

# 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.
- Relevant UK Law: <https://www.legislation.gov.uk/ukpga/1990/18/contents>



# 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 **[shefesh.com/conduct](https://shefesh.com/conduct)**



# Phishing

A type of cybercrime where an attacker will impersonate a legitimate company or person via email, text or phone to trick users into giving up sensitive information

## HOW TO SPOT A PHISHING EMAIL

- Typos
- Dodgy source address
- Urgent
- Needs personal information
- Grammar
- Random links
- Generic information

From: authenticationmail@trust.ameribank7.com  
To: johnsmith@email.com  
Subject: A new login to your bank account



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

**4 new transactions have been made with this account since your last login.**

**If this was not you, please reset your password immediately with this link:**

<https://trust.ameribank7.com/reset-password>

Thank you,  
Bank America



**PHISH OR  
NO PHISH**

**PHISH or NO PHISH**



12:05



◀ Outlook



+1 (641) 629-9766 >

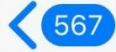
Text Message  
Today 12:04 PM

YOUR MOBILE NUMBER HAS  
WON \$750,000 DOLLARS IN  
THE ONGOING APPLE  
LOTTERY. SEND YOUR NAME:  
ADDRESS: MOBILE:  
OCCUPATION: AND AGE: TO  
THE CLAIM MANAGER DANIEL  
SCOTT([304-729-4653](tel:304-729-4653)).



12:05

◀ Outlook



+1 (641) 629-9766 >

Text Message  
Today 12:04 PM

YOUR MOBILE NUMBER HAS WON \$750,000 DOLLARS IN THE ONGOING APPLE LOTTERY. SEND YOUR NAME: ADDRESS: MOBILE: OCCUPATION: AND AGE: TO THE CLAIM MANAGER DANIEL SCOTT([304-729-4653](tel:304-729-4653)).

# PHISH



Re: Office 365 - Update



Office365 - System <gmarsh@noblesys.com>

To websupdate@office365.microsoft.com

Reply

Reply

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

Action Items

## Office 365 - Update

Dear user

This message is being sent to you to inform you that your account is to be closed

If you wish to continue using this account please upgrade to our services.  
Ignoring this message will cause your account to be closed

[Update your account](#)

Note: Please take a few moment to update your account now

Thanks

Regards  
Microsoft.com Team



Re: Office 365 - Update



Office365 - System <gmarsh@noblesys.com>

To websupdate@office365.microsoft.com

Reply

Reply

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

Action Items

## Office 365 - Update

Dear user

This message is being sent to you to inform you that your account is to be closed

If you wish to continue using this account please upgrade to our services.

Ignoring this message will cause your account to be closed

[Update your account](#)

Note: Please take a few moment to update your account now

Thanks

Regards

Microsoft.com Team

# PHISH





Printerval <hithere@send.printerval.com>  
to me ▾

Sat 25 Apr, 15:15 (2 days ago)



Why is this message in spam? This message is similar to messages that were identified as spam in the past.

Report as not spam



Logo

[Printerval.com](#) 8 The Green Suite, Suite A, Dover, DE 19901, United States

[MANAGE PREFERENCES](#) | [UNSUBSCRIBE](#) | [PRIVACY POLICY](#)

This email was sent to you because you  
have opted into the us email list.

If you wish to unsubscribe from us emails,  
please click the unsubscribe button.

[unsubscribe](#)

← Reply

→ Forward





Printerval <hithere@send.printerval.com>

to me ▾

Sat 25 Apr, 15:15 (2 days ago)



Why is this message in spam? This message is similar to messages that were identified as spam in the past.

Report as not spam



Logo

[Printerval.com](#) 8 The Green Suite, Suite A, Dover, DE 19901, United States

[MANAGE PREFERENCES](#) | [UNSUBSCRIBE](#) | [PRIVACY POLICY](#)

This email was sent to you because you  
have opted into the us email list.

If you wish to unsubscribe from us emails,  
please click the unsubscribe button.

[unsubscribe](#)

← Reply

→ Forward



# NO PHISH



SUSPENSION NOTICE (Action Requested) - Message (HTML)

File Message Help Adobe PDF Tell me what you want to do

Delete Archive Reply Reply All Forward Hashed Out To Manager Team Email Move Tags Editing Speech Zoom

ES Fri 5/17/2019 6:49 AM

Email Suspension Team <sfaccount@pricenegotiator.tech>  
SUSPENSION NOTICE (Action Requested)

To Recipients

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

# Final Update 2019

This message is sent to inform you that your account will expire  
**TODAY !!**

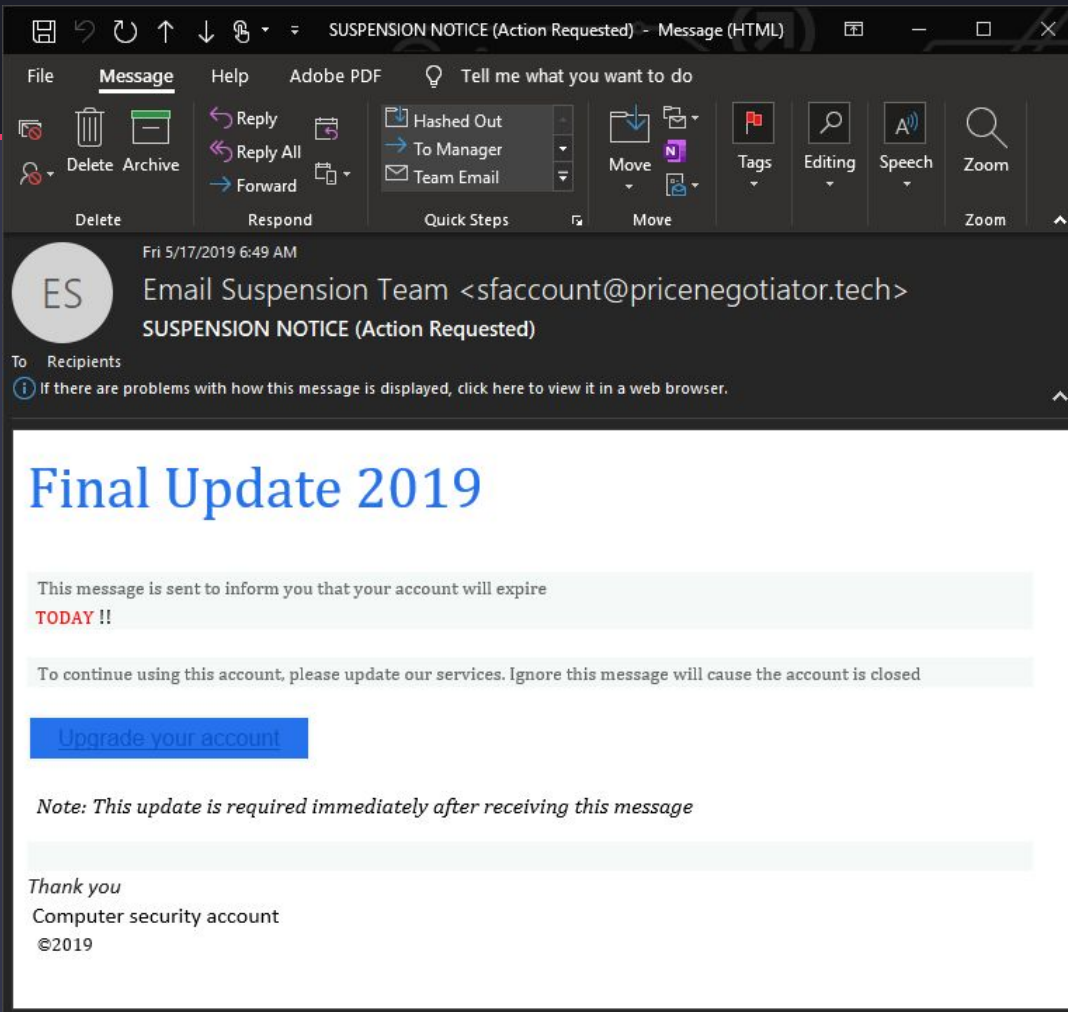
To continue using this account, please update our services. Ignore this message will cause the account is closed

[Upgrade your account](#)

*Note: This update is required immediately after receiving this message*

Thank you  
Computer security account  
©2019





# PHISH



----- Forwarded message -----

From: **Sheffield City Freecycle Group** <[no\\_reply@freecycle.org](mailto:no_reply@freecycle.org)>

Date: Mon, 27 Apr 2026 at 07:13

Subject: [Freecycle Sheffield City] Recent Posts on Sheffield City

To: EchoG <[garrattecho1@gmail.com](mailto:garrattecho1@gmail.com)>



To respond to this message, please use a link below - do not reply directly to this email (when you reply online, you may be asked to log in)

### 22 posts since the last digest:

1. [WANTED: FREE eWaste COLLECTION \(S11\)](#)
2. [OFFER: IKEA Kallax Storage Unit \(Walkley.\)](#)
3. [OFFER: Made.com two seater sofa \(Walkley.\)](#)
4. [OFFER: 2/3 seat electric recliner sofa, teal \(Swallownest S26\)](#)

**DONATE** 

### Freecycle Newswire

- [AOL News: The fiscal freedom of Freecycle, a lesson best learned early](#)
- [Small Business Trends: 7 Best Cheap Craft Stores for Budget Curious](#)



----- Forwarded message -----

From: **Sheffield City Freecycle Group** <[no\\_reply@freecycle.org](mailto:no_reply@freecycle.org)>

Date: Mon, 27 Apr 2026 at 07:13

Subject: [Freecycle Sheffield City] Recent Posts on Sheffield City

To: EchoG <[garrattecho1@gmail.com](mailto:garrattecho1@gmail.com)>



To respond to this message, please use a link below - do not reply directly to this email (when you reply online, you may be asked to log in)

#### 22 posts since the last digest:

1. [WANTED: FREE eWaste COLLECTION \(S11\)](#)
2. [OFFER: IKEA Kallax Storage Unit \(Walkley\)](#)
3. [OFFER: Made.com two seater sofa \(Walkley\)](#)
4. [OFFER: 2/3 seat electric recliner sofa, teal \(Swallownest S26\)](#)

**DONATE** 

#### Freecycle Newswire

- [AOL News: The fiscal freedom of Freecycle, a lesson best learned early](#)
- [Small Business Trends: 7 Best Cheap Craft Stores for Budget Shopping](#)

# NO PHISH



[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com  
to me



Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

**Why is my PayPal account limited?**

We believe that your account is in danger from unauthorized users.

**What can I do to resolve the problem?**

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

[Confirm Your Information](#)



[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com  
to me



Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

**Why is my PayPal account limited?**

We believe that your account is in danger from unauthorized users.

**What can I do to resolve the problem?**

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

# PHISH



Thanks for playing :)

**PHISH** or **NO PHISH**



# Vishing (Voice Phishing)

The act of using phone calls to trick people into giving away sensitive information

Techniques:

Caller ID Spoofing

Urgency and fear

Voice simulation/AI

Targeting



# Physical techniques

**Tailgating** - an unauthorised person follows an authorised person into an area (e.g slipping through before a door closes)

**Shouldering** - observing a users screen or keyboard to steal sensitive info like pins or passwords

**Piggybacking** - similar to tailgating but the authorised user is willfully participating (e.g holding a door open for someone)

**Dumpster diving** - searching through bins and recycling to find sensitive documents or hardware that can be used to gather information



# Real world examples

- **Toyota Boshoku Corporation (2019)**: Attackers posed as a supplier, persuading a finance executive to change recipient bank account information, resulting in a loss of **\$37 million**.
- **Barbara Corcoran (2020)**: A *Shark Tank* judge, she was tricked in a nearly **\$400,000** phishing scam by an attacker impersonating her assistant to request payment for real estate investments.
- **Ubiquiti Networks (2015)**: Hackers impersonated company executives to trick employees into paying fake invoices, costing the firm **\$47 million**
- **Sony Pictures (2014)**: Employees were targeted by fake Apple security emails, leading to a massive breach that leaked confidential data and, according to the FBI, was attributed to North Korea.
- **2016 U.S. Election Leaks**: Hackers sent phishing emails disguised as Google security alerts to members of the Hillary Clinton campaign, leading to the theft of personal emails and documents.
- **Deepfake CEO Fraud (2019)**: Attackers used AI-generated voice cloning to mimic a CEO, instructing an executive to transfer roughly **\$243,000** to a Hungarian supplier



# Preventing social engineering attacks

The main way of preventing social engineering attacks is to educate people on what to look out for.

For example the NHS have training videos like this:



# Typosquatting/ Bitsquatting

**Typosquatting** - Attackers register domain names that are common typos of well known sites hoping users will accidentally use them

**Bitsquatting** - Relies on bit-flip errors that occur during the process of making a DNS request - when this occurs the user is directed to a website registered with a similar domain name except with one bit flipped in the binary representation



# AI use in social engineering

- **Persuasive Content** – Non-native speakers skirt grammar and spelling errors thanks to AI bots like ChatGPT. Given prompts, bots can write realistic-sounding content. Error-free content can get by spam filters, often making it to your inbox where it's hard to detect.
- **Personalized phishing attack** – AI bots assist criminals by creating fake accounts. They can mine social media accounts for data to be used against you in emails. They identify communication styles and emotional triggers that resonate with you.
- **Deepfake creation** – AI Bots can create realistic audios and videos that look and sound like a real person. For example, deepfakes can convince people to reveal personal information in a Zoom meeting. The same is true with deepfake phone calls.
- **Detection Evasion** – Bots can learn how to avoid red flags in security tools and work around them.



# ~Practical

Try sending an email with a forged from field: (You may not receive it today if at all, good to see how your provider handles it) <https://emkei.cz/>

<https://www.mail-tester.com/> - test the spamminess of an email

Social engineering tools:

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

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

Can you create a fake ShefESH web page and see how real you can make it look with HTML and CSS?



# Feedback

Please leave your feedback :) We want to know what we can do to improve.

Please leave constructive and honest feedback only.

<https://forms.gle/VTYd74K5BHqbC7F68>



# Inclusions Concerns

If there's anything preventing you from enjoying our sessions, please let our Inclusions Officer know. You can contact them by email or fill in the form below:

[igledhill2@sheffield.ac.uk](mailto:igledhill2@sheffield.ac.uk)

<https://forms.gle/Qoct6Wyfesv8dWmej7>



# Upcoming Sessions

What's up next?

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

AI prompt injecting

Burpsuite

Guest Lecture

# Any Questions?



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

