

# Business Email Compromise Course – Final Report

NAME: BEN NAGLE  
STUDENT NUMBER: C00247271  
SUPERVISOR: PAUL BARRY

## **Abstract**

The purpose of this document is to discuss the development and implementation of this final year project and demonstrate what was learned and achieved throughout the year.

## Contents

Introduction .....	3
1 - Description of Submitted Project.....	4
1.2 - User Experience .....	6
2 - Description of Conformance to Specification and Design .....	13
3 - Description of Learning:.....	15
3.1 - Technical Achievements:.....	15
3.2 - Personal Achievements:.....	17
4 - Review of Project .....	18
4.2 - What would I do differently? .....	19
4.3 - Recommendations: .....	19
4.4 - Concluding Thoughts: .....	20
Acknowledgments.....	20
Bibliography .....	21
Declaration of Plagiarism .....	22

## Introduction

The purpose of this document is to outline and discuss the development and implementation of this final year project, a Business Email Compromise Course which aims to teach email users about the subject and teach them the skills required to identify compromised emails.

In this document, a description of the submitted project is described focusing on the modules that were developed to form the overall course and how the course was implemented. Using screenshots, the user experience navigating and interacting with the course, on the open-source learning management system 'Moodle', is outlined in detail.

The submitted project is compared to the original specification and design, reasons for diverting from the original specification and technologies is explained and justified. The experience gained by re-evaluating the original implementation is discussed. This document also outlines the achievements, both technical and personal, gained in the undertaking of this final year project.

Finally, a reflection on the project experience is discussed. This section focuses on what went right, what went wrong and how the project evolved throughout its evolution. How this project may have been approached differently is explored and advice for someone attempting a similar project in the future is provided. Justification is given for whether the project met its original requirements.

## 1 - Description of Submitted Project

This project aims to create a series of electronic teaching materials which can be used to educate email users about Business Email Compromise, focusing on how to identify a compromised email and the appropriate steps to take. The course would have a one-hour duration and be graded.

The course, titled 'Business Email Compromise Course', has been created using the PHP based open-source learning management system 'Moodle' [1]. The course is divided into six modules, which aim to teach the user about a specific topic. The course is divided into modules to present the content in a user friendly and digestible manner, each module concludes with a three to five question quiz which the user must pass to complete the module. Once all modules are complete with a passing grade (60 points or higher), the participant has completed the course.

The first module of the course, 'I may not be who you think I am', introduces the participant to the concept of phishing emails. This module focuses on mass-mail phishing examples, such as schemes attempting to trick users into believing an email has come from a trusted organisation such as PayPal or Microsoft. Using real-world examples, the module provides the participant with tips to protect themselves from such scams and indicators to look out for when evaluating the trustworthiness of an email.

BEC Course / Module 1: I may not be who you think I am

LESSON


### Module 1: I may not be who you think I am

✓ Done: View   ✓ Done: Go through the activity to the end   ✓ Done: Receive a grade   ✓ Done: Receive a passing grade

#### Use of Public Domains

Emails sent from large and established organisations will never be from a public domain (such as 'gmail.com' or 'outlook.com'), they will likely use their own unique domain. The below example is a major indicator that this email is fraudulent and not really from 'Paypal'.

**From:** Paypal Support <[resolvetransport11@outlook.com](mailto:resolvetransport11@outlook.com)>  
**Date:** March 27, 2017 at 11:07:15 PM PDT  
**To:** ██████████@hotmail.com"  
**Subject:** Important - Your Account Has Been Limited (Case ID : #PP 690-293-728-351)



Paypal would never use a domain **outlook.com**

Next

You have completed 42% of the lesson

42%

Figure 1: Module 1, Use of Public Domains

Module 2 explores the concept of ‘Account Compromise’ and introduces users for the first time to the term BEC. The modules content aims to teach users the dangers of falling for phishing emails and what attackers may aim to do with their credentials should they successfully steal them.

The third module focuses on teaching the participant on how to identify spoofed emails, especially those that appear to be from a trusted source such as a manger, CEO or friend. The module introduces more sophisticated forms of phishing, like BEC, that are more targeted and can be more difficult to identify on a surface level.

Module 4 delves into how BEC attacks work, by explaining the five types of BEC attacks identified by the FBI. The purpose of this module is to give the participant an idea of the types of schemes used by attackers so that they have a clearer understanding on what to be on the look out for. Famous examples of BEC attacks with large financial consequences are covered to demonstrate how devastating BEC can be to an organisation.

The fifth module starts where the fourth left off, now providing the participant with specific examples of BEC style emails (such as the bogus invoice scheme). Unlike in previous modules, instead of a formal quiz, there are three questions related to the content throughout the module that tests users on the contents.

BEC Course / Module 5: How to identify BEC?

LESSON


## Module 5: How to identify BEC?

✓ Done: View   ✓ Done: Go through the activity to the end   ✓ Done: Receive a grade   ✓ Done: Receive a passing grade

In this example, an attacker posing as Dan Jones (CEO) messages an employee (Dianne) with an urgent request to transfer funds enclosed in an attached invoice.

From: Dan Jones <Dan.Jones@arrow-hawk.com>  
Date: Tuesday, 22nd September 2020 at 17:57

Subject: Urgent Transfer of Funds Required



Hi Dianne,

Please could you urgently transfer the funds enclosed in the attached invoice before you leave today.

Sorry to ask for this so close to the end of the day, the partner we are working with needs to receive the funds today or our project will fall through.

I would appreciate if you could confirm when this has been completed.

Many thanks,

Dan




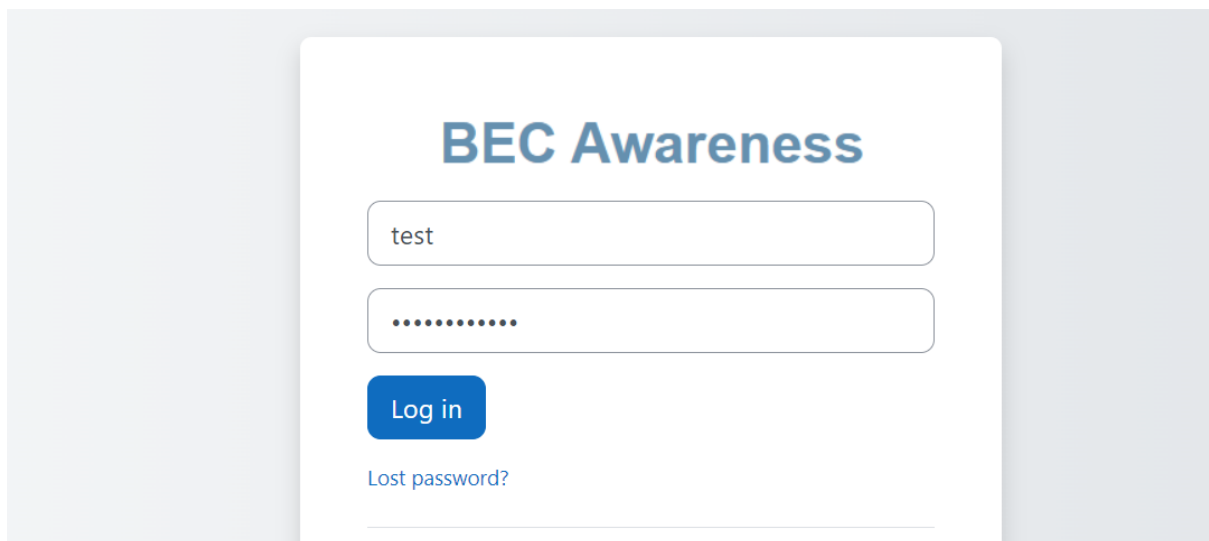
Figure 2: Module 5, CEO Fraud

Module 6, the final module, aims to satisfy the remaining goal of this project – provide users with the steps to take should they receive a suspicious email. This module builds upon the tips the user learned in the first module, by specifically suggesting tips to handle the receipt of more sophisticated compromised emails.

It's hoped that upon the completion of this course that participants will have gained knowledge on not only how to identify phishing, spoofed and compromised emails – but also how to deal with such and the steps they should take to protect themselves and their organisation.

## 1.2 User Experience

When the user first visits the Moodle site, they must enter their login credentials (provided by their administrator). For the purposes of this demonstration, I have created a user 'test'.



*Figure 3: BEC Awareness login page*

Once authenticated, the user is presented with the 'Home' page which displays the available course – Business Email Compromise.

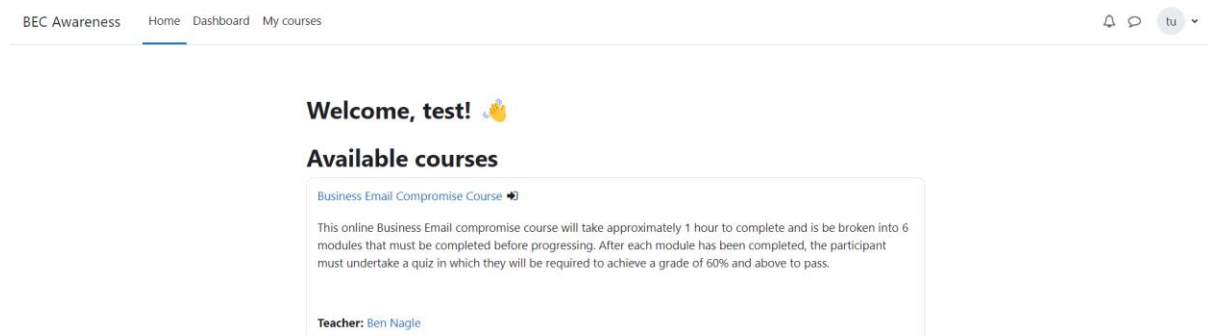


Figure 2: BEC Awareness Home page, with the available courses displayed to the user.

Once the course is selected, the user may choose to enrol themselves with Moodle's 'self-enrol' extension. Once enrolled, the user can begin to take the course either all at once or at their own leisure.

## Business Email Compromise Course

### Enrolment options

[Business Email Compromise Course](#)

This online Business Email compromise course will take approximately 1 hour to complete and is broken into 6 modules that must be completed before progressing. After each module has been completed, the participant must undertake a quiz in which they will be required to achieve a grade of 60% and above to pass.

Teacher: [Ben Nagle](#)

#### Self Enrolment

No enrolment key required.

[Enrol me](#)

Figure 4: The user must enrol in the course before beginning.



Once enrolled, the user is presented with the main course page and their attention is diverted to the modules and activities via the user guide. On the home page, the user is presented with the course instructions which they must acknowledge. This is demonstrated in the next set of screenshots.

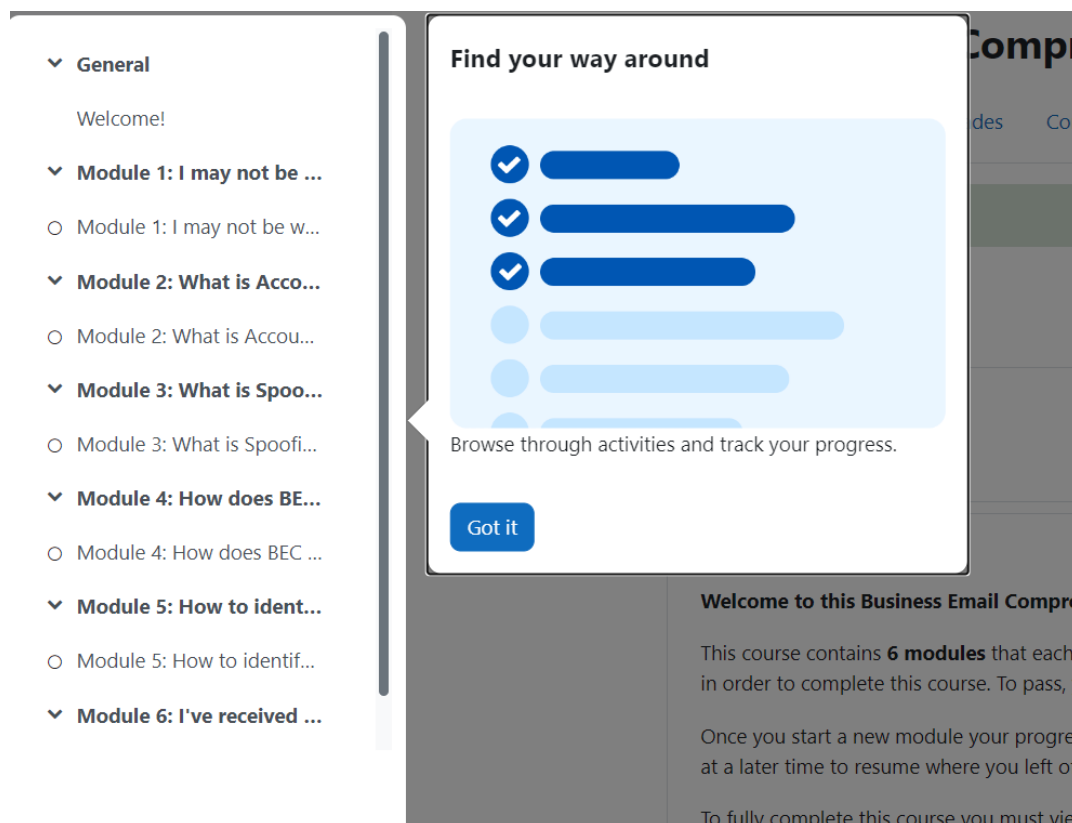


Figure 5: The user is introduced to the modules and activities.

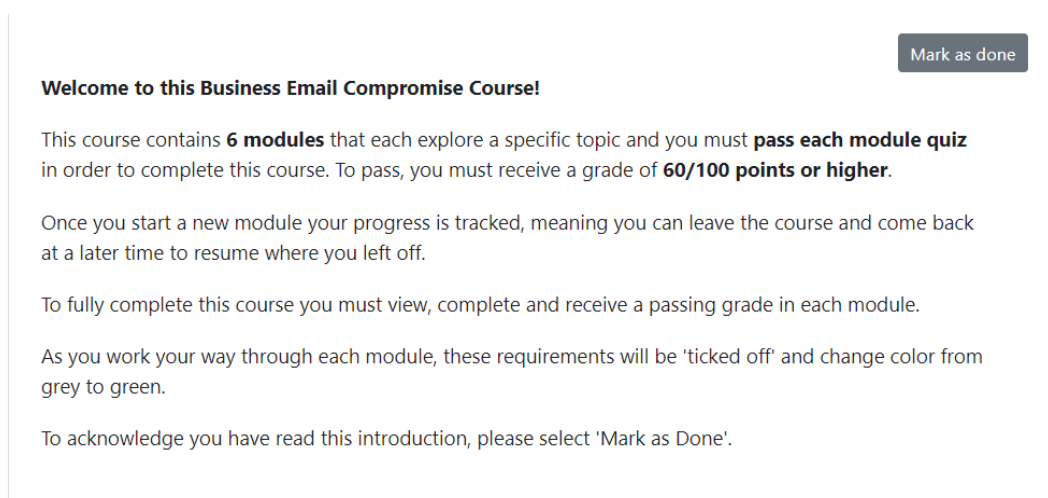


Figure 6: Course Instructions which the user must acknowledge.

The user may then make their way through each module, as they progress through the content, they must meet the requirements required to pass. The requirements are that the user views the module, goes through it until the end, receives a grade and receives a passing grade. The two screenshots below demonstrate a module before and after the user has met the requirements. Once the user achieves a passing grade, they will be presented with a screen congratulating them for their achievement.

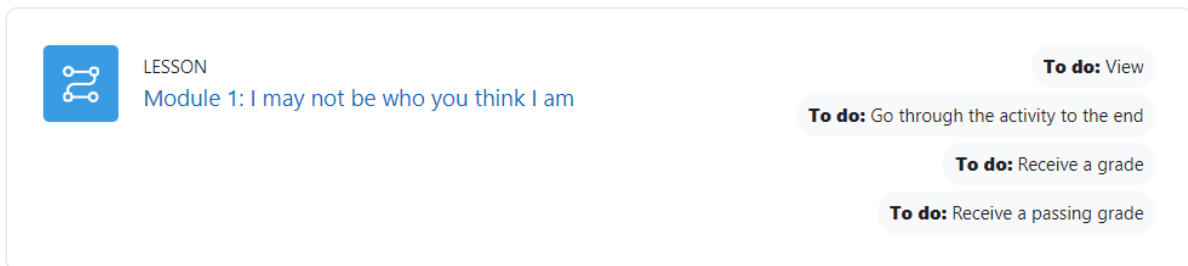


Figure 7: Module 1 lesson activity before the user meets the requirements.

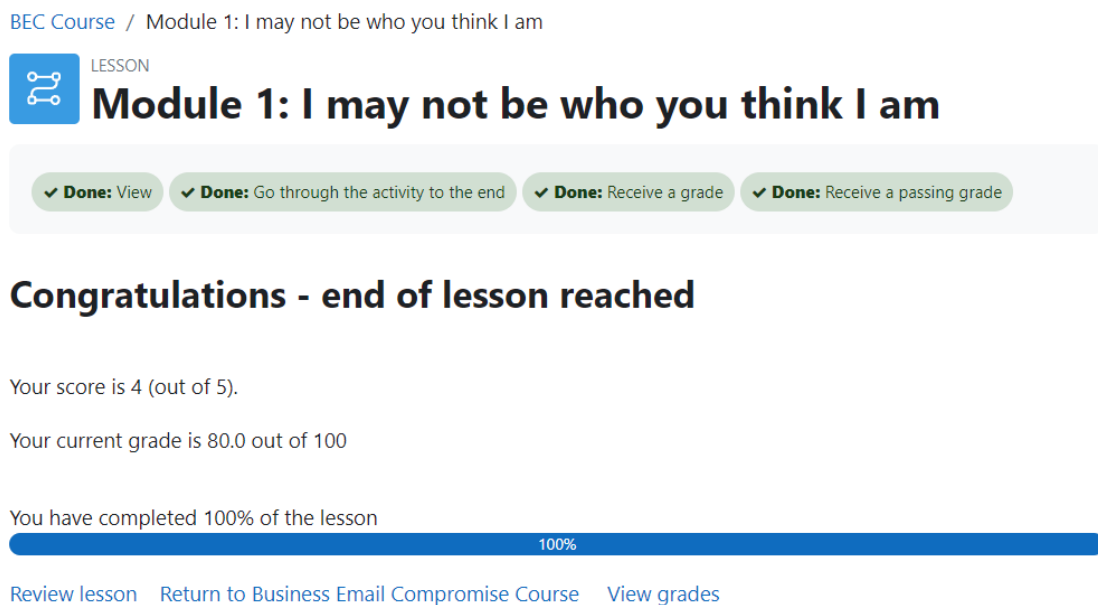
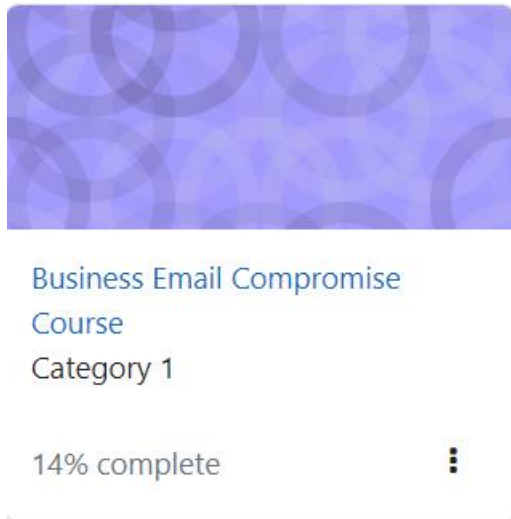


Figure 8: Module 1 lesson activity after the user meets the requirement, this module is now passed.



*Figure 9: Now that Module 1 is complete, this is reflected in the overall course completion percentage.*

The course can be taken at a user’s leisure, and should they require to exit during a module the site will remember where they left off. This allows the user to resume the module and not have to resit content they have already covered. As this course is partly designed for employees, it is important that they can do the course over the workday and step out when needed.

The next screenshot is an example of the type of course content that users are presented, this screen shot is taken from module 3 ‘*What is Spoofing?*’. On the previous page, the user was asked to identify potential red flags in the email (which is an example of spoofing) and they are now shown the indicators that this email is not legitimate.

## Module 3: What is Spoofing?

✓ Done: View   ✓ Done: Go through the activity to the end   ✓ Done: Receive a grade   ✓ Done: Receive a passing grade

### Remember... I may not always be who you think I am!



Here are some of the indicators this email is not from 'John Tuncer'

- The display name 'John Tuncer' seems legitimate, but take a look at the sender's email address 'officeceo1@earthlink.net'. You would expect the sender's address to include John's name and the domain to be your organisation's
- Take a look at the email text, notice the grammatical error "i have....", this may be an indicator the email is fraudulent.
- "i will appreciate a swift email response" - remember phishing/fraudulent emails will often include urgent language like this

Next

Figure 10: Module 3 – 'What is Spoofing?'

The course contains a total of 26 multiple choice questions, modules 1 through 4 have five questions each whilst modules 5 and 6 (which are the shortest) have three. For demonstration purposes I have included two different styles of questions used in the course. The first asks the user to identify the steps they should take to protect themselves from BEC, the second presents the user with a scenario in which they are asked to identify the indicators the email shown is not legitimate.



LESSON

## Module 6: I've received a suspicious email - now what!?

✓ Done: View

To do: Go through the activity to the end

To do: Receive a grade

To do: Receive a passing grade

What can you do to protect yourself from BEC? (choose two)

- Share your credentials (username with password) over email if requested
- Always click on links or download attachments that appear to be from your manager or high ranking official.
- Report suspicious emails to your IT Security department
- Be very cautious of emails requesting an urgent wire transfer even if they appear to be from a legitimate or trusted source.

Submit

You have completed 63% of the lesson

63%

Figure 11: Module 6 quiz question

You work at the University College Dublin and you've just received the following email from your colleague Carl Smith:

From: Carl Smith <corl.smith.ucd@gmail.com>  
Subject: Urgent Request!!!  
Time: 04:12

Hello,

I need you to transfer €20,000 to the following bank account:

Account Name: Ireland Construction Ltd.  
Number: 0044560793

Please let me know when this is done, I'm busy in a meeting and this is urgent!!

Thanks,  
Carl

You suspect that the email is not really from Carl. Which of the following indicate that this email is not legitimate?  
(Select all that apply)

- The email body has mis-spellings that appear unprofessional.
- The subject line includes multiple exclamation marks ("Urgent Request!!!")
- The email is sent from a personal email account (gmail.com), rather than a UCD business account.
- The email was sent outside of normal working hours
- The request is for a large sum of money to be transferred to an unfamiliar account

Submit

Figure 12: Module 3 Quiz question

The user ‘test’ has now completed the course and met all requirements. An Admin can check the progress of individual users who are enrolled in the course, as demonstrated below.

Grade item	Calculated weight	Grade	Range	Percentage	Feedback	Contribution to course total
Business Email Compromise Course						
LESSON Module 1: I may not be who you think I am	16.67 %	✓ 80.00	0-100	80.00 %		13.33 %
LESSON Module 2: What is Account Compromise?	16.67 %	✓ 100.00	0-100	100.00 %		16.67 %
LESSON Module 3: What is Spoofing?	16.67 %	✓ 100.00	0-100	100.00 %		16.67 %
LESSON Module 4: How does BEC work?	16.67 %	✓ 100.00	0-100	100.00 %		16.67 %
LESSON Module 5: How to identify BEC?	16.67 %	✓ 100.00	0-100	100.00 %		16.67 %
LESSON Module 6: I've received a suspicious email - now what!?	16.67 %	✓ 66.67	0-100	66.67 %		11.11 %
AGGREGATION Course total	-	546.67	0-600	91.11 %		-

Figure 13: ‘test user’ grades

Users can also view their own grades for each individual module and the course overall. Having completed and passed the course, a participant may go through the content a second time if they wish.

## 2 - Description of Conformance to Specification and Design

In my original functional specification, written in December 2022, I had intended to create a web application using PHP [2], HTML , CSS, JavaScript, and MySQL [3] to develop the course. In the early stages of the project’s development, I began to create the specifications I had set out in this document using diagrams and descriptions I had outlined.

After creating a home page and the first module, I decided to use Microsoft forms [4] embedded in the web application to handle the quizzes. My thought process for this decision was that it would allow me to focus more on creating the course content rather than spending too much time using PHP and MySQL to create the multiple-choice quizzes. Also, it would allow participants to use their existing Microsoft credentials (college, personal or work) to complete the course. In my re-evaluation, I had determined that the most important element of this project was the course content and I needed prioritise this over all else. Microsoft forms, it seemed, would allow me to focus my energy on the content of the

course and provided a platform for me to create multiple choice quizzes with the questions and answers I had developed.

However, when implementing this design, I encountered issues. Without an Azure subscription (so that I could register my web application with Microsoft), it would be almost impossible it seems to have fully integrated forms with my web application. I attempted to use JavaScript to capture the users score from the Microsoft form quiz so that it could be verified if they passed. I had much trouble in trying to achieve this and I believe that because my web application was hosted externally (on my local machine) from Azure, it would not be possible to fully integrate forms into the course.

As a result, there would be no way of preventing a user who failed module one from moving on and completing the rest of the course, for example. This meant that it would not be possible to “force” a user to complete all modules and pass before completing the course. I then decided to once again re-evaluate my approach and researched platforms that are used by real-world organisations to handle internal training.

I decided that the Moodle platform would provide the integration and functionality required, so I installed the latest version of Moodle on my local XAMPP [5] server and began transferring the content from my old web application to my new Moodle site that I had created during the installation process. Moodle did present its own unique set of challenges, namely the learning curve associated with using a platform I was unfamiliar with. I was satisfied with the level of customisation available on the platform having taken time to “experiment” with different features (such as the various activities available to build your course with). Moodle provided the platform required to put together a course that could be used by organisations to train employees.

Though my submitted project does not match my original specification and design, the changes implemented were necessary to ensure I could create a course that meets the requirements of the project and provides a better experience for the participants of the course.

### 3 - Description of Learning:

#### 3.1 - Technical Achievements:

Over the course of completing this project, due to the re-evaluations and changes of direction as outlined in the previous section, I gained technical experience in a variety of areas – both expected and unexpected.

In the early stages of developing this Business Email Compromise course, I improved my skills in HTML, PHP, MySQL and CSS. Even though I ultimately decided to abandon my original web application, I gained skills in creating it. For example, prior to embarking on this project my skills in CSS and web design were lacking. When developing the original web application, I for the first time thought out every decision (placement of buttons, text, image, margins, size etc.) so that the user experience for the course would be optimal.

An example of the home page of my original web application and some of the content from module one are demonstrated in the below screenshots.

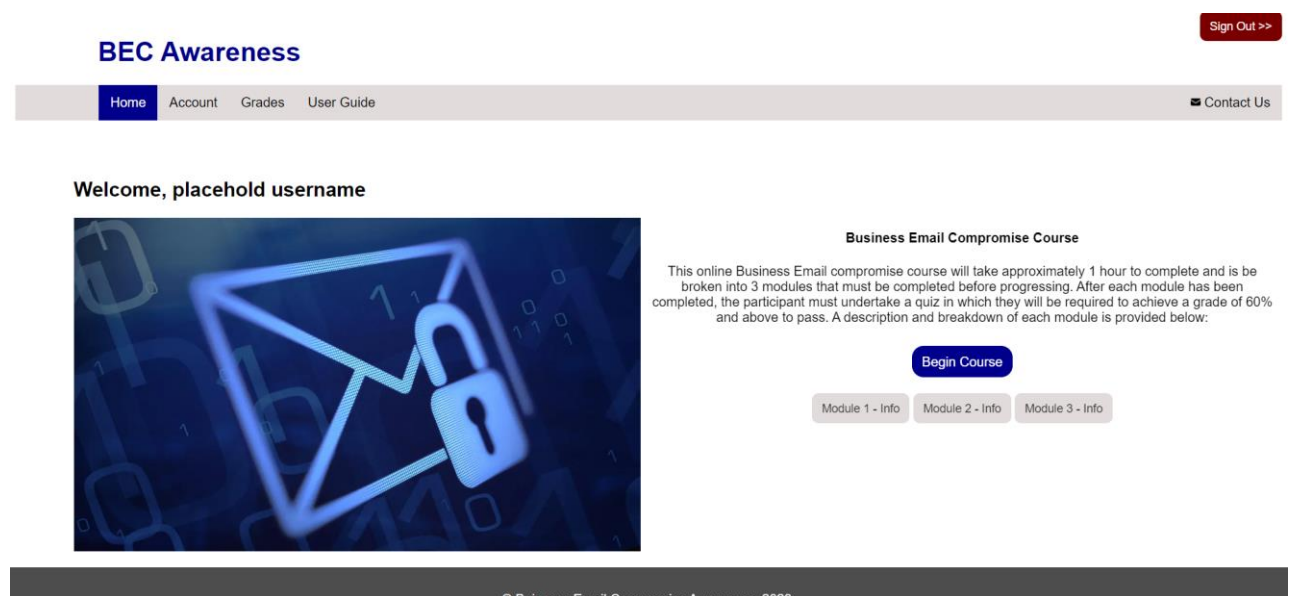


Figure 14: The original home page based off my design diagram in the functional specification document.



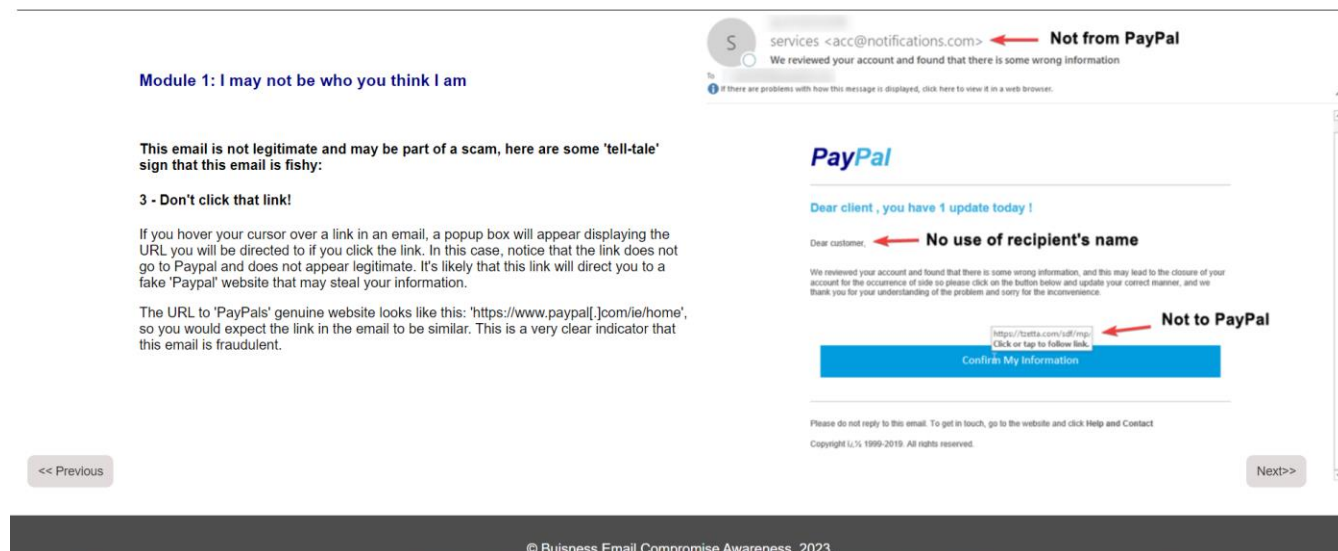


Figure 15: An early version of 'Module 1'

After changing direction and settling on the Moodle platform, I had to quickly adapt to using it. After the initial installation, I spent a week researching to determine the best way to create the course I wanted in Moodle. I settled on the 'Lesson' activity [6] to bring each module and quiz to life, as it allowed me to add both content and question pages and also offered customisations such as buttons (which 'jump' the user to the next page), progress menus, completion requirements and minimum scores.

Having familiarised myself with Moodle and deciding on how to implement the course, I began the process of adding each content and MultiChoice page required in the lesson activity for each module.






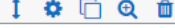


Misspelt / Unusual Domain Names	Content	Next page	 Add a new page... ▾
Use of Public Domains	Content	Next page	 Add a new page... ▾
Urgent Language/Request	Content	Next page	 Add a new page... ▾
Spelling/Grammar errors	Content	Next page	 Add a new page... ▾
Request Sensitive Information	Content	Next page	 Add a new page... ▾
Suspicious Attachments	Content	Next page	 Add a new page... ▾
Suspicious Links	Content	Next page	 Add a new page... ▾
Module 1 Quiz	Multichoice	Next page Next page Next page Next page	 Add a new page... ▾

Figure 16: Edit Module 1 admin page

Once I gained the appropriate technical skills in Moodle, I was able to add each module to the course and re-focus my attention on the course content.

### 3.2 - Personal Achievements:

In terms of personal achievements, prior to this project I had never taken on a task that would require constant dedication and work over the course of an academic year. I had to learn how to manage my time on this project in balance with the rest of my modules, work, and personal life. Projects that I had worked on before would span the course of no more than a couple of months, so ensuring that I managed and split the workload over the course of the year for this project presented a new challenge.

I learned the value of thorough research and that its okay to stop, reevaluate and change direction from a predefined plan if necessary. This was a valuable learning experience that I'm sure not to forget.

## 4 - Review of Project

In this section, I will reflect on my over all project experience. From the offset, I was aware that this project would require a lot of research. Therefore, my focus for the first few months was solely on researching Business Email Compromise extensively. As my Research document began to come together, I realised that I would have to widen the scope of my research significantly if I was to develop a course aimed at non-technical users.

This involved going back to basics, focusing my research on how email works, the email delivery process and the technologies that make it happen. I also realised I would have to establish foundation, so I set myself the question – “How did we end up with attacks like Business Email Compromise?”.

To answer that question, I researched the origins of the term “social engineering” and how its definition evolved over the decades. In doing this background research, I discovered that BEC scams are no different than scams of centuries passed – only that they’ve evolved and become more sophisticated with advancements in technology.

I also researched broader email related cyber security issues, like phishing, spoofing and email account compromise. Educating participants of the course about these issues and attacks would make it easier to explain BEC and provide them with the tools to not only identify sophisticated spear phishing and BEC emails, but also more generic campaigns like mass mail Phishing.

Another area of research was existing tools, courses and online materials surrounding Business Email Compromise. I discovered during my research that few courses seem to specifically teach email users about these more sophisticated schemes like BEC.

However, an oversight in my research was realised as I began to put the course together using a web application which I had created using HTML, CSS and PHP. I came to the realisation that I had focused my research so much on the course content, that the technologies I would use became an oversight. Creating a web application from scratch was slowing me down. I had to learn, for example, how to create a PHP/MySQL multiple choice quiz, store user results/answers, track user progress, manage scores/grades, encrypt user data, facilitate the creation of accounts, encrypt passwords, include secure session management, create a user-friendly interface and so on.

Upon reflection, I realized that my focus has been diverted from the most crucial aspect of my project: developing a Business Email Compromise course. The course content, including multiple choice questions and the wording used to make the course as clear and understandable as possible held a greater significance. I decided to incorporate Microsoft Forms into my existing web application as it seemed to be the best solution that allowed me to retain much of my original work. However, I now recognise that this decision may have been rushed and I did not properly evaluate the pros and cons associated with it.

Although on the surface this appeared like an appropriate solution, over time I realised that it presented its own set of unique problems. Notably, that there was no way for me to confirm a user had passed a quiz within the web application, meaning a user could complete

all of the modules but fail all of the associated quizzes with no penalties. With this problem, my course would not be appealing to organisations wishing to educate employees around the subject matter of BEC.

I again went back and did further research, this time focusing on platforms that I could use to build my course and that's when I settled on Moodle which seemed to strike the balance between customisation and prebuilt features. Now, users could log into their account, complete the course in their own time (as progress is saved and tracked) and they would not reach 100% completion until requirements (outlined earlier) were met. On the admin side, they could track and view a breakdown of the grades and status of all enrolled users. I was then able to focus my time and energy on producing each module.

Once 'back on track' the course, it's content and quizzes, started to come together. I feel that making the decision to drastically change descion in the end benefitted my final submitted project.

#### **4.2 - What would I do differently?**

Based on what I just described in the prior section, if I was to start this project again, I would have not overlooked the technologies. Perhaps had I properly thought out my approach during the research phase, I would have avoided wasted time and stress associated with having to change my original implementation plan. I made the mistake of focusing too much on researching the course content itself and should have made myself aware of the various options of implementation, instead of building everything from scratch. Of course, change of plans are inevitable in a project of this scale and unexpected or unforeseen challenges can arise, but if I could have perhaps realised Moodle was a good platform for creating teaching materials sooner, I could have avoided changing direction.

However, there was value gained form this experience. I learned that it's okay take a step back and change your original plan, it's better to choose a path that will result in a better overall finished project than stubbornly stick to your original plan.

#### **4.3 - Recommendations:**

I would advice someone doing a similar project in the future to ensure they strike the balance between researching the subject matter (in this case BEC) and the electronic teaching materials used to bring the eventual course to life. I didn't realise such open source platforms existed at first and that attempting to build everything from scratch was not necessary.

Additionally, I would recommend that they be open for changes in direction and scope. As you research and learn new things, you may come across new areas that may be worth delving into more. In order to create a course that will teach people about your subject matter, you need to have a good, well rounded knowledge of it and expanding the scope of

your research where necessary can be helpful. But like most things, do this in moderation and you do not want to spend too long on a topic that may not be entirely relevant.

Reports (such as the FBI internet crime report and others) can be a great primary source when researching BEC and other topics in Cybersecurity. During my research, if an article referenced or mentioned a specific report, I would look for the original document itself to source my information and get more context. When developing a course like this, it's important that you try and find as accurate source information as possible.

#### **4.4 - Concluding Thoughts:**

Overall, I feel as though my project was a success in the end. I managed to complete my goal of creating a series of electronic teaching materials that educate email users about Business Email Compromise. The Moodle site I developed allows for registered users to enrol in the course and work their way through six modules in which they will learn and be tested on areas surrounding email security such as phishing, account compromise, spoofing and of course Business Email Compromise.

Users who participate in the course should be more aware of the various type of BEC schemes used by threat actors and should be less susceptible to their attacks.

#### **Acknowledgments**

I would like to give a special thanks to my project supervisor, Paul Barry, for his continued support, guidance and advice throughout the year which was greatly appreciated.

## Bibliography

- [1] Moodle , “Moodle Docs, Installing Moodle,” 30 December 2022. [Online]. Available: [https://docs.moodle.org/401/en/Installing\\_Moodle](https://docs.moodle.org/401/en/Installing_Moodle). [Accessed 17 April 2023].
- [2] PHP, “php.net,” [Online]. Available: <https://www.php.net/>. [Accessed 17 April 2023].
- [3] MySQL, “MySQL 'The world's most popular open source database',” [Online]. Available: <https://www.mysql.com/>. [Accessed 17 April 2023].
- [4] Microsoft , “Microsoft Forms,” 2023. [Online]. Available: <https://forms.office.com/Pages/DesignPageV2.aspx>. [Accessed 17 April 2023].
- [5] Apache Freinds , “XAMPP Apache + MariaDB + PHP + Perl,” 2023. [Online]. Available: <https://www.apachefriends.org/>. [Accessed 17 April 2023].
- [6] Moodle, “Moodle Docs, Lesson Activity,” 21 May 2022. [Online]. Available: [https://docs.moodle.org/401/en/Lesson\\_activity](https://docs.moodle.org/401/en/Lesson_activity). [Accessed 17 April 2023].

## Declaration of Plagiarism



I declare, this document in this submission in its entirety is my own work except for where duty acknowledged. I have cited the sources of all the quotations, paragraphs, summaries of information, tables, diagrams, or other material. This includes software and other electronic media that is integral property rights may reside. I have provided the complete biography at the end of my document detailing all the works and resources used in the presentation of this submission. I am aware that failure to comply with the Institute’s regulations governing plagiarism constitutes a serious offense.

<b>Student</b>	Ben Nagle
<b>Tutor</b>	Paul Barry
<b>Institution</b>	South East Technological University
<b>Title</b>	Business Email Compromise Course – Final Report
<b>Submission Date</b>	17 <sup>th</sup> April 2023

Ben Nagle

17/4/2023

Signature

Date