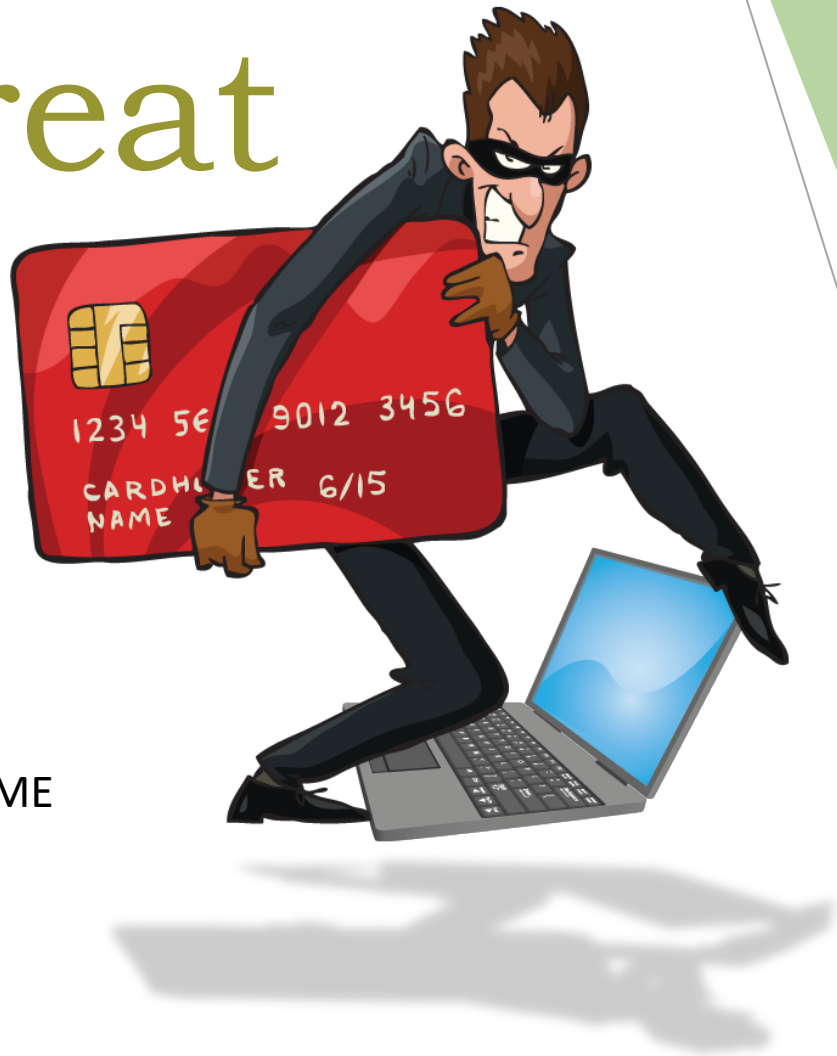
TCS Forensics LIMITED

The Cyber Threat Phishing



Presented by:

Andrew Anderson, EnCE, ACE, CCNA, CCO, CCPA, CCME
Cyber Forensic Examiner

OVERVIEW

1) What is Phishing?

2) What are Phishing Indicators?

3) How Phishing attacks are perpetrated?

4) What are the different types of Phishing attacks?

4) Dealing with Phishing Attacks.

WHAT IS PHISHING?

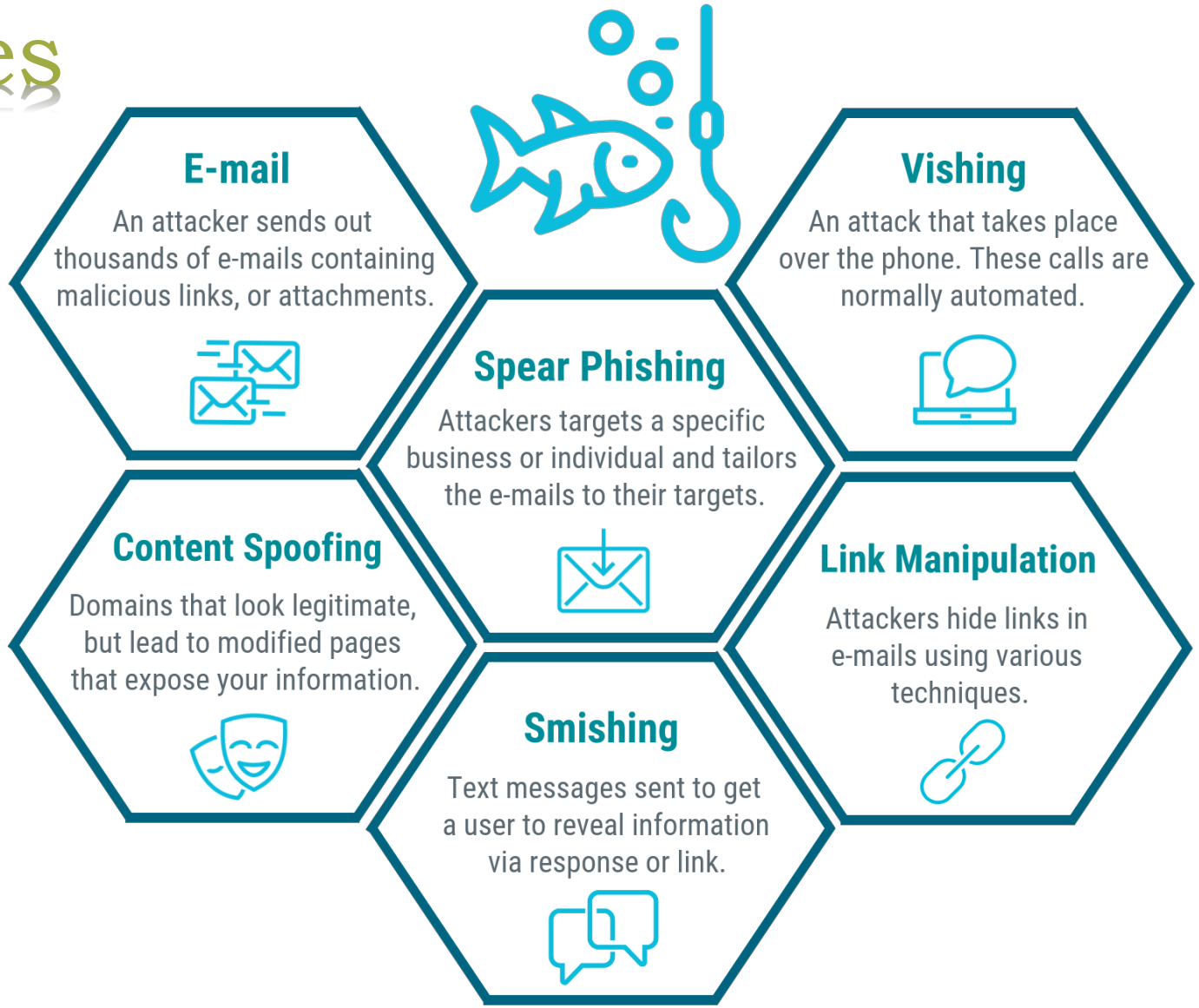
- Phishing is the '**malicious**' attempt to obtain sensitive information such as Personally Identifiable Information by disguising oneself as a trustworthy entity in an electronic communication

History of Phishing

- The practice originated sometime around the year 1995.
- Phishing scams use spoofed emails and websites as lures to prompt people to voluntarily hand over sensitive information.
  - Eg. passwords, usernames, and credit card details.
- The first way in which **phishers** conducted attacks was by stealing users' passwords and using algorithms to create randomized credit card numbers.

Phishing Techniques

There are a number of different techniques used to obtain personal information from users.



Emails

- The Most common.
- Millions of users with a request to fill in personal details
- An urgent note which requires the user to enter credentials to update account information, change details, or verify accounts.

Spear Phishing

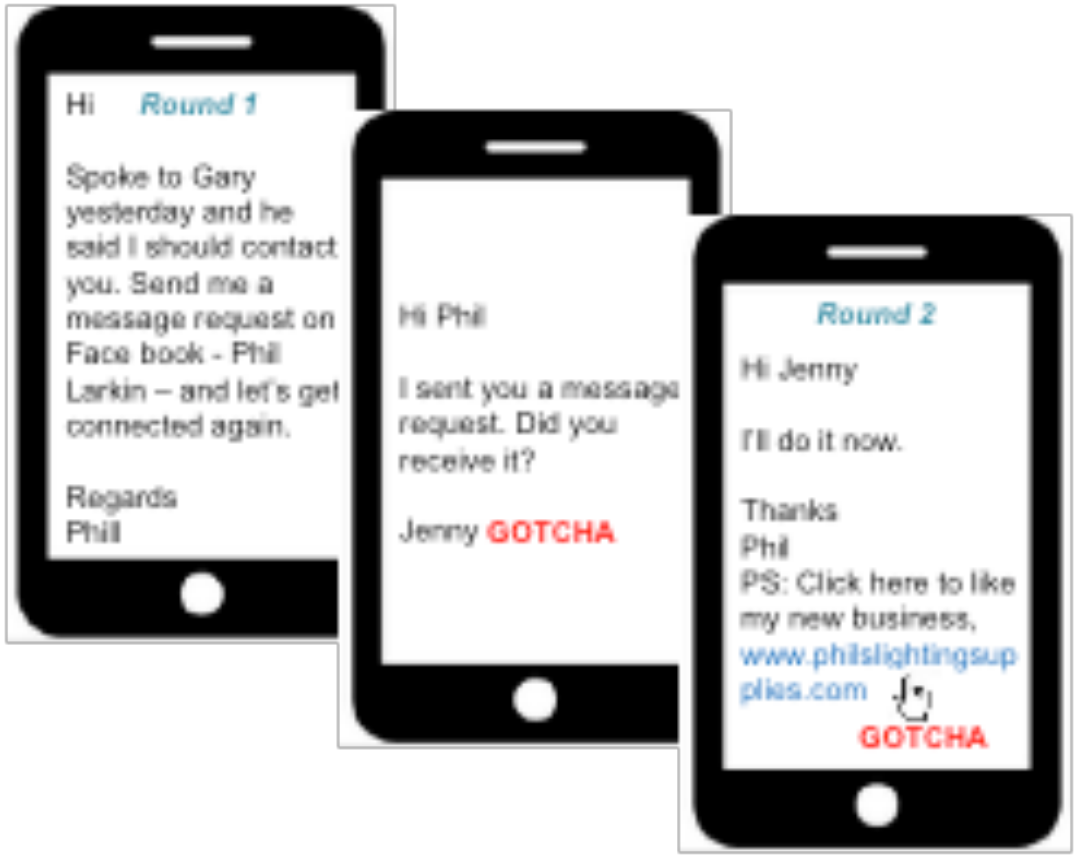
- Spear phishing is a much more targeted attack in which the hacker knows which specific individual or organization they are after.

Vishing

- In phone phishing, the phisher makes phone calls to the user and asks the user to dial a number. The purpose is to get personal information of the bank account through the phone.

Smishing (SMS Phishing)

- Phishing conducted via Short Message Service (SMS), a telephone-based text messaging service.

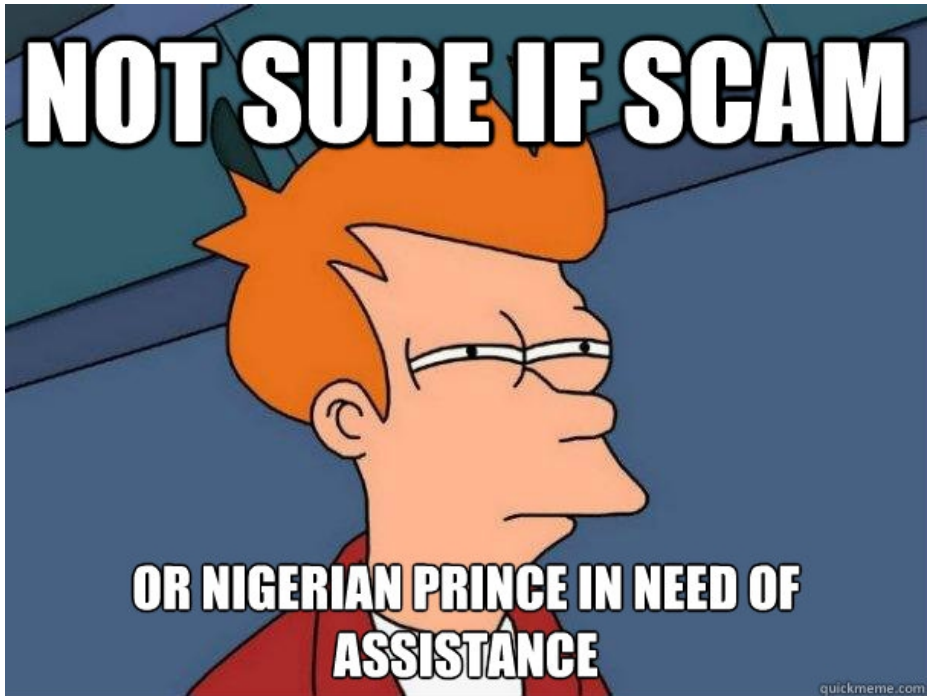


Common features of Phishing Emails

- Too Good to be True
- Sense of Urgency
- Hyperlinks
- Attachments
- Unusual Sender

Too Good To Be True

- Eye-catching or attention-grabbing statements designed to attract your attention immediately.



Sense of Urgency

- A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time.

- Some of them will even tell you that you have only a few minutes to respond.

Hyperlinks

- A link may not be what it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking it.
  - for instance '**www.amazon.com/tracking/1Z9Y425V0235449T**'- may redirect you to '**www.phishing.ru/exploit.php**'

Attachments

- If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it!
  - They often contain payloads like ransomware or other viruses.

Unusual Sender

- Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

From: Amazon Customer Service <customerservice@amason.com>

Check Email address, TO, FROM, CC

Subject: **Package Not Delivered**

Date: November 5, 2019 10:48 PDT (-7)

➡ 1 Attachment, PackageTracking.pdf (180kb)

Suspicious attachment

Dear Customer,

Generic Salutation

Grammar and Spelling mistakes

Unfortunately we unable to deliver you package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.

Order# 78541

Shipping Tracking information

Tracking #: 1Z9Y425V0235449T

Tracking Information: https://www.amazon.com/tracking/1Z9Y425V0235449T

Ship Date: 11/02/2019

http://www.phishing.ru/exploit.php

Thank you

Amazon Customer Service

Tue 2019-10-29 3:00 AM

PC

Publishers Clearing House <br1597@bangla.net>

Congratulation

Check Email address, TO, FROM, CC

To

--

Dear Lucky Winner,

Generic Salutation

Grammar and Spelling mistakes

We are pleased to announce to you that your email address emerged alongside 4 others as a category 2 winner in this year's Publishers Clearing House Consequently. You have won One million dollars and therefore been approved for a total payout of One million dollars ($1,000,000.00 USD) The following particulars are attached to your lotto payment order:

Winning Numbers: 1400
Email Ticket Number: ETN9091176

Please contact the underlined claims officer with the Contact info below

AGENT: Mr. James Patrick
EMAIL: pch claimsdept@msn.com

Winner, you are to send the details below to process the immediate payment of your prize

1. Name in full:
2. Address:
3. Phone Number:
4. Sex:
5. Nationality:
6. Age:
7. Present Country:

Requesting Personally Identifiable Information

Yours Sincerely,
Mr. Jason Sebastian
ONLINE CO-ORDINATOR.

WHY Should you Care?

- You are the **MOST** effective way to detect and stop a phishing attack.
- If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately.
- You and your devices are worth a tremendous amount of money to cyber criminal, and they will do anything they can to hack them.

Summary

Main takeaways from this presentation

- Check email for common feature of Phishing indicators
- Contact your help desk immediately, if you are concerned you may have fallen victim.
- If it seems too good to be true, it probably is!