

PHISHING AWARENESS TRAINING

RAUNAK KUMAR JHA
TASK-2





WHAT IS PHISHING?

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

TYPES OF PHISHING ATTACKS

Social Engineering - On your Facebook profile or LinkedIn profile, you can find: Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, your Relationship Status, Telephone Number, Email Address and Favorite Food. This is everything a Cybercriminal needs in order to fool you into thinking that the message or email is legitimate.

Link Manipulation - Most methods of phishing use some form of deception designed to make a link in an email appear to belong to the spoofed organization or person. Misspelled URLs or the use of subdomains are common tricks used by phishers.

TYPES OF PHISHING ATTACKS

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

Clone phishing - A type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email.

TYPES OF PHISHING ATTACKS

Voice Phishing - Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to personal and financial information from the public for the purpose of financial reward. Sometimes referred to as 'vishing', Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

EXAMPLES OF PHISHING ATTACKS

Spear Phishing



1. The first question you have to ask is, “**Do I know this person?**” or “**Am I expecting an email from the person?**” If you answered no to either question, you must take a harder look at other aspects of the email
2. A large amount of phishing emails will blank out the To: or Cc: fields so that you cannot see that this is a mass email to a large group of people.
3. Phishing emails will often come with subjects that are in all capitals or have multiple exclamation marks in order for you to think that this email is important or that you should take the recommended action within the email.
4. This is a targeted email (Spear Phishing) to VSU, so more than likely, this was sent to everyone at VSU that the sender had in their address book.

EXAMPLES OF PHISHING ATTACKS

Clone Phishing



Dear Valued Customer

2
[REDACTED] The payment have been made to your paypal account for an auction item: (ACER LAPTOP{Like New!} +FREE SOFTWARE!! +=) the money have been transferred to your paypal account by one of our client (alexjohnsoncole02@gmail.com) and it has also been **Approved** and confirmed here with us but we just need the shipment confirmation from you so that we may credit and release the money to your account immediately. Go ahead with the shipment of the item now to it's destination address and get back to us with the shipment tracking number of the item being sent to our client and we used this NEW POLICY of ours to protect both the BUYER and the SELLER from any internet fraud activities.

SHIPPING ADDRESS

NAME..... [REDACTED]

house no..... 80

street [REDACTED]

county [REDACTED]

state..... [REDACTED]

post code..... [REDACTED]

country..... [REDACTED]

****PLEASE NOTE****

Once shipment has been verified and the tracking number sent to us, You will receive a "CONFIRMATION Email" from PayPal® informing you that the Money has been credited.

Note: Pay pal will be responsible for the item loss or damage once we receive the tracking number.

This PayPal® payment has been deducted from the buyer's account and has been "APPROVED" but will not be credited to your account until the shipment reference/tracking number is sent to us for shipment verification so as to secure both the buyer and the seller. Below are the necessary information requested before your account will be credited. Make sure you send the tracking number to us through this mail (paypalonlinefundteam@mail2world.com) and our customer service care will attend to you. As soon as you send us the shipment's tracking number to us for security purposes and the safety of the buyer and the seller, the money will be credited to your account. 3

Thank you for using PayPal!
The PayPal® Team



EXAMPLES OF PHISHING ATTACKS

Link manipulation

From: [REDACTED] <[REDACTED]@valdosta.edu> ¹
Date: Wednesday, January 28, 2015 at 2:09 PM ²
Subject: UPDATE YOUR E-MAIL ACCOUNT!!

UPDATE YOUR E-MAIL ACCOUNT!! ³

Your email account will soon be suspended (<http://tuto-web.fr/wp-addon/notice/> ⁴ Click to follow link nce).
To update your email account, please [CLICK HERE](#) immediately for reactivation of your mail account. This mail is sent to you from our secured CSSD service Center. Please follow instruction on this message and your account will be updated within 24 hours.
We sincerely apologize for the unusual problem.

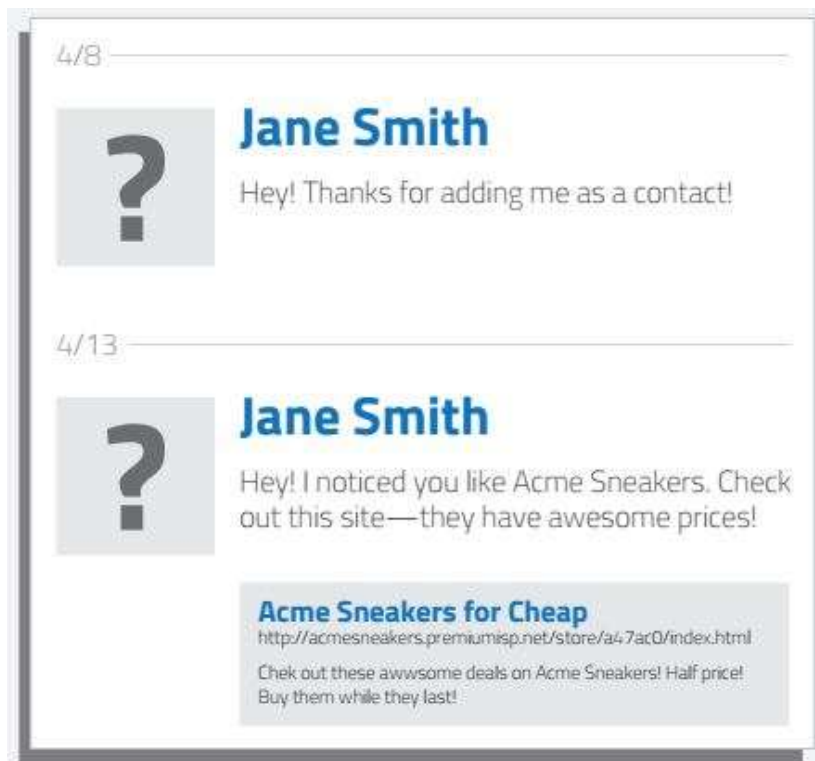
Thank you for using our online services.

Web-Administrator. ⁵

1.

EXAMPLES OF PHISHING ATTACKS

Social Engineering



The example on the left is a targeted social engineering attack. Cybercriminals scan your profile for your likes and then send you a crafted message over social media trying to trick you into clicking the link, which would then steal your social media login and take over your profile sending out more phishing attacks to your friends/contact list.

The one on the right is an example of a mass phishing attack through social media. No doubt many of you have seen these in Facebook, from random people in messages, or from your friends through their timelines..



CAN YOU SPOT THE TELL-TALE SIGNS OF A PHISHING EMAIL?

From: [REDACTED]
Sent: Wednesday, January 21, 2015 2:58 PM
Subject: Account Update..

Attn: Faculty/Staff/Students,

Your email account will soon be suspended (Reason: Quarterly quota maintenance). To update your email account, please [CLICK HERE](#) immediately for reactivation of your Web-Mail Account.

This message is from Webmail Administrator Messaging Center to all Webmail Account Owners. Please follow instruction on this message and your account will be updated within 24hours. We sincerely apologize for this unusual problem.

Thank you for using our online services.
Webmail Administrator.

CAN YOU SPOT THE TELL-TALE SIGNS OF A PHISHING EMAIL?

From: [REDACTED]@Vanderbilt.Edu>
Sent: Monday, December 8, 2014 6:35 AM
To: [REDACTED]
Subject: RE: ITS HELP-DESK

Dear user,

The following evaluations have been assigned to you. Please log in to complete these evaluations.

[CLICK HERE TO EVALUATE USING SECURE ENCRYPTION](#)

NOTE: Your log in will time out after 60 minutes. Your responses will be lost if you do not click on the "secure" button before 60 minutes lapses. There is no prompt when your 60 minute session has expired. Please save extensive comments periodically and check your time.

ITS help desk
ADMIN TEAM

©Copyright 2014 Microsoft
All Right Reserved.

CAN YOU SPOT THE TELL-TALE SIGNS OF A PHISHING EMAIL?

From: [REDACTED] **1**
Sent: Wednesday, January 21, 2015 2:58 PM
Subject: Account Update..

2

Attn: Faculty/Staff/Students,

<http://mstitches.twomini.com/gbriton/>
Click to follow link

Your email account will soon be suspended (Reason: Quarterly quota maintenance). To update your email account, please [CLICK HERE](#) immediately for reactivation of your Web-Mail Account.


3


This message is from Webmail Administrator Messaging Center to all Webmail Account Owners. Please follow instruction on this message and your account will be updated within 24hours. We sincerely apologize for this unusual problem.

Thank you for using our online services.
Webmail Administrator. **4**

1. The first thing to ask yourself, do I know this person and should they be emailing me about email accounts. If you answered no, then more than likely it is a phishing attempt.
2. The To: and Cc: are not showing so that you won't be able to tell this is a mass email attempting to get as many people as possible.
3. **Hovering your mouse over the link**, you can see that this is not a valid valdosta.edu address, but rather an external address attempting to get your email credentials or install malicious software. This should be your main "Aha" moment to let you know that this is indeed a phishing email."

TIPS TO PROTECT YOURSELF FROM PHISHING EMAILS.

- I.T. will **NEVER** ask for your password over email. Please be wary of any emails asking for passwords. **Never send passwords, bank account numbers, or other private information in an email.**
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. If you are not expecting an email with an attachment from someone, such as a fax or a PDF, please **call** and ask them if they indeed sent the email. If not, let them know they are sending out Phishing emails and need to change their email password immediately.
- **Never** enter private or personal information into a popup window.
- If there is a link in an email, use your mouse to hover over that link to see if it is sending you to where it claims to be, this can thwart many phishing attempts.
- Look for '**https://**' and a **lock icon**  in the address bar before entering any private information on a website.
- Look for spelling and bad grammar. Cybercriminals are not known for their grammar and spelling..



WHAT TO DO WHEN YOU THINK YOU RECEIVED A PHISHING EMAIL.

- First, **do not** click on any links within the email or download any attachment. Forward the email to abuse@valdosta.edu for Information Security to examine and determine if legitimate.
- If there is an attachment in the email, and you recognize the sender but aren't expecting an attachment from them, please **call** them and ask if it is legitimate.



SIGNS OF A PHISHING PHONE CALL:

- You've been specially selected (for this offer).
- You'll get a free bonus if you buy our product.
- You've won one of five valuable prizes.
- You've won big money in a foreign lottery.
- This investment is low risk and provides a higher return than you can get anywhere else.
- You have to make up your mind right away.
- You trust me, right?
- You don't need to check our company with anyone.
- We'll just put the shipping and handling charges on your credit card.



TIPS TO PROTECT YOURSELF FROM PHISHING PHONE CALLS.

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- **Never** send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.



WHAT TO DO IF YOU THINK YOU ARE RECEIVING A PHISHING CALL

- Always look up the phone number in Google. Often times, others have received these calls before and will log the number and the type of scam to different websites. Some of the websites are 800notes.com, callercenter.com, and callercomplaints.com. Users will let you know whether or not this is a scam, and what the caller will ask for.
- Resist pressure to make a decision immediately.
- **Keep your credit card, checking account, or Social Security numbers to yourself.** Don't tell them to callers you don't know — even if they ask you to “confirm” this information. That's a trick.
- Get all information in writing before you agree to buy.
- Beware of offers to “help” you recover money you have already lost. Callers that say they are law enforcement officers who will help you get your money back “for a fee” are scammers.



THANK YOU