



# Abertay University

## **An Examination into and Evaluation of 'GoPhish'**

**Declan Doyle**

1600219

Ethical Hacking 3

BSc Ethical Hacking  
Year 3

2018-2019

# Abstract

Email is used frequently in businesses and organisation as a way of communicating instantly without the need for paper or any physical materials. Email technologies have advanced so that it is no longer just text that is sent back and forth. HTML and other languages can be used in email to make them more appealing in design and functionality. One of these new functions is the addition of hyperlinks, where links can be put inside emails that will take the user to a webpage. Both these new features and email, in general, have been exploited to get users to do things they would not normally do. Phishing emails attempt to get a user to click on a link that will either download a malicious file to the user's computer or get them to enter credentials to a fake site, effectively handing those credentials over to an attacker. In order to prevent phishing emails, users must be aware of them, and how to spot them.

GoPhish is a tool created to help organisations train their staff to spot phishing emails and be more resilient towards them. They claim that it is easy to use and effective in demonstrating the dangers of phishing emails. By setting up a GoPhish server, and creating two campaigns, these claims were tested.

It was found that GoPhish is an excellent tool designed perfectly for purpose. It is straightforward to set up, and with detailed instructions, even a non-technical user could do so. It also conclusively demonstrates key characteristics of phishing emails and can make it incredibly difficult to differentiate between a legitimate and malicious email. The tool has detailed analytics that can provide an organisation with the information needed to efficiently direct resources at the areas of their organisation which need improved resilience. Overall, GoPhish meets the aims it sets out to achieve.

# Table of Contents

1. Introduction	1
1.1.Aims	1
1.2.Phishing	1
1.3.GoPhish	2
2. Procedure	3
2.1.Installation	3
2.2.Set up	5
2.2.1.Sending Profiles	5
2.2.2.Landing Pages	7
2.2.3.Email Templates	9
2.2.4.Users and Groups	11
2.3.Starting a Campaign	12
3. Results	13
3.1.Abertay Campaign	13
3.2.Facebook Campaign	14
4. Discussion	16
4.1.Countermeasures	17
5. References	18

# 1. Introduction

## 1.1. Aims

- To demonstrate how to set-up and use the open source tool 'GoPhish' with clear and concise instructions that can be replicated by reading this report.
- To evaluate the effectiveness of 'GoPhish' as a phishing tool, and how it can be used to launch a successful phishing campaign.

## 1.2. Phishing

Phishing is the name given to the act of impersonating a person or organisation and attempting to fool an unsuspecting victim that this person or organisation wishes them to do something. This is usually attempting to get a victim to click on a link in an email which will either download a malicious file to the victims device, or take them to a web page where they can insert credentials to what they believe is a legitimate site, but is, in fact, a fraudulent site set up by an attacker. The credentials entered can then be used by this malicious actor to log into the legitimate site, and the user is none the wiser.

There are different types of phishing attacks. General phishing attacks aim to be sent to a vast number of victims in hopes that even if a tiny percentage click on the malicious link and fall victim to the attack, that is still a significant number of people. Spear phishing is a targeted phishing attack. This consists of an attacker crafting a message or email specifically designed for an individual or a small group of people. These attacks require information on a target and so are usually paired with other social engineering attacks and open source intelligence gathering. Whale phishing is the name given to a phishing attack aimed a very large 'fish' - a high ranking member of an organisation. These targets can be easier than the average employee of a company as these targets have a great deal of authority in companies and organisations, and so rules and company policies, such as only using a work email address, may not apply to them. CEO fraud is the opposite of whale phishing and is a specific type of spear phishing. An attacker will impersonate a CEO or a high up official in an organisation and target the finance department pretending to authorise a transfer of funds to a different account.

There are several key characteristics of a typical phishing email. These can be used to spot a phishing email amongst legitimate ones. Firstly, the email will often appear too good to be true. It will offer something or have attention-grabbing statements within the body of the email. These are designed to attract a victim's attention immediately, with the promise of them winning large amounts of money, or a prize of some sort. The only caveat is that a user will have to enter their bank details or address to receive the prize. Another characteristic is a sense of urgency. The email will often contain language that conveys to the victim that if they do not act fast, they will either miss an opportunity to win something or be locked out of an account. Phishing emails will almost always contain a link to a webpage. These links will also almost always never link to a legitimate site. They will usually be to clones of the sites they are impersonating, getting a victim to input their credentials to that site, effectively giving them to the attacker. Emails may also contain malicious attachments that can be masquerading as information that might appeal to the user, such as a list of salaries at the company they work for. More often than not, these attachments will be pieces of malware that can cause significant damage. The final key characteristic of a phishing email is the sender of the email. If a special tool is not used to craft the email, then the sender may appear very unusual. It may come from an email address that a victim is not familiar with. (Phishing.org, 2019)

Phishing works a significant amount of time as it exploits a persons social interest, like being helpful or efficient. People cannot be patched or upgraded like computers, and so it is much harder to prevent phishing attacks compared to regular malware-based attacks. (Ncsc.gov.uk, 2019) The scale of phishing attacks is continually increasing. A study on email attacks on the Fortune Global 500 companies showed that so far in 2019, the amount of web-based social engineering attacks increased by 233% than the last quarter of 2018. (Proofpoint, 2019) The average cost of a phishing attack for a medium-sized company has been estimated at as much as \$1.6 million. (Katz and Katz, 2019) With the ease of setting up these attacks, and the minimal cost involved in bulk sending emails, it is clear why phishing is such a popular method of attack with cybercriminals.

### **1.3. GoPhish**

GoPhish is an open source tool that provides a phishing framework which can simulate real-world phishing attacks. It is designed to allow industry grade phishing training to be available to everyone. It has no cost due to its open-source nature and is written in the 'Go' programming language, which means it can be compiled with no dependencies, allowing for a 'click and go' experience. (Wright, 2012) Using GoPhish, organisations can replicate what an experienced malicious user could do when creating phishing emails. They can then send this to their staff, and see how they respond. Using this information they can better prepare themselves for an actual phishing attack. An organisation can also use GoPhish to train their staff on what to look for in phishing emails, giving real-world examples. GoPhish can also be used to not only test resilience to phishing attacks, but also general social engineering attacks. There is an example online of a person using GoPhish to test against USB dropping and seeing if staff in an organisation would plug in a USB into a company computer without checking to see if it contained malware. (Chrismerkel, 2019)

## 2. Procedure

### 2.1. Installation

In order to install GoPhish, a Digital Ocean virtual private server was deployed. This is a virtual server stored in the cloud, that can be configured to run various Linux distributions. For this evaluation, a digital ocean droplet was deployed with the Linux distribution, Ubuntu. This was selected as it is a versatile Linux distribution that is ready to be used as soon as the server is spun up.

#### Create Droplets

Choose an image 

Distributions Container distributions Marketplace Custom images

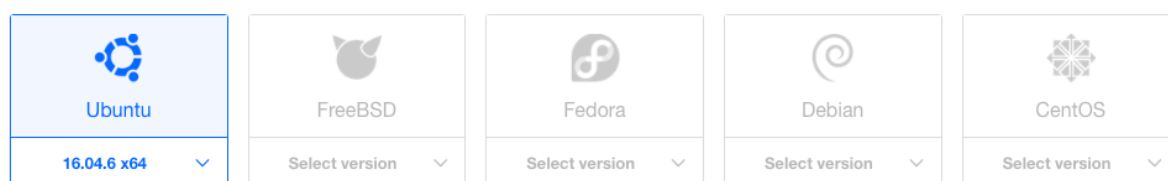


FIGURE 1 - DEPLOYING DIGITAL OCEAN SERVER WITH UBUNTU

Once the droplet was configured and running, it was accessed via the SSH protocol on a local computer. The droplet was given a public IP of 134.209.16.176, so SSHing to this address with the root user account resulted in a prompt for the password for the local machine's SSH key. Once this was entered, control over the droplet was achieved.

```
Declan — root@GoPhish-VPS: ~ — ssh root@134.209.16.176 — 82x24
[Declans-Mini:~ Declan$ ssh root@134.209.16.176
The authenticity of host '134.209.16.176 (134.209.16.176)' can't be established.
ECDSA key fingerprint is SHA256:WJryA/ciVGoEzoQ6NtCr/nF4PSuFWcQ9KJrimktmxGo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '134.209.16.176' (ECDSA) to the list of known hosts.
Enter passphrase for key '/Users/Declan/.ssh/id_rsa':
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-145-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

FIGURE 2 - SSH ONTO DROPLET

As stated previously, the Ubuntu distribution allowed the droplet to be ready for the GoPhish installation immediately. To begin this, the command 'wget' was used to download the GoPhish package from the internet:

```
wget https://github.com/gophish/gophish/releases/download/0.7.1/gophish-v0.7.1-linux-64bit.zip
```

Once this was downloaded onto the droplet, the package was unzipped and made an executable using the following command:

```
chmod +x gophish
```

Before the program could be launched, the configuration file had to be edited to allow the program to listen on all interfaces, so it has access to the internet. This was completed by editing the config.json file using the inbuilt text editor, Nano. The listen URL for the admin server was changed from 127.0.0.1 to 0.0.0.0, which meant that when the virtual server IP was navigated to on a web browser, the GoPhish admin login would be present.



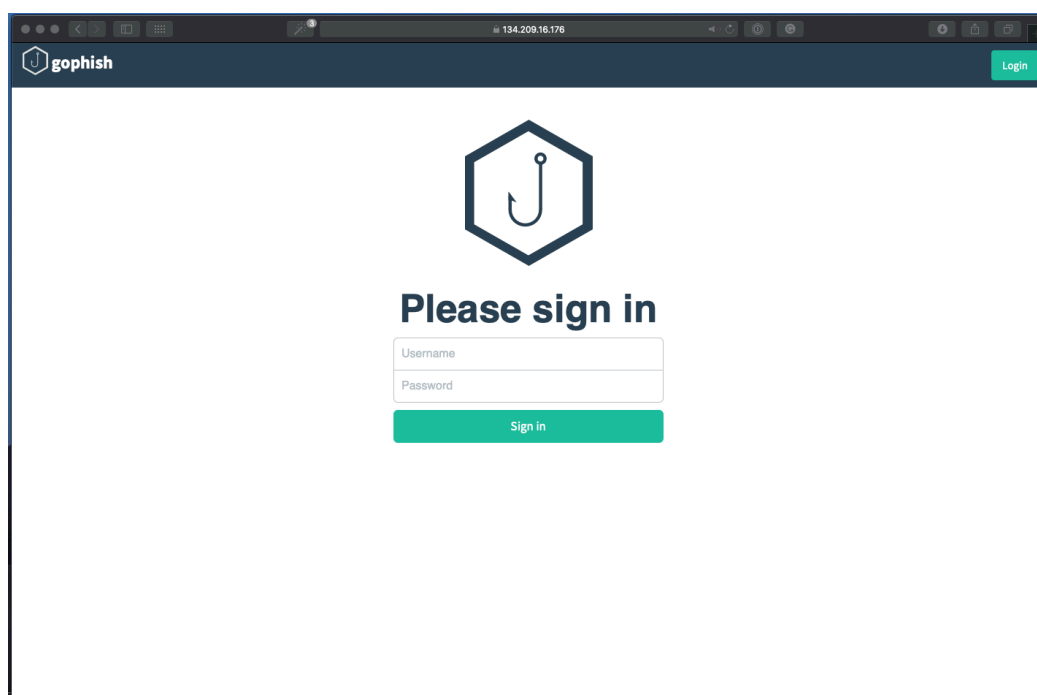
```
{  
  "admin_server": {  
    "listen_url": "0.0.0.0:3333",  
    "use_tls": true,  
    "cert_path": "gophish_admin.crt",  
    "key_path": "gophish_admin.key"  
  }  
}
```

**FIGURE 3 - CHANGING THE LISTEN URL**

Once the configuration was changed, the final stage in setting up the GoPhish server was to execute the GoPhish file on the Digital Ocean droplet. This was done with the following command:

```
./gophish
```

This resulted in GoPhish running, which was shown by opening a browser and navigating to the IP address of the droplet, with the port that GoPhish runs on: 3333.



**FIGURE 4 - GOPHISH LOGIN PAGE**

## 2.2. Set up

To log into the GoPhish web application, the username 'admin', and password 'gophish' should be used. GoPhish has 4 sections that need to be configured before a campaign can be run. These 4 sections consisted of adding a sending profile so that emails can be sent, creating a landing page so that when a link is clicked, there is a webpage that the user is redirected to. An email template also needs to be created, which will be sent upon starting a campaign, and finally, the users and groups must be set to who the campaign will be run against.

### 2.2.1. Sending Profiles

The sending profile is what is used by GoPhish to send emails to a target of a campaign. The profile is configured by firstly giving it a name so it can be identified. The user can then enter any email address they want, which will be the email address that GoPhish displays in the sent email. Note that this is not the actual email address that is used to send emails, but rather the email address that the victim will see. Following this, the host address of the SMTP server should be entered, as this is the server that will be used to send the email. There is then a username and password field for the credentials to the SMTP server. There is the option to ignore certificate errors, which allows GoPhish to ignore any certificate errors from the SMTP server, such as self-signed certificates. Finally, there is the option to add custom HTTP headers to the email so that further information can be doctored to result in a higher quality phishing email.

**New Sending Profile**

Name:

Interface Type:

From:

Host:

Username:

Password:

☒ Ignore Certificate Errors ⓘ

Email Headers:

Header	Value
X-Custom-Header	[[URL]]-gophish

Show  entries Search:

No data available in table

Showing 0 to 0 of 0 entries Previous Next

**FIGURE 5 - NEW SENDING PROFILE WINDOW**

To evaluate GoPhish as a phishing tool, two sending profiles were created. Firstly, before any profiles could be created, an email account with Google's email service, Gmail, was created to be used as the sender email address. The email address 'eh3project@gmail.com' was created and used for the duration of this project.

The first sending profile was given the name 'Abertay' as the first campaign will be an imitation of Abertay University's IT support. In the from field, the following was entered:

IT Service Desk <is@abertay.ac.uk>



This displays the sender email as a name which will read 'IT Service Desk'. This makes the email look like it has legitimately come from Abertay's IT department. The host field, as discussed earlier, requires the host address of the SMTP server. As a 'Gmail' address is used, Google's SMTP server is required, so the following was entered:

```
smtp.gmail.com:587
```

In the username and password fields, the credentials for the account created were entered, and the checkbox to ignore certificate errors was checked. No custom HTTP headers were entered, and this profile was completed and saved.

The second sending profile was created with the name 'Facebook' as it will be an email informing the victim that they have a new notification from a member of the Abertay Ethical Hacking Facebook group. In the from field, the following was set:

```
Colin Mclean <notification@facebook.com>
```

This displays the sender email as it would regularly from a facebook notification - the creator of the post appears to be the sender of the email, which in this instance is Colin Mclean. The remaining fields were the same as the previous sender profile, and so this profile was saved. Both sending profiles were now set up and ready for a campaign.

The figure shows two side-by-side screenshots of a web application interface for creating a 'New Sending Profile'. Both forms have the same layout and fields, but with different values entered.

**Left Form (Abertay Profile):**

- Name:** Abertay
- Interface Type:** SMTP
- From:** IT Service Desk <is@abertay.ac.uk>
- Host:** smtp.gmail.com:587
- Username:** eh3project@gmail.com
- Password:** [Masked]
- Ignore Certificate Errors:** ☒

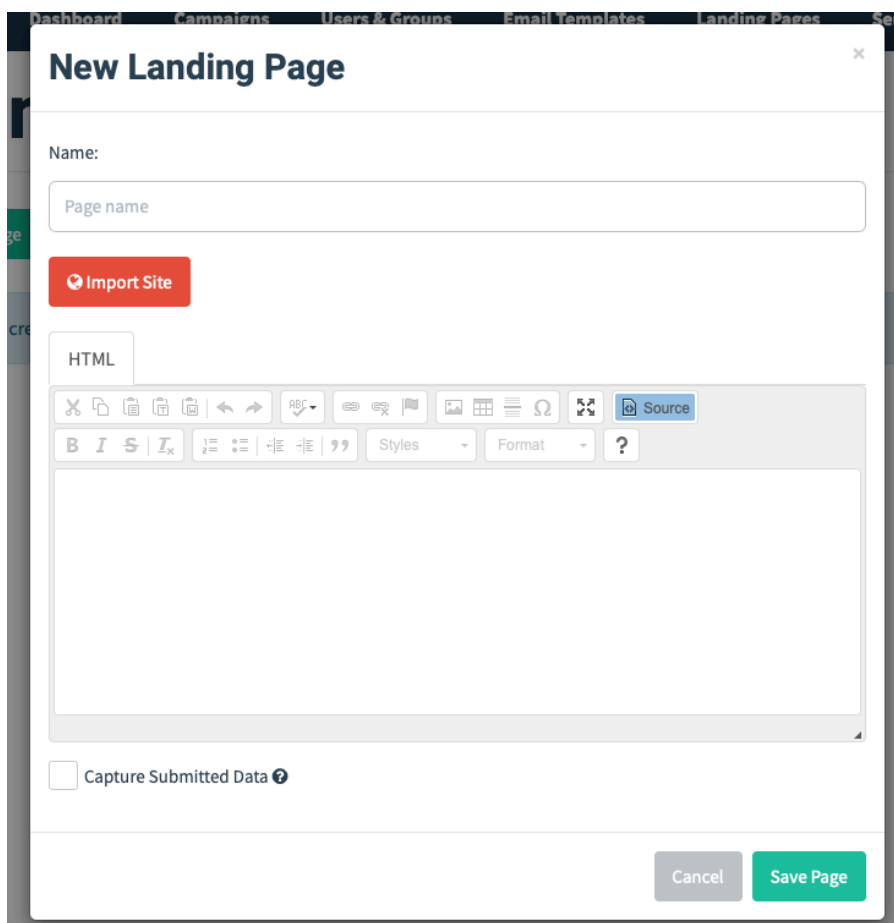
**Right Form (Facebook Profile):**

- Name:** Facebook
- Interface Type:** SMTP
- From:** Colin Mclean <notification@facebook.com>
- Host:** smtp.gmail.com:587
- Username:** eh3project@gmail.com
- Password:** [Masked]
- Ignore Certificate Errors:** ☒

**FIGURE 6 - SENDING PROFILES AS COMPLETE**

## 2.2.2. Landing Pages

The landing page is used by GoPhish when a victim clicks on a link within the email that they are sent. They are directed to the URL which will display whatever landing page is set in the campaign options. To set up a landing page, the user must first give it a name so it can be identifiable. Then there is the option to import a website, where GoPhish will take a URL and download all the HTML source code for that website so that it can be replicated. There is also the option to write HTML code if a custom landing page is preferred. Following this, there is a checkbox where if selected, GoPhish will capture any submitted data to the landing page, and there is an option to capture passwords too. If these options are chosen, then there is a field where the user can enter a URL where the landing page will redirect to if credentials are entered and a submit button is clicked. This can be used to fool a victim into thinking that they have entered their credentials to a legitimate site.



**FIGURE 7 - NEW LANDING PAGE WINDOW**

Two landing pages were created for this project. Following the themes of the campaigns that were to be launched, the first landing page impersonates the login page for the MyAbertay web application. This is used frequently by students at Abertay to access various services the University offers. The page was given the name 'MyAbertay', and the login page for the actual MyAbertay page was imported. No custom HTML was added as the desired page result was for the page to directly imitate the login portal for the MyAbertay page. Both checkboxes were selected for capturing submitted data and for passwords. These would only be test credentials in the actual campaign, so there was no concern over malicious behaviour. Finally, the redirected page was set to be the website for Abertay University so that the user will think something has gone slightly wrong and instead of being logged into MyAbertay, they have been logged into the main university page.

The second landing page was named 'Facebook' due to the second campaign being a Facebook phishing example. The Facebook login page was imported, and no custom HTML was added. Like previously, both checkboxes were selected so that credentials could be captured.

The redirect page was set to Facebook's homepage. Both landing pages were saved and were ready to be used in campaigns.

**New Landing Page**

Name: MyAbertay

**Import Site**

HTML

```
<!DOCTYPE html><html lang="en-GB"><head>
<base href="https://adfs.abertay.ac.uk/adfs/ls/?client-request-id=17205e1c-423c-4855-b7bd-2a58cc66844&username=&wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsredirect%3d%26estsrequest%3drQIIAZVT04-jVhQexjPOziJa
rKJI2SLFFKk2wuZpY2u3uGAbjMGM@NCgWAvzGLDh4jWX8UK2NC1XSrdlyi3T5CH1D2xSbD3KD4hSRaISxp5N
fkBOcY70450-83rSIFtk_3OmS3ssTN4p8cxOBNNRHM7RBInTIduJfI7jVuRq9_Hlo8-eX3361De1739-Yv8a
xYPX2EXpBS3Pb5WbN1g7Rmhb9Ntr0RkK6sCr_LTVaxafp61kyCEKEFPvu0huYAJxzwT-wLB3GPY7hr05LTp0
p0cx8MccCHQ5qseSLdWQY9XgU9XYIG2g7rU5Qa1UySgLOdWQ-Su9dhZOISTuamazWqltjJIDf2TykROffCP
">
```

☒ Capture Submitted Data

☒ Capture Passwords

**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: <https://www.abertay.ac.uk>

**Cancel Save Page**

**New Landing Page**

Name: Facebook

**Import Site**

HTML

```
<!DOCTYPE html><html id="facebook" lang="en"><head>
<base href="https://www.facebook.com/"><meta charset="utf-8"/><meta name="referr
er" content="default" id="meta_referrer"/><script>window.__cstart+=new Date();</scrip
t><script>function envFlush(a)(function b(b)(for(var c in a)b[c]=a[c])window.require
Lazy?window.requireLazy(["Env"],b):(window.Env=window.Env||{}),b(window.Env))envFlus
h({"ajaxpipe_token":"AXjBnQaXGxinks7g","timeslice_heartbeat_config":{"pollIntervalMs
":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":{"requestAnimationFrame":true,"
Event listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event list
```

☒ Capture Submitted Data

☒ Capture Passwords

**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

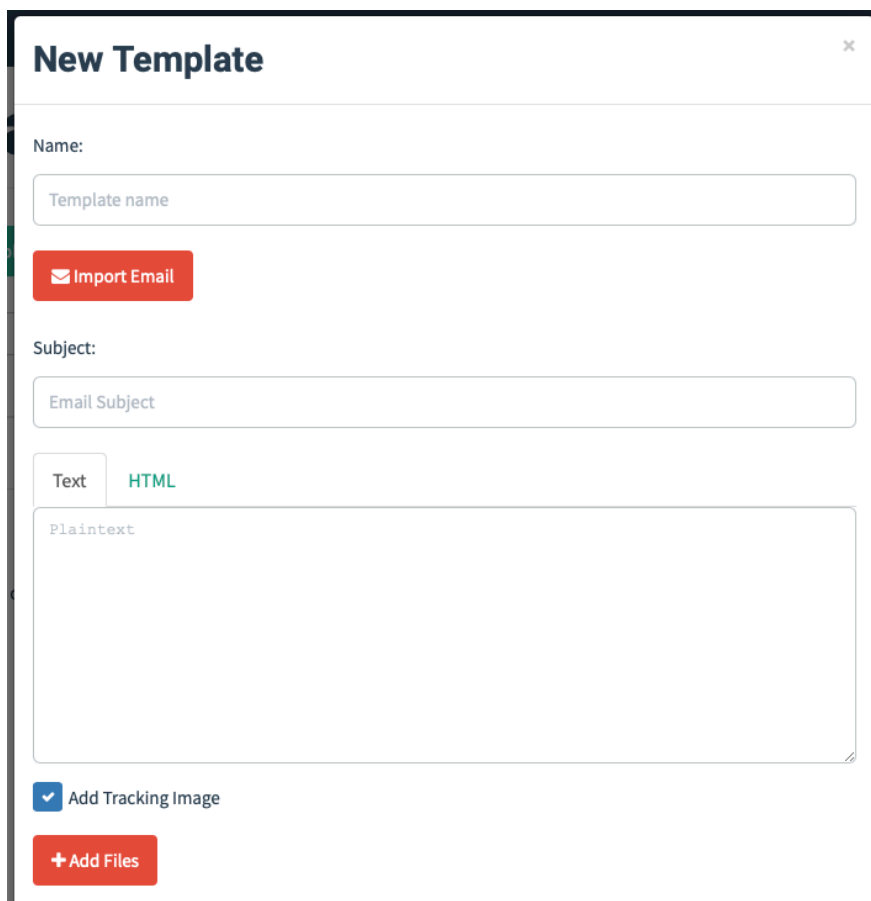
Redirect to: <https://www.facebook.com>

**Cancel Save Page**

FIGURE 8 - LANDING PAGES AS COMPLETE

## 2.2.3. Email Templates

GoPhish uses the email template as the design for the emails that will be sent to a victim. To create a new template, first, it must be given a name so it can be identified. There is then an option to import an email if the user has the source code for an email that they would like to be replicated. Then, there is a field for the email subject, which will be the actual subject of the email sent in a campaign. There is then a text box where the user can write an email with either plain text or HTML if they did not import an email, or wish to edit an imported email. There is a checkbox with the option to add a tracking image. This will insert a transparent image to the email which will allow GoPhish to track if the email has been opened. This helps with the analytics of a campaign. Finally, there is the option to attach a file to the email template.



**FIGURE 9 - NEW EMAIL TEMPLATE WINDOW**

As previously, two email templates were created for the project. Both followed the themes of the campaigns that will be launched when the setup process is complete. The first email template designed was designed to impersonate an email received from Abertay University's IT department about password renewal. It was given the name 'Abertay', and the subject was as follows:

IT Service Desk Notification: Your Abertay password is about to expire.

This was an actual subject of an email received from Abertay. No email source code was imported, but instead, a section of an email received from Abertay was copied. The body of an email informing a user that their password was about to expire was used. GoPhish allows a user to insert placeholder text which, upon launching a campaign, would be replaced with data that the user has entered. For example, in the email body, the first line was as follows:

Dear {{.FirstName}} {{.LastName}}

This allows GoPhish to replace the two placeholder texts with the first and last names of the victims the user has entered. This can also be done with a URL so that a link in an email can be

set to a link that will redirect to a landing page that the user has created. This was done in the Abertay email template. Finally, a tracking image was added to the email so that the campaign could be monitored more in-depth.

The second template was named 'Facebook' as it continued the theme for the second campaign. The email subject was set to the following:

[Abertay Ethical Hackers] Status Update

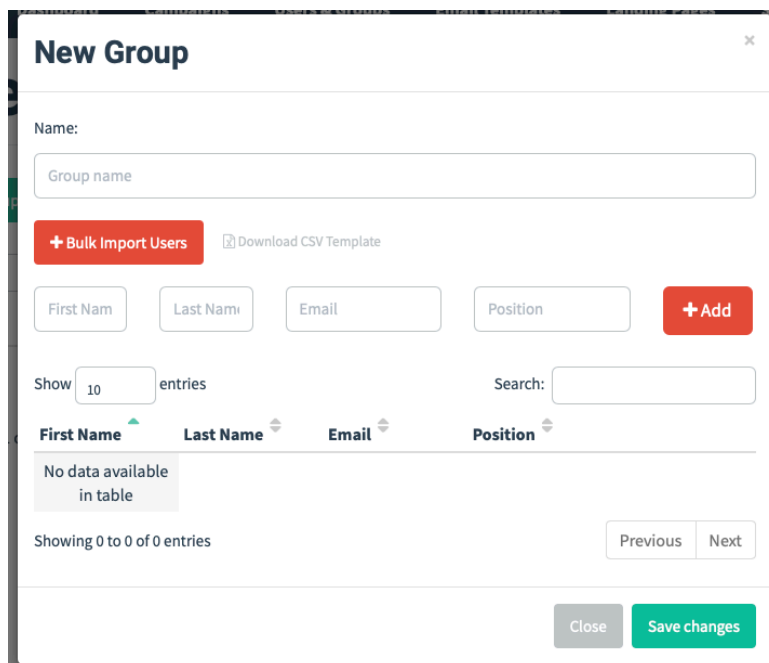
This also, like the previous template, was a subject of an email sent from Facebook. The email body was copied into the template, and the URLs were changed so that the landing page for the campaign could be used when a user clicks on a link in the email. Finally, as previously, a tracking image was added to the email. Both templates were now complete and ready to be used in the campaign.

The image displays two side-by-side screenshots of the 'New Template' form in a web application. Both forms have a 'Name' field at the top, followed by an 'Import Email' button. Below this is a 'Subject' field. The left form is for a template named 'Abertay' with the subject 'IT Service Desk Notification: Your Abertay password is about to expire.' The right form is for a template named 'Facebook' with the subject '[Abertay Ethical Hackers] Status Update'. Both forms have a 'Text' tab selected, showing a rich text editor with various formatting options. The left form's body text includes a personalized greeting 'Dear {{.FirstName}} {{.LastName}}', a section titled 'What's happening?' with a paragraph about a password expiration, and a section titled 'How do I change my password?' with a bullet point linking to a password change page. The right form's body text includes a Facebook logo and a post snippet from 'Colin McLean' about 'Abertay Ethical Hackers'. Both forms have a checkbox for 'Add Tracking Image' and an 'Add Files' button. At the bottom, there are 'Show' and 'Search' fields.

FIGURE 10 - EMAIL TEMPLATES AS COMPLETE

## 2.2.4. Users and Groups

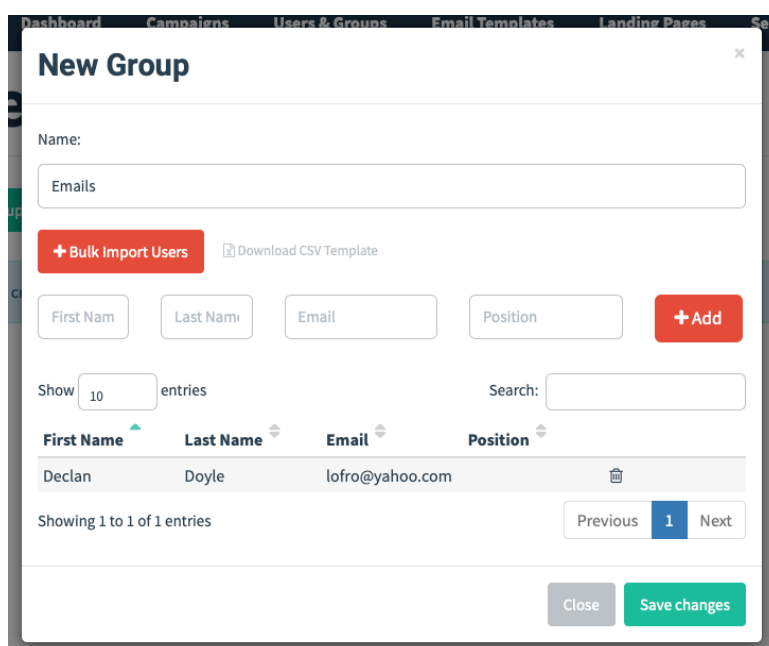
The last stage in the setup process for a campaign is to create the group of users that a campaign will be launched against. The group must be given a name so that it can be identifiable. Then the user has the option of bulk importing a list of users in the form of a CSV file. The user can also import users by entering their details manually. The details needed are a first name, last name, their email, and their position. It should be noted that not all details are required.



The 'New Group' window is a modal form for creating a new user group. It features a title bar with a close button. The main content area includes a 'Name' field with the placeholder 'Group name'. Below this are two buttons: '+ Bulk Import Users' (red) and 'Download CSV Template' (blue). Further down are four input fields: 'First Name', 'Last Name', 'Email', and 'Position', followed by a red '+ Add' button. A pagination section shows 'Show 10 entries' and a 'Search' field. Below this is a table with headers 'First Name', 'Last Name', 'Email', and 'Position'. The table is currently empty, displaying 'No data available in table'. At the bottom of the table area, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons. The modal footer contains a 'Close' button and a 'Save changes' button (green).

FIGURE 11 - NEW GROUP WINDOW

As this project was not intended to be used to test the effectiveness of phishing emails, only one user was entered into the user group, and it was a throwaway email that was created for this project. It was given the name 'Emails', and the first name and last name were set to 'Declan' and 'Doyle' respectively. The email address used was 'lofro@yahoo.com', and the position field was left blank. This user was added to the group, and the group was saved. The user group was now ready for the campaign.

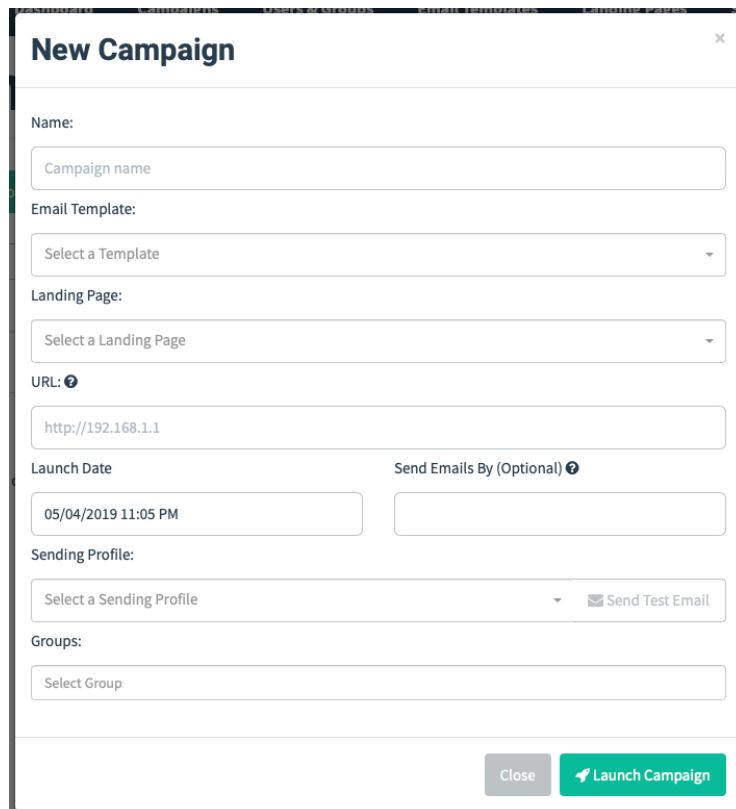


This screenshot shows the 'New Group' window after it has been saved. The 'Name' field now contains 'Emails'. The '+ Bulk Import Users' button is still present. The input fields for 'First Name', 'Last Name', 'Email', and 'Position' are still there, but the '+ Add' button is no longer visible. The table now contains one entry: 'Declan' in the 'First Name' column, 'Doyle' in the 'Last Name' column, and 'lofro@yahoo.com' in the 'Email' column. The 'Position' column is empty. The table footer shows 'Showing 1 to 1 of 1 entries' and has 'Previous', '1' (selected), and 'Next' buttons. The 'Close' and 'Save changes' buttons remain at the bottom.

FIGURE 12 - GROUP AS COMPLETE

## 2.3. Starting a Campaign

Once all portions of the GoPhish tool were configured, it was time to set up and launch a campaign. In the New Campaign window, several options must be set before the campaign can be launched. Firstly, a name must be given to the campaign, and then an email template must be chosen. Following this, a landing page must be selected, along with a URL that the landing page will be hosted on. This must be the location of the GoPhish listener, which will be the location that GoPhish is installed. The user must then chose the launch date and time for the campaign, which is when the emails will be sent. There is also the option to have a finishing date for sending the emails. If this is chosen, then the emails will be sent over a period of time between the starting date and finishing date. Finally, the user must select the sending profile and the group of users that the emails will be sent to.



The screenshot shows the 'New Campaign' window with the following fields and options:

- Name:** A text input field with the placeholder 'Campaign name'.
- Email Template:** A dropdown menu with the option 'Select a Template'.
- Landing Page:** A dropdown menu with the option 'Select a Landing Page'.
- URL:** A text input field with the placeholder 'http://192.168.1.1'.
- Launch Date:** A date and time picker showing '05/04/2019 11:05 PM'.
- Send Emails By (Optional):** An empty date and time picker.
- Sending Profile:** A dropdown menu with the option 'Select a Sending Profile' and a 'Send Test Email' button.
- Groups:** A dropdown menu with the option 'Select Group'.
- Buttons:** 'Close' and 'Launch Campaign' buttons at the bottom right.

**FIGURE 13 - NEW CAMPAIGN WINDOW**

Two campaigns were created for this project. The first was a campaign that sends an email impersonating Abertay University's IT department, informing a user that they must change their password. This campaign was set up using all of the previously created sections that were made for the 'Abertay' campaign. The launch date was set to immediately, and the URL was the IP address of the digital ocean server: 134.209.16.176. The campaign was launched, and the email was sent.

The second campaign involved impersonating Facebook. An email would be sent to a victim informing them that they have a new notification from the Abertay Ethical Hacking facebook group. The campaign was set up using all of the previously created sections for the 'Facebook' campaign. Again the launch date was set to immediately, ad the URL was the IP address of the digital ocean server. As before, the campaign was launched, and the email was sent.

## 3. Results

### 3.1. Abertay Campaign

The email for the Abertay campaign was successfully sent and received by the intended account. It looked very legitimate, as was intended, and appeared to come from the IT department of Abertay. The email correctly addressed the user as “Declan Doyle”, as was set up in the email template.

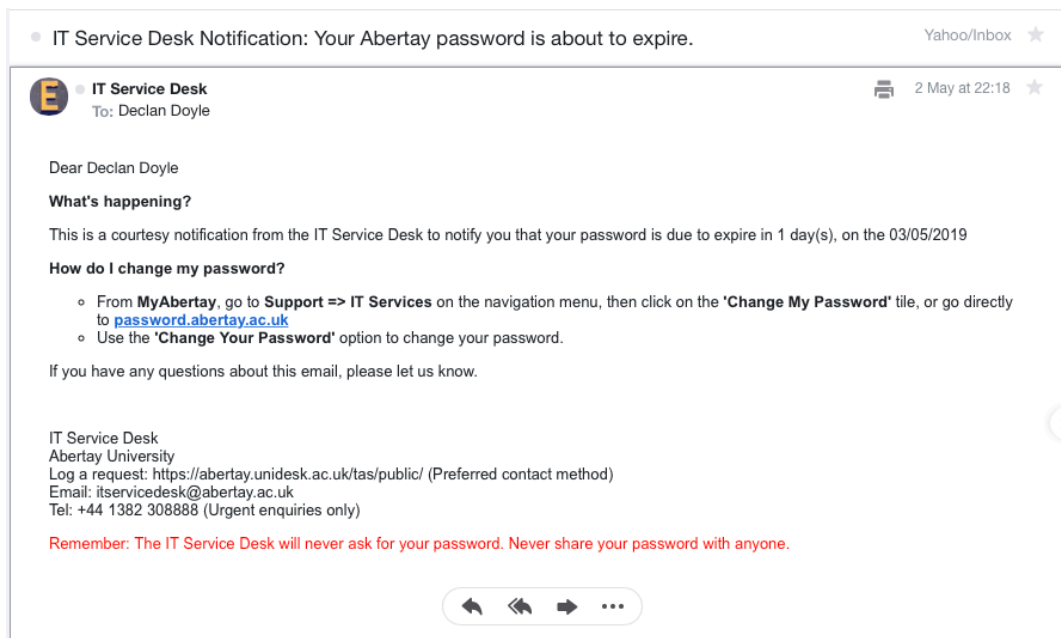


FIGURE 14 - ABERTAY CAMPAIGN EMAIL

When the link in the email was clicked, it took the victim to the landing page that had been previously set up. When any credentials were entered, and the sign in button was clicked, the webpage redirected to Abertay’s home page, so everything in the campaign worked as expected.

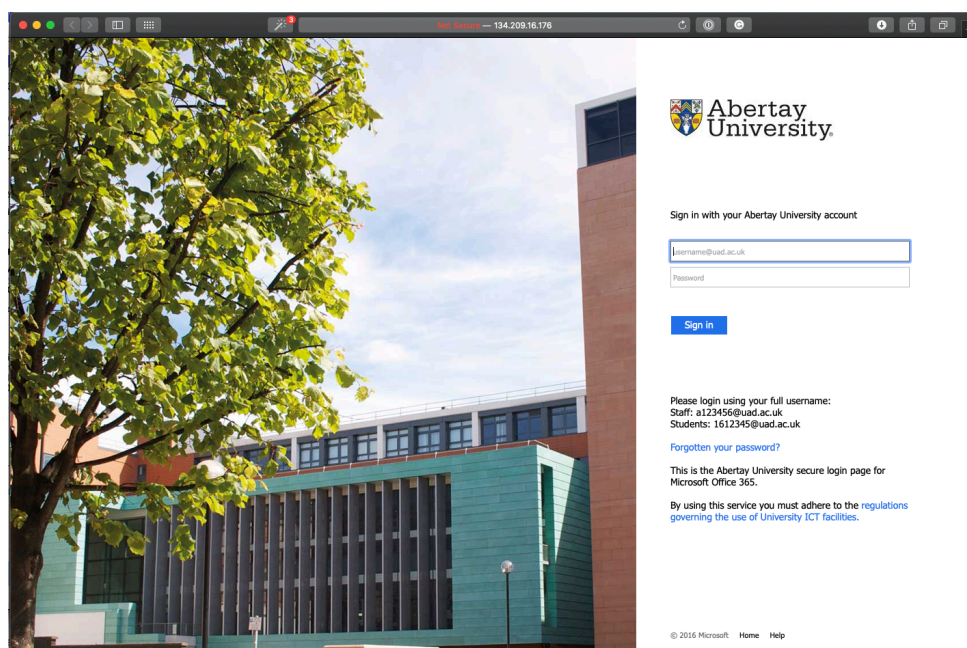


FIGURE 15 - ABERTAY CAMPAIGN LANDING PAGE

On GoPhish, there is a window where campaigns can be analysed, with statistics being shown and information on the emails and their status. The results show the number of emails sent, how



many of those emails were opened, the number of links clicked within emails, and the number of times data was submitted on landing pages. GoPhish will also show the status of each email sent out, with the option of the credentials entered being shown. There is also a timeline for each user, which shows the time that the email was sent, the time that they opened it, the time that they clicked the link, and the time that they sent data.



FIGURE 16 - TIMELINE FOR ABERTAY CAMPAIGN

### 3.2. Facebook Campaign

The Facebook campaign shared the success of the Abertay campaign, as there were no problems encountered. The email sent had a legitimate look as the email subject, and sender email looked realistic and almost identical to an email received from Facebook.

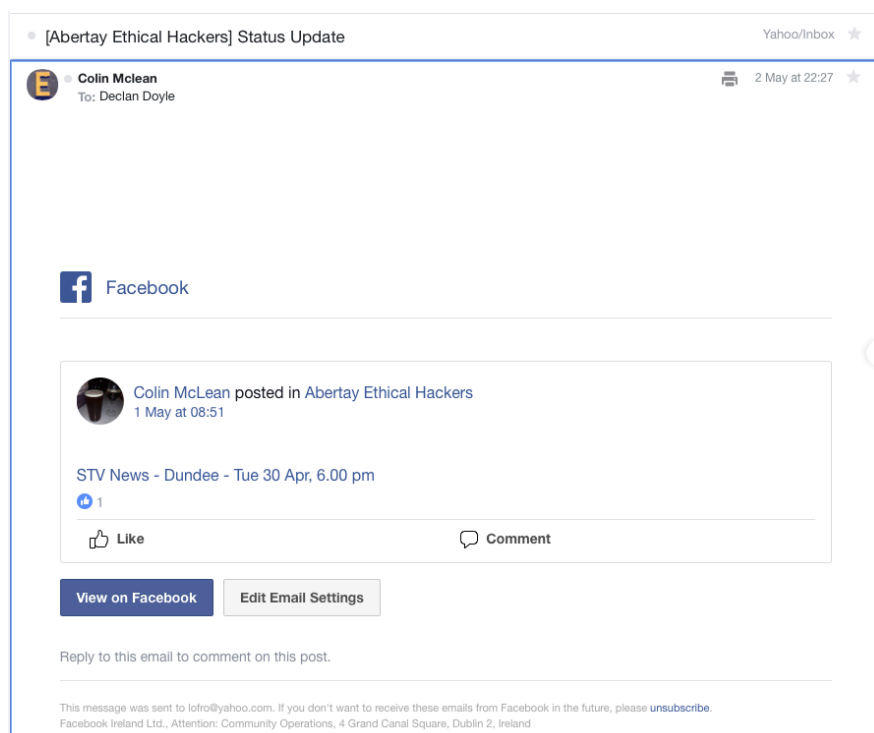
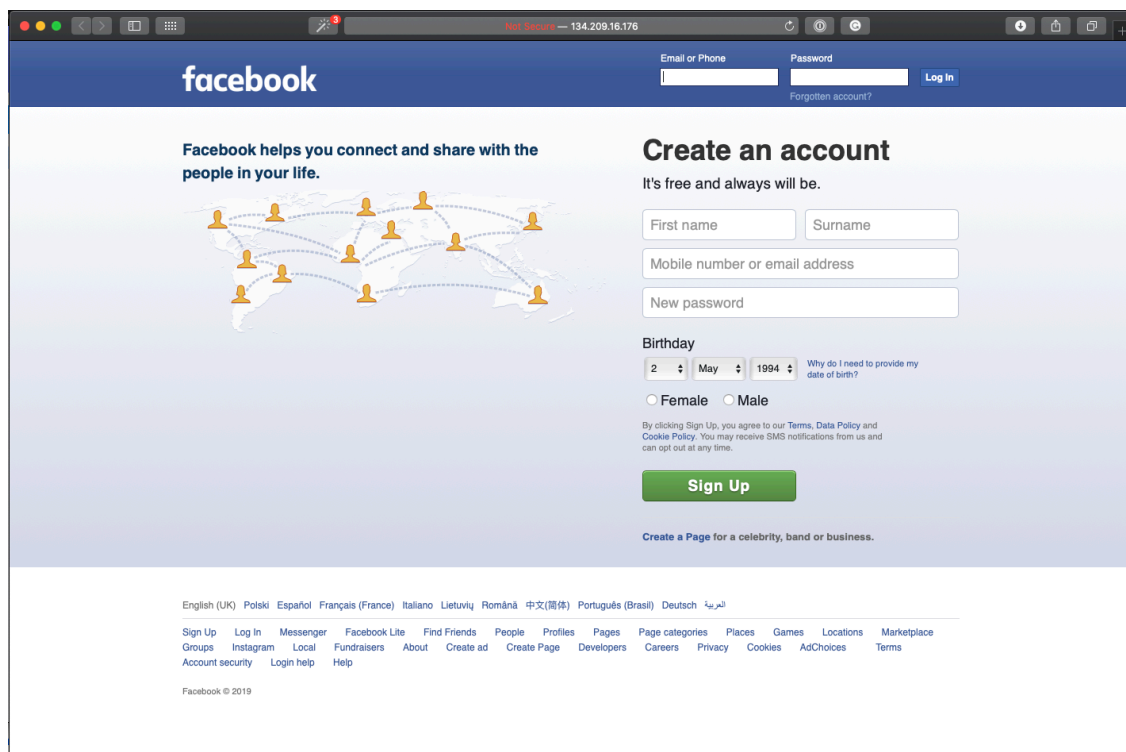


FIGURE 17 - FACEBOOK CAMPAIGN EMAIL

When either of the buttons in the email were clicked, the victim was taken to the landing page of the campaign, which looked like the Facebook login page. When credentials were entered the webpage redirected to Facebook's homepage, as was intended.



**FIGURE 18 - FACEBOOK CAMPAIGN LANDING PAGE**

GoPhish showed the campaign's success with the overview showing that the campaign resulted in a 100% success rate, with all emails sent resulting in submitted data.



**FIGURE 19 - FACEBOOK CAMPAIGN ANALYTICS**

## 4. Discussion

GoPhish's claim is that they provide an easy to use platform that can be used to test an organisations resilience to phishing attacks. Through the intended use of the application, this claim stands true. This can be shown through the following reasons. Firstly, GoPhish was incredibly easy to install and configure. Using the Digital Ocean platform, it took minutes to install it onto a server, and after a simple configuration file edit, the application was accessible through the internet. Using the credentials given in the setup documents, logging into the web application showed the easy to understand user interface. There were no complicated menu screens and no hidden option screens. With clear and easy-to-follow instructions, even a non-technical user could use the application.

Secondly, the sending profile feature allows for the creation of a profile that can appear as a legitimate email address. This is an excellent way of testing phishing resilience as stated in the introduction, a key characteristic of phishing emails is an unfamiliar email address. By creating a sending profile, a GoPhish user can set a sending email address that may look similar to the legitimate email address, but not quite right, encouraging staff to look for suspicious characters or other things that do not look quite right in the email address. When testing this feature, the only issue encountered was part of the email client used. Yahoo displays an image for the contact of the email that has been received. The email used to test began with an 'E', so Yahoo displayed the contact picture as this, which did not tie into the theme of the email.



**FIGURE 20 - CONTACT PHOTO FROM EMAIL**

Thirdly, the ability to create a custom landing page gives the ability to further test staff after they have clicked on a link within an email. The page, while not done in this project, can be hosted on a server that can get an SSL certificate, meaning that the browser will display that the website is secure. This is a problem on the broader cyber-security community, as many people have been made to believe that when the browser says that a website is secure, it is legitimate. This is incorrect, as all this means is that data sent back and forth between the server and client is encrypted, and gives no indication as to how legitimate a site is. This misconception can be exploited, and by giving a landing page an SSL certificate, it will appear more legitimate to the staff base. GoPhish also allows for the capture of credentials - usernames and passwords. This is a useful feature as it can show what the staff members are entering. However, caution must be taken when using this feature. GoPhish warns that any credentials captured are stored in plaintext, and so if the GoPhish server were ever to be breached, potentially sensitive information could be leaked. It is strongly recommended that GoPhish only be deployed on an internal network if being used for legitimate organisational testing.

Fourthly, the email template feature of GoPhish can be used to create almost identical looking emails that have been sent by big companies, or even the creation of new emails that can imitate the language of a corporate environment. A vital feature of these templates is the ability to add links to the body of the email. Using HTML, these links can be disguised, so that only a savvy user will identify them as suspicious links. This is arguably one of the most important features of phishing emails, and so this inclusion makes GoPhish a useful tool in testing staff resilience. Another important feature that GoPhish includes in the email template is the ability to have placeholders for names. This means that when the email is sent, it can identify a user by their name, which is an uncommon characteristic of phishing emails, increasing the difficulty of staff members identifying the email as suspicious.

Fifthly, while a relatively small feature, the ability to add many users to the Users and Groups section allows for the mimicking of a real-life phishing campaign. Phishing campaigns are usually sent out to hundreds of thousands, if not millions of people, also by adding a name with an email, it allows for a more personalised email to be created, making it more difficult to detect as a phishing email.

Finally, at the end of a campaign, the statistics and analytics that GoPhish provide allow for an in-depth analysis of how an organisation has performed in a phishing campaign. This gives the ability to pinpoint weak spots in an organisation and shows which staff members need further

training to increase their resilience. It can also show what time staff routinely check emails, which can be helpful for management to establish a workflow for their employees.

## **4.1. Countermeasures**

Unlike computers, human beings cannot be secured by simply upgrading software. Because of this, there is no specific countermeasure to phishing attacks. The best way to prevent them from working is to increase the resilience of users by training them to identify a phishing email amongst regular emails. GoPhish was designed for this purpose and so makes an ideal solution to the growing phishing problem. There are also several organisations that offer phishing resilience testing and training to businesses. While this may seem like an unnecessary expense when taking into consideration the amount of money and reputation an organisation may lose if they are a victim of a successful phishing attack, it makes sense to invest in this training.

## 5. References

Phishing.org. (2019). Phishing | What Is Phishing?. [online] Available at: <http://www.phishing.org/what-is-phishing> [Accessed 7 May 2019].

Ncsc.gov.uk. (2019). NCSC. [online] Available at: <https://www.ncsc.gov.uk/guidance/phishing> [Accessed 7 May 2019].

Proofpoint. (2019). Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks. [online] Available at: <https://www.proofpoint.com/us/resources/threat-reports/quarterly-threat-analysis> [Accessed 7 May 2019].

Katz, E. and Katz, E. (2019). Phishing Statistics: What Every Business Needs to Know. [online] Dashlane Blog. Available at: <https://blog.dashlane.com/phishing-statistics/> [Accessed 7 May 2019].

Wright, J. (2012). Gophish - Open Source Phishing Framework. [online] Getgophish.com. Available at: <https://getgophish.com> [Accessed 7 May 2019].

Medium. (2019). Conducting USB Drop Tests With GoPhish. [online] Available at: <https://medium.com/@chrismerkel/conducting-usb-drop-tests-with-gophish-44cc7e1a88b9> [Accessed 7 May 2019].