



# Cyber Security Awareness Month

---

Do Your Part. #BeCyberSmart

# Spam & Phishing

---

Do Your Part. #BeCyberSmart



# Panelists

---

Rita Uddin	Tremmelle Thomas	James Cronen	Eliud Perez	Pak Tong
Assistant VP CIO	Helpdesk Manager	Security	Network	Exchange Admin



# Agenda

---

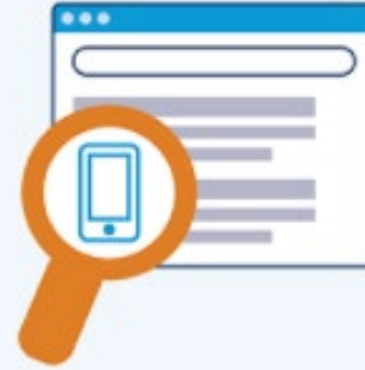
## Spam and Phishing

## Types of Spam and Phishing Attacks

## Avoid Being a Victim

## Tips For Victims

## Helpful Links



### Check it out.

- » Look up the website or phone number for the company or person who's contacting you.
- » Call that company or person directly. Use a number you know to be correct, not the number in the email or text.
- » Tell them about the message you got.

### Look for scam tip-offs.

- » You don't have an account with the company.
- » The message is missing your name or uses bad grammar and spelling.
- » The person asks for personal information, including passwords.
- » **But note: some phishing schemes are sophisticated and look very real, so check it out and protect yourself.**



### Protect yourself.

- » Keep your computer security up to date and back up your data often.
- » Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts





# What is SPAM

Spam is digital junk mail that is unsolicited communications sent in bulk over the internet or via any electronic messaging system. There are several types of Spams.

- **Email** - clogs up your inbox and distracts you
  - **SEO** - is the abuse of search engine optimization (SEO) methods to improve search rankings for the spammer's website.
- They are 2 categories – **Content** and **Link** Spams
- **Content** - Spammers list popular keywords on their websites so their sites may rank higher in searches for those keywords. Others will rewrite existing content to make their pages seem more interesting and unique
  - **Link** - a blog comment or forum post that is filled with irrelevant links to have more traffic on their web pages
  - **Social Networking** - fake “throwaway” accounts on popular social networking platforms
  - **Mobile** - text messages, including push notifications to draw your attention to their offers
  - **Messaging** - similar to email spam, but quicker. These blast messages are sent on instant messaging platforms including WhatsApp, Skype, and Snapchat.





# What is PHISHING

## Phishing: Don't Take the Bait

*Phishing* is when you get emails, texts, or calls that seem to be from companies or people you know. But they're actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.



### What is Phishing?

Phishing is a type of social engineering attack often used to steal your data such as login credentials, banking, credit card or personal information. The attacker usually use an email or malicious websites (usually occurs by clicking on a link) to acquire your information or to infect your machine with malware and viruses.

There are 5 common types of Phishing attacks occurring today. They are **Email**, **Spear**, **Whaling**, **Smishing** & **Vishing** and **Angler** phishing.

# SPAMMING VS PHISHING

## Differences Between Spamming and Phishing

The difference between **Spamming** and **Phishing** is the intent of the spammer or phisher. **Spammers** are usually selling a product and wants you to purchase it. By spamming users, spam can be an effective technique for promoting their product, offer, or service but the products and/or services may be low quality or fraudulent.

As opposed to **Phishers**, they are cybercriminals seeking to gain access to your sensitive personal information either via deception or using malware.

## How to Recognize Spam

- **Health and medical services:** Miracle cures, weight-loss shortcuts, dietary supplements of dubious repute, hair loss therapies etc.
- **Computers, internet, and tech:** software or hardware offers, internet or mobile services advertisements
- **Service enrollment:** attempts to enroll in a long-term service such as educational programs or insurance policies
- **Financial services and rewards;** promises to help you lessen monetary woes with low-interest loans, debt assistance etc.



# For Your Information

## College Administrative Email System Spam Filtering

Blocked	Last 30 days	Last 7 days
Dnsbl	124,278	37,842
Spam	548,040	134,366
Virus	1,325	380

## Federal Trade Commission

2018

There were more than 1.4 million fraud reports, where people lost money to the fraud; People lost over 1.25 billion to fraud

Top reports were: imposter scams, debt collection and identity theft

Younger people reported losing money more often than older people

When people in their 70s did lose money, the amount tended to be higher



# Email Phishing

## What is Email Phishing

An Email Phishing attack is an attempt to steal sensitive information via an email that appears to be from a legitimate organization. It is not a targeted attack and is usually sent to many individuals simultaneously.

An attacker may send several fraudulent messages to mimic actual emails from a spoofed organization. This is done by using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.

## How to Recognize an Email Phishing

- Emails demanding urgent actions
- Requesting confirmation of personal/financial information
- Email with unfamiliar greeting or salutation
- Offer coupons for free stuff
- Emails with incorrect grammar and spelling mistakes
- Inconsistencies in Email Addresses, Links & Domain Names





## Email Phishing Example

- **Subject: Urgent Job Opportunity**

From: John.Doe@mail.citytech.cuny.edu

Date: Sat 9/22/2020 2:15pm

Good Day,

Are you seeking a for a flexible part time job you can work from home and earn \$500 and above weekly?

If interested kindly contact Mr. Leon Thomas via email {Leon.Thomas@warren-interiors.com} and also include your Full Name | Alternate email address | Phone number for urgent details of employment

Regards,

Academy Career Opportunity.

Copyright 2020 © New York City College of Technology. All Rights Reserved.

# Spear Phishing

## What is Spear Phishing

A Spear Phishing attack targets a specific person, group of individuals or enterprise, as opposed to random users as in an Email Phishing attack. This attack is done to acquire information or access to systems. It requires special knowledge about an organization, including its power structure.

## How to Recognize Spear Phishing

- An email or social media message from a familiar or trusted source requesting your personal information, such as account passwords, pin, social security number and /or access codes.
- Message contains odd grammar, poor word choices or misspellings.
- An email that appears to be from a manager or colleague at work that includes an urgent request for money or your financial information.
- Contains a peculiar or unexpected attachment





# Spear Phishing Example

- Notification Reminder

Reminder: [Recent News] [Statement Appointment] Information Updates - New Notice : We sent Summary of your bill has expire, Renews your membership Sunday, Jan 22, 2020 [Statement:- [FWD] Case ID: M68EXXSC

TeamNetflix <noreplyrthismailerid33@ieuwgfuiwegfi>  
owe [REDACTED]  
Wed 22/01/2020 02:51

**NETFLIX**

**Automatic payment.**

Hi Customer,

Your Auto payment cannot process.  
Your subscription period will end on Wed, January 22, 2020.

[Click Here](#) to update payment method

please update your payment methode for continue Netflix feature.

# Whaling Phishing

## What is Whaling Phishing

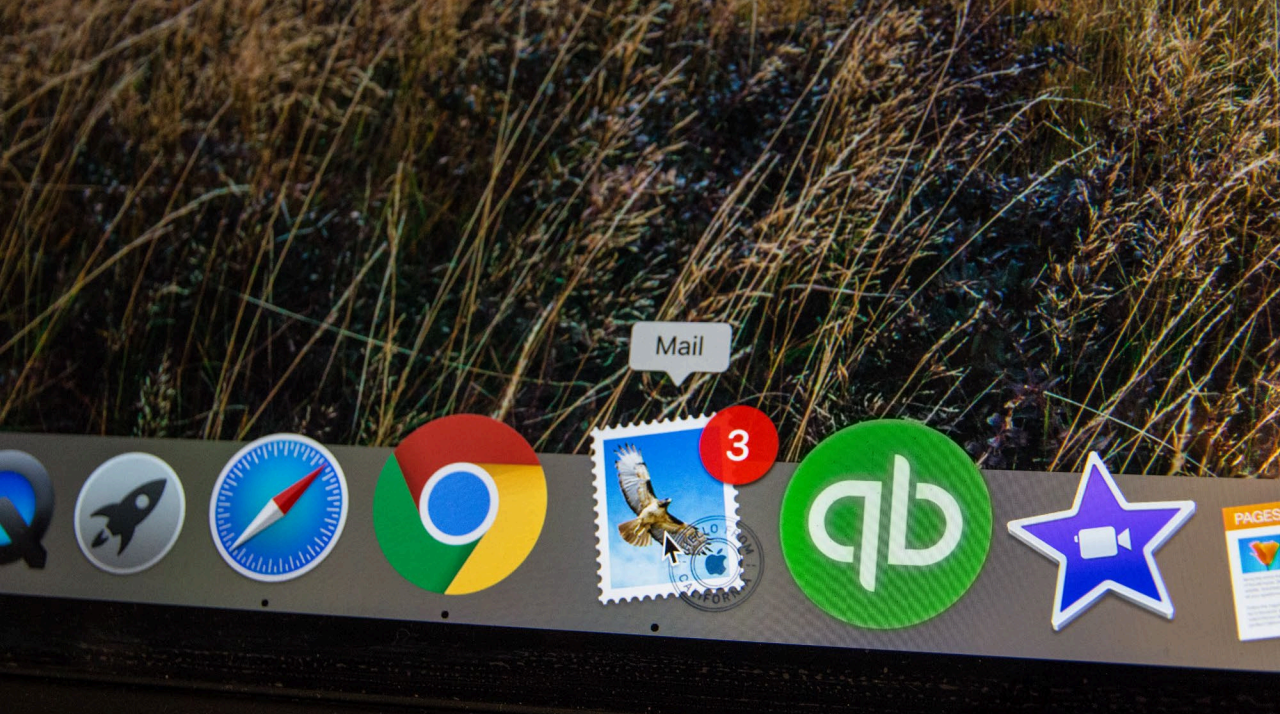
A Whaling Phishing attack targets high ranking employees such as CEOs or upper management employees who have access to sensitive information. This attack is done to steal data from companies. The attacker's goal is to manipulate the victim into authorizing an executive into revealing personal or corporate data most often via email and website spoofing.

These attacks are more difficult to detect than standard phishing attacks.

## How to Recognize Whaling

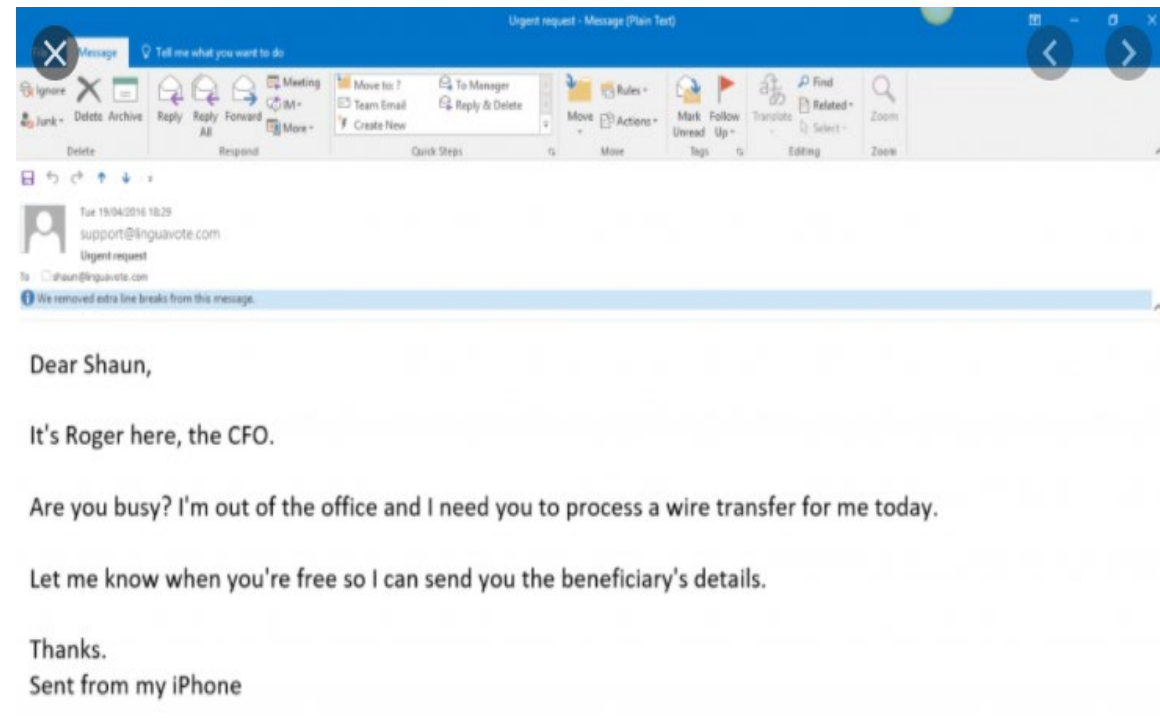
- Does the sender email address look correct?
- Are there added numbers and /or letters to the email address?
- Does it use the correct domain?
- Check for spelling and grammatical errors in the subject line and the body of an email
- An email that appears to be from a manager or colleague at work that includes an urgent request for money or your financial information.





# Whaling Phishing Example

- Request for a Wire Transfer



# Smishing & Vishing

## What is Smishing & Vishing

**Smishing** is a SMS-enabled phishing that delivers malicious short links to smartphone users, often disguised as account notices, prize notifications, political messages, links to risky sites or requests to download a malicious app onto a smartphone.

**Vishing** is a type of social engineering done by a scammer via phone about free offers or informing you that you have won a prize but in order to obtain the free offer or prize, you must first pay for shipping and handling.

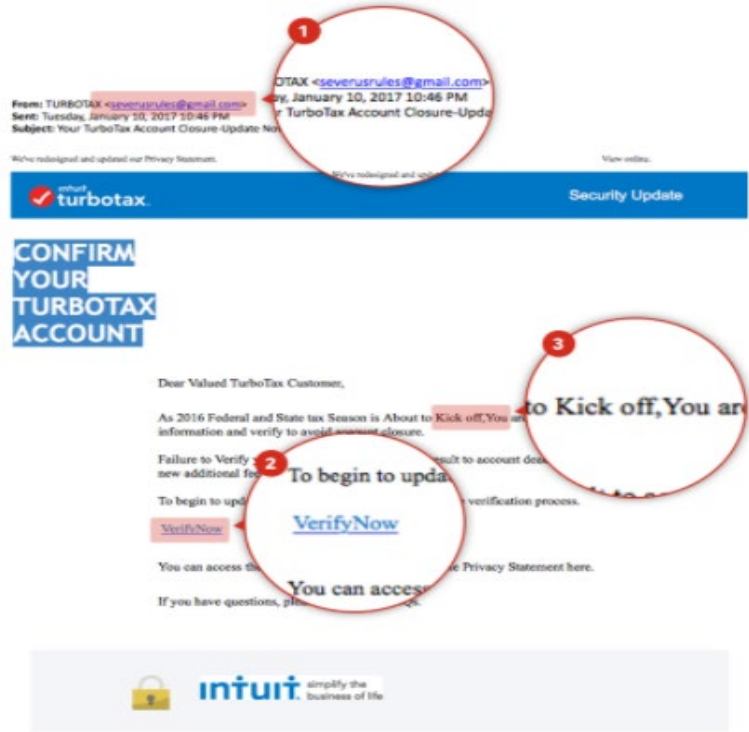
## How to Recognize Smishing & Vishing

- Be aware of links that may trigger the downloading of apps
- Don't send sensitive information in response to strange texts
- Be mindful of text messages claiming to offer free gifts but requiring your financial information
- The caller claims to be an IRS employee requesting financial information
- The caller asks for verification of your personal information





- Verification and Activation Requests



# Smishing & Vishing Examples

Today 07:25

Your Santander Bank Account has been blocked. All services have been withdrawn. Go to <http://santander.onlineupdatesecures.he.net.pk> to reactivate now.



# Angler Phishing

## What is Angler Phishing

Angler Phishing is the practice of masquerading as a customer service account on social media, that con customers into revealing their personal information.

## How to Recognize Angler Phishing

- Check the keywords in the body of the message, including phrases such as a bank or wire transfer, which are often suspicious
- Request to contact customer support because your account maybe cancelled
- The caller claims to be an IRS employee requesting financial information
- The caller asks for verification of your personal information
- Links or attachments in emails that come from anonymous sources





# Angler Phishing Example

- Customer Service Request

[Paypal Team] : Login to your account and update your information✓



This is an automated email, please do not reply

information about your account :

**Warning! Your PayPal account was limited!**

Your account has been limited temporarily in order to protect it. The account will continue to be limited until it is approved.

Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

The process does not take more than 5 minutes.

Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

[Click here to Confirm Your Account Information.](#)

Department review PayPal accounts

copyright 1999-2016 PayPal.All rights reserved  
PayPal FSA Register Number:1388561750

PayPal Email ID PP**156930**

# How to Avoid Being a Victim

# Avoid Being a Victim

Do Your Part. #BeCyberSmart



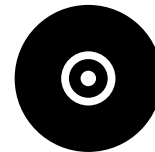
Protect your device by using security software



Protect your mobile phone by setting software to update automatically



Protect your accounts by using multi-factor authentication



Protect your data by backing it up on a regular basis

# Tips for Victims of Phishing Attacks


# Tips for Victims

Do Your Part. #BeCyberSmart


## The Bait



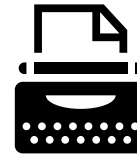
Scammers use familiar company names or pretend to be someone you know.



They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information.



They pressure you to act now — or something bad will happen.



Change your passwords immediately



Scan all devices used online



Contact your bank and credit card institution(s)



File a police report with your local precinct



Request a free credit report



# Helpful Links



- <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing>
- <https://www.identitytheft.gov/databreach>
- <https://www.cisa.gov/cyber-safety>