work-or-school. [Accessed 03 February 2023].

[47] Micorsoft , “Microsoft Support,” [Online]. Available: https://support.microsoft.com/en-us/office/create-a-quiz-with-microsoft-forms-a082a018-24a1-48c1-b176-4b3616cdc83d. [Accessed 03 February 2023].

[48] Moodle, “About Moodle,” 14 July 2022. [Online]. Available: https://docs.moodle.org/401/en/About_Moodle#:~:text=Moodle%20is%20a%20learning%20platform,Moodle%20Partners%20to%20assist%20you.. [Accessed 16 April 2023].