


All Things Phishing

What is phishing, spear phishing, whaling?

Johnny Chuah
jchuah@csc.c.edu
 Columbus State Community College

Phishing

- ▶ What is phishing?
 - ▶ From imperva.com = Phishing involves sending malicious messages from supposed trusted sources to as many people as possible,
 - ▶ Combines the nature of spamming with a malicious fraudulent twist, intent to trick
 - ▶ For example, a phishing email might appear or claim to be from your utility company
 - ▶ Ask the recipient to verify their account details by clicking on an enclosed link
 - ▶ It then leads to the installation of malware on the victim's computer
 - ▶ Phishing is a type of cyberattack that uses disguised email (primarily) as a weapon
 - ▶ A form of social engineering - uses psychology and human-nature manipulation techniques
- ▶ Objective of phishing
 - ▶ To trick the recipient into believing that the message is from someone else




Phishing II

- ▶ I see it in my emails but is it really common?
 - ▶ About **15 BILLION spam emails daily**
 - ▶ From comparitech.com = "phishing attacks hit an all-time high in 2021"
- ▶ Does phishing really work?
 - ▶ From cybertalk.org = "When asked about the impact of successful phishing attacks, 60% of security leaders stated that their organization lost data, 52% experienced credential compromise, and 47% of organizations contended with ransomware."
- ▶ IT WORKS
 - ▶ Phishing = mass messaging, indiscriminate, large list of recipients
 - ▶ Spearphishing = targeted list of recipients, eg. List of staff workers in the accounting department
 - ▶ Whaling = or whale phishing, targeted at the big fish of the company, CEO, CFO, VP, senior accountant, high-value target of a company




Phishing - their M.O. Modus Operandi

- ▶ After **convincing / tricking you to think they are someone else...**
 - ▶ Eg. Your bank, your shopping store, your uncle, your HR
- ▶ Next step is **convince you to DO something...**
 - ▶ Click on a link
 - ▶ Reset your password
 - ▶ Enter your credentials to logon
 - ▶ Send money
 - ▶ Divulge personal information (or "secret" information that lead to revealing other information)
 - ▶ Accept a friend request
- ▶ Messages...
 - ▶ Alerting of a delivery
 - ▶ Soliciting donations or blood drive due to a natural disaster
 - ▶ Cheap medications or shopping deals
 - ▶ Password needs to be changed
- ▶ Popups and notifications...
 - ▶ Warning that your computer is infected
 - ▶ Notifying you that your computer needs to be updated
 - ▶ Notifying you that your software needs update




Phishing - How to detect?

- ▶ Check the FROM email address
 - ▶ The name of sender can be easily spoofed
 - ▶ The email address of sender can also be spoofed but a little more difficult
 - ▶ Is the email account name correct, the part of the email before the @ symbol
 - ▶ Check the spelling!! Look out for transposed letters, is the email johnny@companyxyz.com or jonny@companyxyz.com
- ▶ Check the domain name of the email address
 - ▶ The part of the email after the @ symbol
 - ▶ Check the spelling!! Look out for transposed letters, is the domain name really companyxyz.com or thecompanyxyz.com
- ▶ Check and validate the links in the email
 - ▶ Details in next slide
- ▶ Check for spelling or content errors
- ▶ Be suspicious



Phishing - How to check?

- ▶ Links in email - NEVER click on them unless you verify
 - ▶ NOT BY CLICKING THEM and seeing where the links take you
 - ▶ Too late, just the act of landing on these malicious websites could infect and compromise your computer
 - ▶ Hover over link, validate from the popup or status bar of what the URL/domain is
 - ▶ Copy and paste, verify with online checkers
 - ▶ Copy and paste, and just visually verify
 - ▶ Shortened URLs - copy and paste to online checkers
 - ▶ Demo = tinyurl.com, shorturlcheck.com
- ▶ Check and validate information or request for information using another mode of communication
 - ▶ Call the person, text, meet
 - ▶ Validate with IT administrator if email telling you to change the password is valid - can be phone call, separate email, office memo, weekly meeting
 - ▶ That is like a "multi factor authentication"
- ▶ Check for typos - usually, not always



Phishing - How to respond?

- ▶ Delete
- ▶ Inform others
- ▶ Inform IT department
 - ▶ They could be conducting a phishing exercise or the real phishing emails are getting past their filters
 - ▶ A heads up to colleagues, other staff
- ▶ If it's too good to be true...



Examples of Successful Phishing

- ▶ Phishing/spear phishing/whaling campaign with a highly attractive or applicable scenario
 - ▶ Cheap online drugs - not really
 - ▶ Online dating - small percentage
 - ▶ Amazon delivery - 70% Americans are Amazon Prime members
 - ▶ Appeal for help after natural disaster
 - ▶ "Tax season" emails
 - ▶ Internal email / memo - company-specific messages, giveaways, survey
 - ▶ Email content can be specific, targeted at company, business, industry, location
 - ▶ Can be highly targeted if attacker has "inside" information
 - ▶ Or can be highly researched for specific information

Review of What, Why, How

- ▶ Phishing attackers want to bait and trick you
 - ▶ Bait - something that applies to you, that you want, interested in
 - ▶ Trick - To fool you to believe they are what you think they are
- ▶ Methods that worked in the past
 - ▶ Messages that appeal to your good nature (so that you'll give them what they want)
 - ▶ Create a sense of urgency (so that you'll rush and skip the necessary verification processes)
 - ▶ Create a convincing scenario (so that you'll bypass the "inconvenient, time consuming" checks)
 - ▶ Using easily confusing information - incorrect names, emails, links, etc

Recommendations for NOT Falling to Phishing

- ▶ BE VIGILANT
- ▶ DO not rush, especially when it comes to responding to requests for secure information, financial assets
- ▶ Especially when it comes to such requests, no shortcuts but take the time for validation and verification
 - ▶ That means, phone calls, texts, verifying emails
- ▶ VERIFY
- ▶ VALIDATE
- ▶ BE VIGILANT
- ▶ Be safe
- ▶ Questions?
