



# Ethical Student Hackers

Social Engineering

# The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

# Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at  
<https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf>

# Social Engineering - What is it?

---

*Social engineering is the psychological manipulation of people into performing actions or divulging confidential information*

Vishing, phishing, smishing, impersonation, pretexting, spear phishing, water holing, baiting, quid pro quo, tailgating, scareware, credential harvesting...


# Phishing

*Cyber attack that targets victims via email that lures the victims into providing sensitive data or completing an action*

- Credential harvesting
- Downloading malware
- Identity fraud
- Financial fraud

The list goes on and on...

# Phishing examples

**From:** GlobalPay <VT@globalpay.com>   
**Subject:** Restore your account  
**Date:** February 7, 2014 3:47:02 AM MST  
**To:** David

Hide

1 Attachment, 7 KB

Save ▼

Quick Look

Dear customer,

We regret to inform you that your account has been restricted.

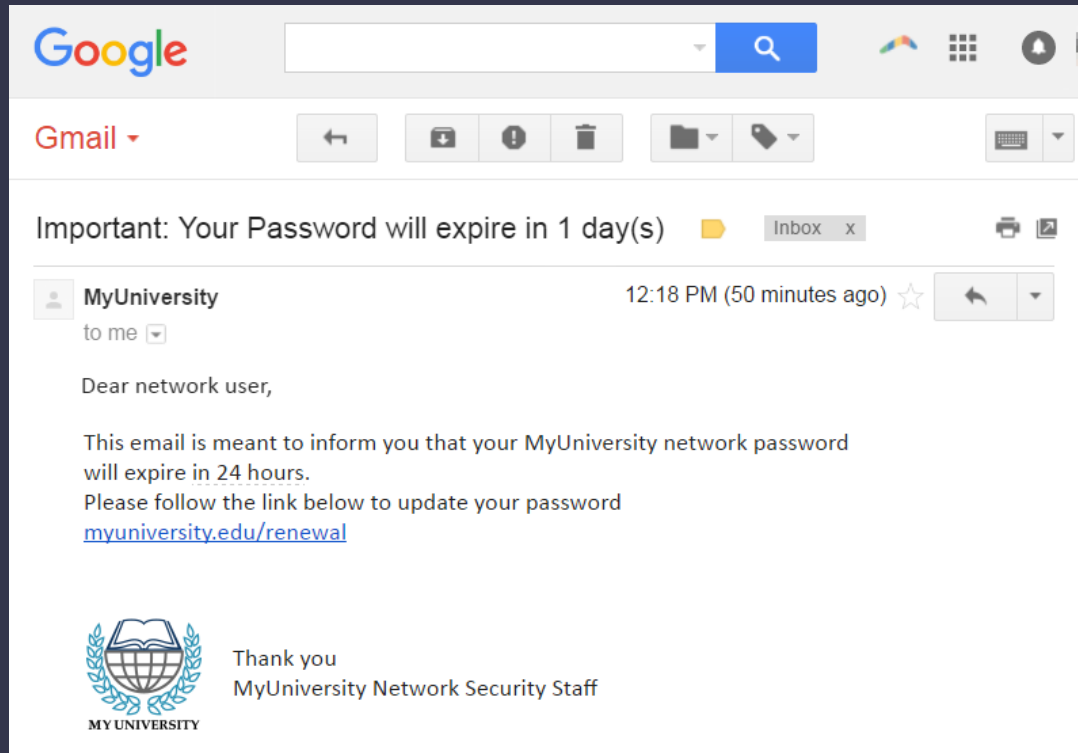
To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc



[update2816.html \(7 KB\)](#)

# Phishing examples



The screenshot shows a Gmail interface with a search bar at the top. Below the search bar, the Gmail logo and navigation icons are visible. The main content area displays an email from 'MyUniversity' with the subject 'Important: Your Password will expire in 1 day(s)'. The email body contains a message from 'MyUniversity Network Security Staff' with a link to 'myuniversity.edu/renewal'.

Google

Gmail

Important: Your Password will expire in 1 day(s)


Inbox x

MyUniversity 12:18 PM (50 minutes ago)

to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.  
Please follow the link below to update your password  
[myuniversity.edu/renewal](http://myuniversity.edu/renewal)

 Thank you  
MyUniversity Network Security Staff

# Phishing examples

## Nice to Know You

Naomi Surugaba [azlin@moa.gov.my]



Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,

I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.

I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US\$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.

I am here seeking for an avenue to transfer the fund to you in only you're reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent's and I want you to help me transfer the fund into your bank account for investment purpose.

Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent's. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.

Remain blessed,  
Miss Naomi Surugaba.



# Creating a phishing campaign

---

## Legalities of phishing

Phishing that is not for educational and training purposes breaches The Fraud Act 2006 and is **ILLEGAL!** Offences under these Acts are punishable by fines and / or imprisonment up to 10 years

# Creating a phishing campaign

---

## GoPhish

*Gophish is an open-source phishing toolkit designed for businesses and penetration testers. It provides the ability to quickly and easily setup and execute phishing engagements and security awareness training*

<https://github.com/gophish/gophish>

# Creating a phishing campaign

## Optimising your campaign

You want to trick your users into thinking the email is genuine

- Look professional
- Accurate spelling and grammar
- Pass SPAM filters
- Get something out of it (in this case, credit card info)
- Email headers

Find a SPAM score for our email - <https://www.mail-tester.com/>

# Protecting against a phishing campaign

---

- Anti-spam filters
- Training of staff/yourself
- Protect yourself from malicious links if you do click them using a proxy

The best form of protection is being aware and being careful!

# Anti-spam filters

A program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox

## SpamAssassin

*Apache SpamAssassin is the #1 Open Source anti-spam platform giving system administrators a filter to classify email and block "spam" (unsolicited bulk email). It uses a robust scoring framework and plug-ins to integrate a wide range of advanced heuristic and statistical analysis tests on email headers and body text including text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases.*

# SpamAssassin - I run a mail server

## Using with Procmail

*Procmail - A mail delivery agent that processes all messages before they reach your mailbox*

Put some the following into the .procmailrc file...

(Instructions for other setups are available here  
<https://cwiki.apache.org/confluence/display/SPAMASSASSIN/StartUsing>)

# SpamAssassin - I run a mail server

```
:0fw: spamassassin.lock
```

```
* < 512000
```

```
| spamassassin
```

# The lock file ensures that only 1 spamassassin invocation happens at 1 time, to keep the load down

---

```
:0:
```

```
* ^X-Spam-Level:
```

```
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
```

```
almost-certainly-spam
```

# Score of 15+ is almost certainly spam. Move to different mailbox

# SpamAssassin - I run a mail server

```
:0: # Mail that is tagged as spam  
* ^X-Spam-Status: Yes based on set threshold is moved to  
probably-spam a different mailbox
```

---

These are only some basics and there are so many more setup options available!



# Social Engineering Tools

<https://github.com/trustedsec/social-engineer-toolkit>

*The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly.*

Many of the techniques learnt today can also be applied to other packages such as the SEToolKit

# Upcoming Sessions

What's up next?

[www.shefesh.com/sessions](http://www.shefesh.com/sessions)

22d Feb - Introduction to Assembly

1st Mar - Game Breaking

8th Mar - Making a CTF

15th Mar - Web App Hacking

22nd Mar - HTB Walkthrough

# Any Questions?



[www.shefesh.com](http://www.shefesh.com)  
Thanks for coming!