# CIT 285 - Lab #7 – Social Engineering

## Introduction

Social engineering is a hard to combat issue in cybersecurity due to the human elements involved. One of the most effective nontechnical mitigation techniques is user education. Among the number of social engineering attacks utilized by malicious actors, phishing is one of the most common and effective types of attacks. As the textbook states, “phishing is a form of social engineering in which you ask someone for a piece of information that you are missing by making it look as if it is a legitimate request.” There are many tools, open source and commercial, that can be used to create phishing campaigns. These are often deployed in enterprise settings to test employee awareness.

In this lab, you will create your own phishing campaign using open source tools specifically designed for education and training purposes. Please be aware that the tools used in in this lab are for informational purposes only and using them for malicious reasons is strictly prohibited. In other words, remember the Ethics Agreement signed at the beginning of the semester.

**References:**

GoPhish User Guide: <https://docs.getgophish.com/user-guide/>

## 1: Setup

The GoPhish application has been installed on your Kali VM. Open a terminal, change to the Downloads directory and issue the following command to start the Gophish program.

**# ./gophish**

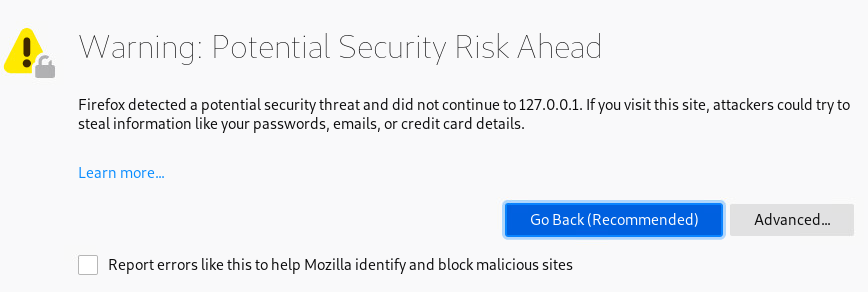
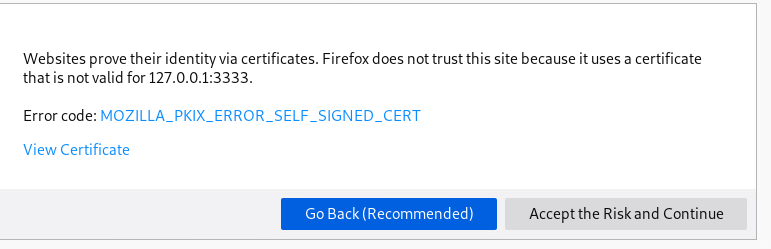
**You will need to leave this terminal open while continuing with the rest of the lab.**

## 2: Phishing Email

### Accessing Gophish

In a new browser tab, enter the following address <https://127.0.0.1:3333>. This takes you to the Graphical User Interface (GUI) database login page for GoPhish.

*If you receive a security error about the connection not being secure, select the ‘Advanced’ button, then the ‘Add Exception’ button, next hit the ‘Confirm Security Exception’ in the left bottom corner*.

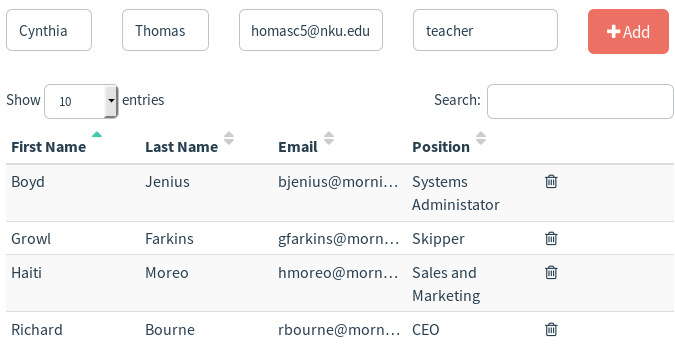
 

Enter the following credentials at the login page:

* UN = admin
* PW = gophish

### Adding Users

Click the ‘Users & Groups’ link, then the ‘NewGroup’ button

* Enter CIT 285 – Your\_nkuID as the Group name, then select the ‘+Bulk Import Users’ button
* In the new window, navigate to the file “MorningCatch.cvs’ in the Downloads folder of your Kali VM. The file will automatically open and populate a list of users in the lower pane
* Add your name and NKU email to create a total of 5 users, as shown in the image
* Save the Changes

### Creating the Email Template

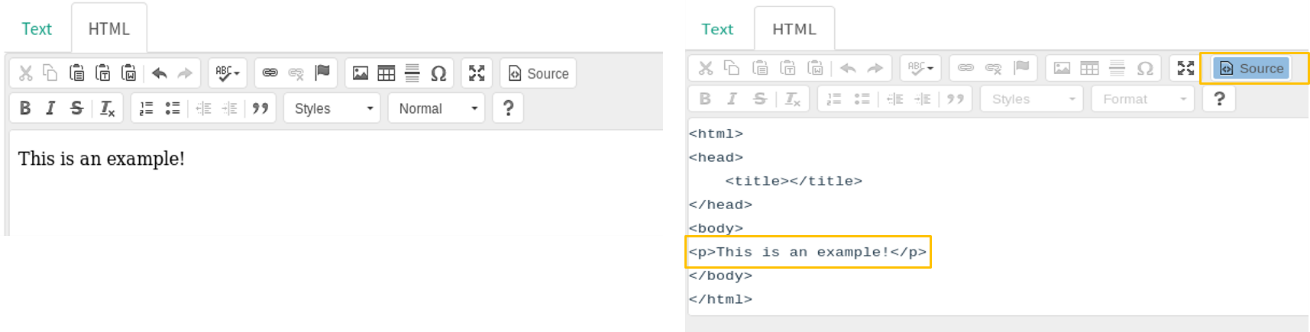
In this section of the lab, you will create a phishing email using HTML to send to the users created in the previous section.

* Select the ‘Email Templates’ link
* Click the ‘+New Template’ button
* Name the email – MorningCatch – CIT 285

**Create a phishing email of your choosing, but it must include the following items**

* + **1 button or link** for users to click to be taken to a landing page (see the next section)
  + **1 or more images**
  + Your email should be based on one or more of the principles behind social engineering
    - (Authority, Intimidation, Consensus, Scarcity, Familiarity,trust, Urgency)

Select the HTML tab to enter HTML code. You can start typing directly in the window as shown in the image on the left. Hitting the ‘Source’ button in the menu bar will show your text in HTML.



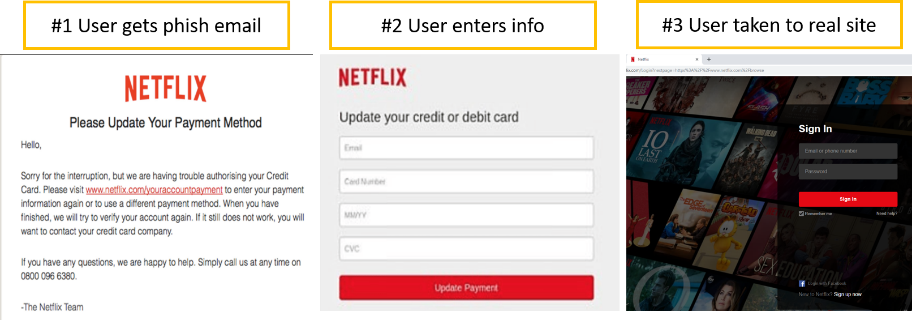
It is recommended you use the formatting buttons for bolding text, adding images, bullets, etc., when creating the visual aspects of your email and use HTML code to add buttons or links

* + HTML resources:
    - <https://www.w3schools.com/html/html_forms.asp>
    - HTML button code example
      * <input type=”submit” value=”Submit” id=’submit’>
    - HTML link code example
      * <a href=”{{.URL}}”>link</a>
  + Phishing Email resources:
    - <https://socialexploits.comblog/how-to-write-phishing-emails/>
    - <https://www.securitymetrics.com/blog/top-10-types-phishing-emails>

Once you have your email created, give it an appropriate subject, and then hit the ‘Save Template’ button.

### Creating a Landing Page

When a user clicks a link or button in a phishing email, they are taken to a webpage controlled by a malicious user. Once a user enters their information on a bad site, they are usually redirected to a legitimate website. The goal is to keep the user unaware they were ever on the attacker’s site. Well-crafted phishing emails and landing pages are created to match official sites as closely as possible.



Since this lab is in an isolated environment, you will not be able to create a working landing page and although Gophish requires a page be created, we can work around it by using a working URL.

Select the Landing Pages link, then the ‘+New Page’ button.

* Name: **Morning Catch Landing Page**
* Select the ‘Import Site’ button, then enter ‘https://google.com”
* **Save the page**

### Creating a Sending Profile

#1 User gets a phishing email and clicks the link

In this step you will provide a sender for your phishing email. By creating a fake profile, malicious users are able to hide their identity. For the purposes of this lab, a test account has been created for you. This account is intended for educational purposes and **should NOT** be used for anything else.

Click the Sending Profiles link, then the ‘+New Profile’ button

Enter the following information in the new window

* Name: **CIT 285 – Morning Catch**
* From: **NKUstudent Acct <nkustudent2@gmail.com>**
* Host: **smtp.gmail.com**
* Username: **nkustudent2**
* Password: **TESTonly!**
* Select the ‘**Ignore Certificate Errors**’ box

These settings allow your email to be sent and properly routed. Save the profile.

### Launching the Phishing Campaign

A phishing campaign is the process of sending phishing emails to potential victims. Usually this is a list of email addresses gathered from a repository or created specifically for a certain individual (e.g. spear and whale phishing).

Click on the Campaigns link, then ‘+New Campaign’

Enter the following information in the new window

* Name: **Lab 7 – yourNKUid**
* Email Template: **use the drop down**
* Landing Page: **use the drop down**
* URL: **leave blank**
* Launch Date: **leave as is**
* Sending Profile: **use the drop down**
* Groups: **use the drop down**

Click the ‘Launch the Campaign’ button

Once the campaign launches, you’ll be taken to the campaign’s dashboard. The first four addresses of your group list will show as being sent, but will not actually reach the mail server hosting them.

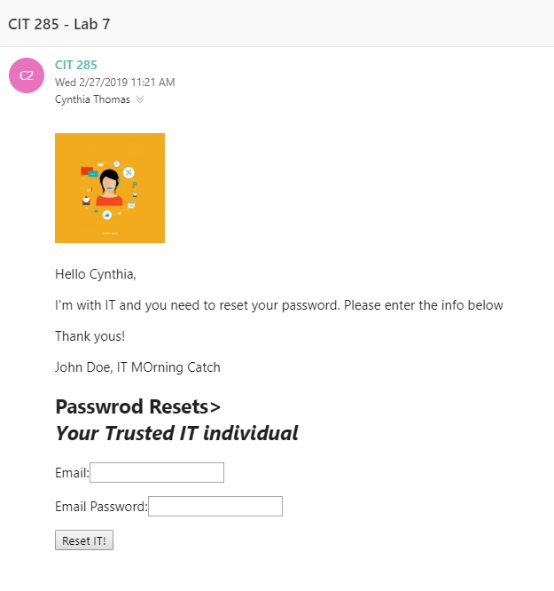
The address manually added to the group list will reach NKU’s email server, but will most likely get caught by the spam filter. Since the email has been quarantined, you will have to wait a few hours to release it to your inbox.

## 3: Submission

* When you receive a copy of the email to your NKU account, screenshot it in your inbox and upload it as part of your submission in Canvas.
* If an email is not received to your NKU email account, provide a screenshot of the phishing email you created.

**Reference Example**

Use the following as guidance when creating your phishing email. **Do not** use this example as your submitted assignment.

*****HTML code used for the example email*

<!DOCTYPE html>

<html>

<head>

<title>Morning Catch IT page!</title>

</head>

<body>

<h2><a href="https://www.google.com/url?sa=i&amp;rct=j&amp;q=&amp;esrc=s&amp;source=images&amp;cd=&amp;cad=rja&amp;uact=8&amp;ved=2ahUKEwjOrteTvdfgAhUCOa0KHTeWB18QjRx6BAgBEAU&amp;url=https%3A%2F%2Fwww.freepik.com%2Ffree-photos-vectors%2Ftelemarketing&amp;psig=AOvVaw0gZPQjbriAFrFRhnFFPikw&amp;ust=1551204470021152"><img alt="" height="124" src="https://img.freepik.com/free-vector/support-service-concept\_1325-57.jpg?size=338&amp;ext=jpg" width="124" /></a></h2>

<p>Hello {{.FirstName}},</p>

<p>I&#39;m with IT and you need to reset your password. Please enter the info below</p>

<p>Thank yous!</p>

<p>John Doe, IT MOrning Catch</p>

<h2><strong>Passwrod Resets&gt;</strong><br />

<em>Your Trusted IT individual</em></h2>

<p>Email:<input type="text" /></p>

<p>Email Password:<input type="password" /></p>

<p><input type="button" value="Reset IT!" /></p>

<p>&nbsp;</p>

</body>

</html>

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**I was struggling with the picture part and trying to get it to show up, but there is an image there. I don’t know how to work html that well but was able to get everything I needed besides the picture showing up in the actual email**

**-Thanks Kaleb**