Defense Against Phishing

Social Engineering

Introduction

- Organizations spend a fortune purchasing technology and security services, but their network infrastructure could still remain vulnerable to old-fashioned human manipulation.
- You'll learn about eight unique phishing traps and how to spot them. You'll also learn what you should and shouldn't do to protect yourself from becoming a victim; and steps you can take if you suspect you've become a victim.

What is Phishing?

- Phishing is the fraudulent use of emails, websites and phone calls to trick recipients into disclosing personal information such as account names, passwords, addresses, credit card and Social Security numbers.
- Phishers pose as a trustworthy organization to get people to unwittingly click on images and fake links in emails, visit malicious websites or call fraudulent phone numbers.

The Goal of Phishing

- The information is then either used by fraudsters for their own needs such as impersonate the victim to transfer funds from the victim's account, purchase merchandise, or sell it in a variety of online brokering forums and chat channels for a profit.
- Phishers and internet criminals are often very organized and connected. They may go after one piece of information, such as an ATM card PIN, to correlate it later with existing information, such as the card number and CVV.

Common Phishing Vectors

- Email
- Pop ups
- Phone phishing
- SMS text messages on cellular phones
- Malicious websites
- Poisoned search results
- Fake wireless networks

General Email Attacks

Defense Against Phishing

General Email Attacks

- Attackers congregate email addresses from a variety of sources such as:
- Newsgroups,
- Web pages
- Guesswork

and more

- They may stalk social networking sites, hack into company databases or compromise the personal email accounts of those who don’t adhere to security best practices. These lists are then traded across the Internet.

General Email Phishing Attacks

- In many cases, the phisher entices the user into opening an email attachment, visiting a fake website or downloading a file

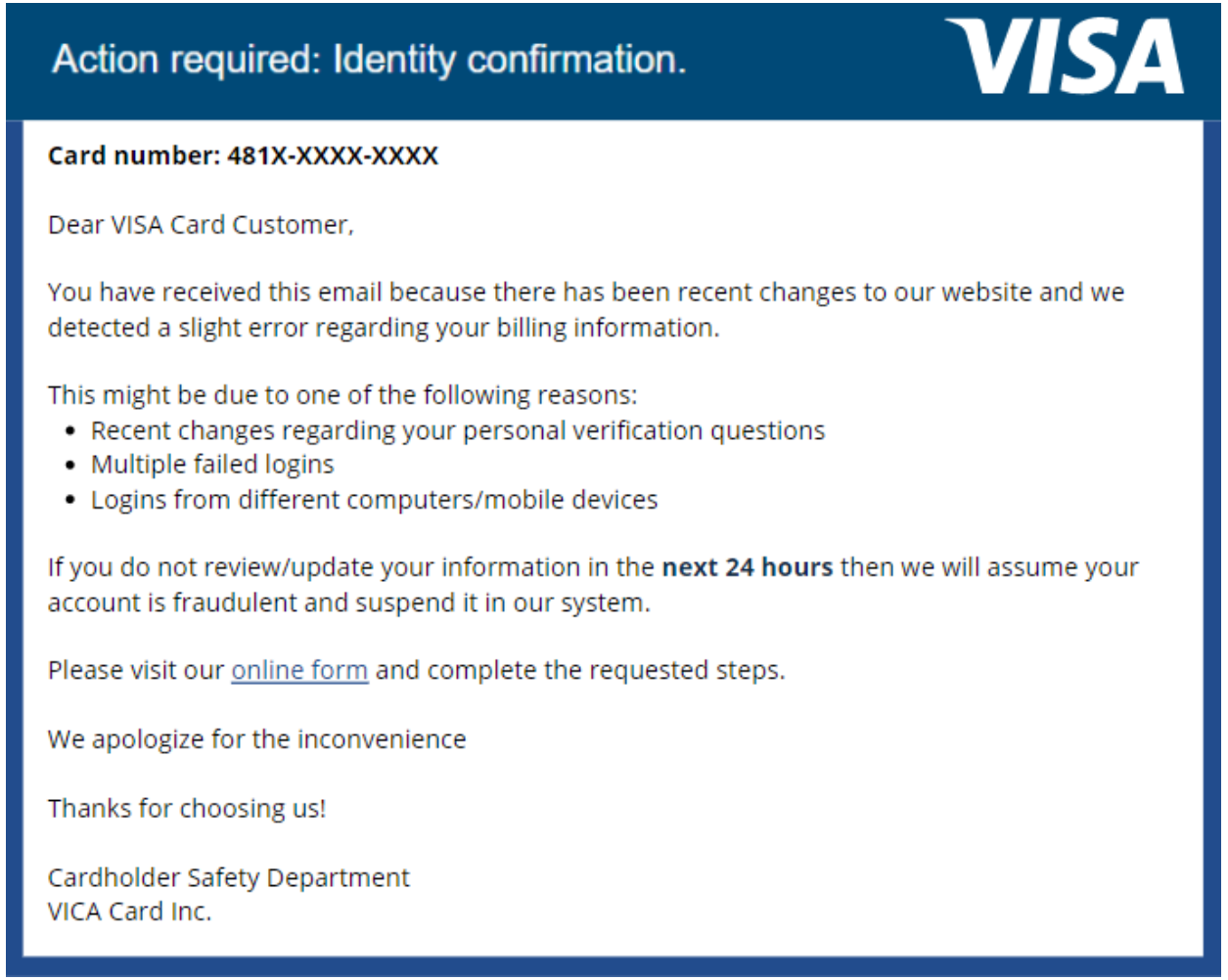
The Three Components of a Phishing Email

1. **Hook:** tells you why you should trust what the email is saying. For example, “We detected fraudulent attempts to access your account.”
2. **Required Action:** what the phishers want you to do. For example, the phish may ask you to email personal account information or click on a link purporting to take you to the targeted institution’s website to provide personal account information.
3. **Push:** provides incentive to carry out the required action before you either forget or the phish is taken down. An example of a push is “If you do not update your account information within 24 hours, we will lock access to your account.”

General Email Phishing Attacks

The Hook
Why you should trust what the email is saying

The Action
What the phishers want you to do



The Push
Incentive to carry out the required action

How to Spot a Phishing Attack

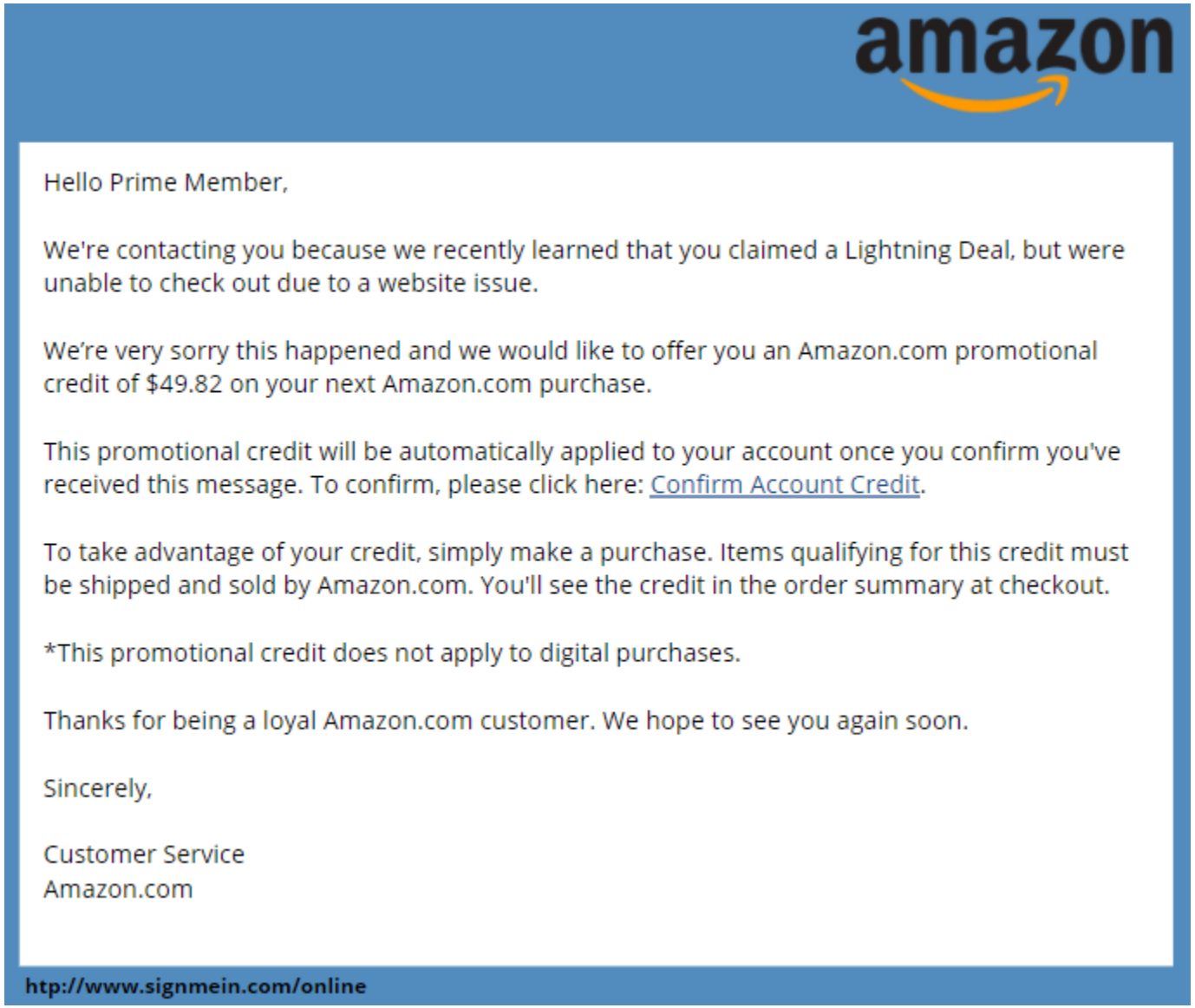
- Who is the email from?
  - Look at the “From:” field. Is the sender’s name or email address familiar to you? Does it use a webmail account like Hotmail when it claims to be from my bank?
- Is there a URL in the email?
  - Where's the hyperlink going to? To see where the hyperlink is actually going, hover over it with your mouse (don’t click it). The true URL will be displayed on the bottom in the status bar.
- Is there a threat of immediate detrimental action if you don’t respond with personal information?
  - A message demanding an immediate response deserves a good dose of skepticis

How to Spot a Phishing Attack (Continued…)

- Does the email refer to a current news event?
  - Major news events such as large-scale catastrophes or the death of celebrities are quickly followed by a wave of phishing messages touting the same news events in their subject lines or email body. Phishers are hoping that overeager users will let their guard down and click on their proffered URL links in their haste for more information.
- Does the tone of the email from friends or colleagues sound right?
  - Filter the messages based on what you know of the purported senders and how they typically write.

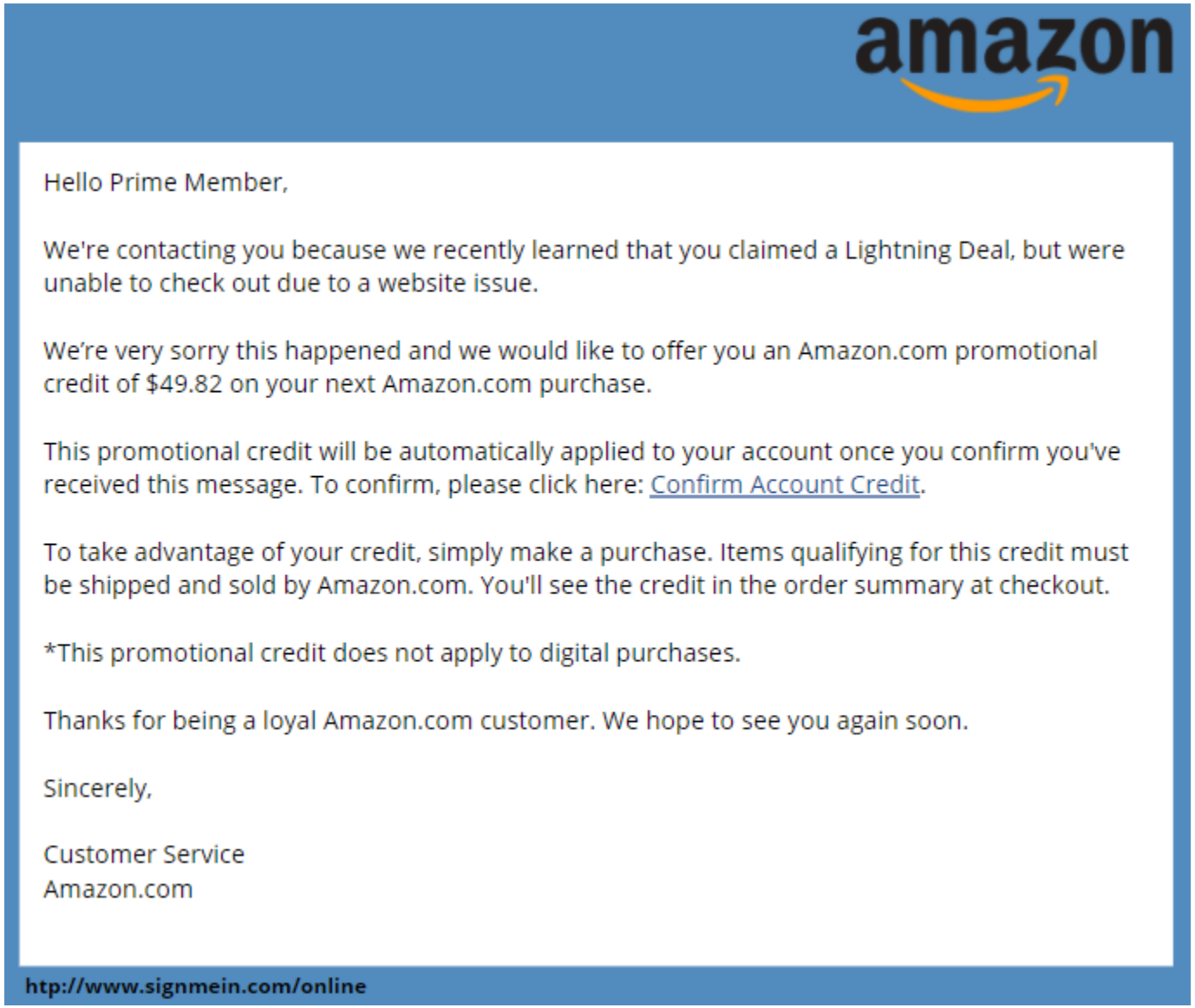
Test Your Knowledge

- Can you tell the difference between a legitimate email and a phishing email?
- Look at the email and see if you can determine whether or not it’s legitimate.
- The following slide will evaluate the components of the email & display the results.



Test Your Knowledge

- This is a phishing email
- Key Takeaways:
  - The logo at the top makes the email look real
  - The email does not address you directly
  - The URL on the bottom of the email does not line up with what they are advertising on the clickable link
  - The use of technical and exciting terms such as “Lightning deal” are used to mask the fact it is a phishing email



Spear Phishing Attacks / Targeting Emails

- In spear phishing, attackers identify a company to compromise and send email to select groups and individuals within the organization whom they have previously researched.
- Their goal is to obtain small amounts of information, bit by bit, from a number of different employees within the same organization.
- Spear phishing has proven successful in numerous high-profile breaches, including those of RSA and Google.
- In the case of the Google breach, phishers stalked Google employees on social networking sites such as Facebook where they were able to harvest and exploit data on employees, impersonate the friends of Google employees and share malicious links that ultimately gave them access to Google's corporate network.

Pop-Up Windows/Pharming

- With this type of attack, hostile code is used to generate rogue pop-up browser windows on legitimate websites requesting that you reenter your username and password.
- Malware injected onto a compromised website can also identify which website you're currently logged onto, when using multiple tabs. This attack is especially plausible if you navigate to another site, while leaving a secure session running in another tab. Note that these pop-up windows can be made to look like part of the website you're visiting or even your company network.

Malicious Website

- Several million of those websites contain malicious software or malicious code. Some of these sites are legitimate websites that have been compromised, while others are created by hackers whose main mission is to infect your computer with spyware, Trojans and worse.
- Even if you don’t click on any links on a malicious website, your computer can get infected just by visiting it.
- Phishers often use counterfeit emails to lead users to these fake websites designed to trick them into divulging personal information and to plant malicious software onto their computers.

Phone Phishing & Vishing

- Criminals often use phone number spoofing to make a different number show up on the target's caller ID to give the appearance that calls come from a trusted organization.
- They also may try to get you to call a phone number listed in a fraudulent email. Email messages can appear to be from a bank and tell users to dial a phone number regarding problems with their bank account.
- Once the phone number (owned by the phisher and provided by a voice over IP service) is dialed, prompts tell users to enter their account numbers and PIN. This type of attack is called vishing, short for voice phishing.

Poisoned Search Results

- Even when you are using a popular search engine to find information, you may run across fake and poisoned links in search results. In search results poisoning — the use of search engines as a conduit for profit-driven hackers.
- Some search terms are riskier than others. Some examples include:
  - Screensavers
  - Game cheats
  - Free music downloads
  - Word unscramble
  - Work from home
  - How do I?
  - Popular celebrity names

Smishing: Phishing SMS Messages

- Cell phones, tablets and mobile devices are becoming increasingly targeted by perpetrators of malware, viruses and scams. Text messages (SMS) are read immediately as people have cellphones with them all the time.
- Smishing is short for "SMS phishing," the act of phishing for private information, often to be used for identity theft.
- These smishing attempts come to your phone saying things like:
  - We're confirming you've signed up for our service
  - Your account has been suspended
  - (Random) bank is confirming your purchase.
- The recipient is tricked into divulging personal information or into downloading a Trojan horse, virus or other malware onto their cellular phone or other mobile device.

Fake Wireless Networks

- A fake wireless network is a phishing technique that is hard to detect. A phisher creates a fake wireless network that looks similar to a legitimate public network or wireless “hotspot” that may be found in public places such as airports, hotels or coffee shops.
- Whenever someone logs on to the bogus network, fraudsters try to intercept and capture their passwords and/or credit card information and may even attempt take complete control of your device.
- Public wireless networks are not secure. They are akin to the old analog phone system party line when lines were shared and if you happened to pick up your phone while another was using the same line, you could hear what others were saying.
- When your mobile device or your laptop connects to a public WiFi, it is sharing the airwaves with other devices in the vicinity. Unless the traffic your computer is transmitting to the network is encrypted, other network devices have the ability to see your transmissions.

Tabnabbing

- Tabnabbing comes into play while using multiple browser tabs
- It takes advantage of the multiple tabs that users open in a browser and silently replaces the contents of an inactive browser tab with a malicious site
- Tabnabbing operates in reverse of most phishing attacks in that it doesn’t ask users to click on an obfuscated link but instead loads a fake page in one of the open tabs in your browser.

How to Protect Yourself

Defense Against Phishing

Tips to Protect Yourself From Online Phishing

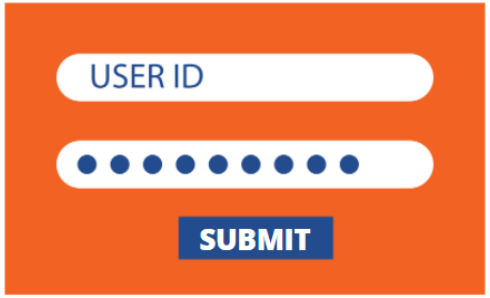
- Be suspicious of any email that requires immediate action or creates a sense of urgency. This is a common method used to trick people.
- Be suspicious of emails addressed to “Dear Customer” or some other generic salutation.
- Be suspicious of grammar or spelling mistakes, most businesses proofread their messages very carefully.
- If a link in an email seems suspicious, hover your mouse over the link. The true destination will display in the status bar at the bottom of your screen.
- Do not click on links. Instead copy the URL from the email and paste it into your browser.
- To check whether the message is really from the company or agency, call it directly or go to its website (use a search engine to find it).
- Be suspicious of attachments.
- Don’t assume that the presence of personal information alone guarantees that a message is legitimate.

Tips to Protect Yourself From Spear Phishing Emails

- Be careful what personal information you include about yourself on social networking sites. Less is better.
- The information you provide in your profile and posts can be used to piece together your identity.
- Private information should always be regarded as belonging to the public domain once it can be found on social networking sites such as Facebook.

Tips to Protect Yourself From Deceptive Pop-Up Windows

- Never enter your personal information in a pop-up screen. Legitimate companies, agencies and organizations don’t ask for personal information via pop-up screens. Install pop-up blocking software to help prevent this type of phishing attack.
- To access your online banking account, type the domain name into a new browser window yourself. The address of your genuine bank website will start https.



Tips to Protect Yourself from Malicious Websites

- Never click on links within an email. Instead, type the destination name into your browser yourself.
- Look for website verification. Valid sites that use encryption to securely transfer sensitive information are characterized by a lock on the bottom right of your browser window or a green address bar, and they have addresses that begin with https:// rather than the usual http://
- Install a safe search tool like McAfee SiteAdvisor on your browser which will notify you of risky websites

Protect Yourself From Phone Phishing & Vishing

- Never give your personal information over the phone unless you have initiated the call and you know with whom you are talking.
- Always verify a contact number. If the “bank” called you, call them back at a number you’ve verified.
- If someone contacts you and says you’ve been a victim of fraud, verify the person’s identity before you provide any personal information.

Protect Yourself Against Poisoned Search Results

- The latest generation web browsers come with built-in phishing protection
- When searching the Web, use a safe search tool like McAfee SiteAdvisor
- Don’t click on links in the search results that are not verified by a certified authority

Protect Yourself From Fraudulent SMS Text Messages

- Never reply to an SMS or email message that requests personal information.
- Do not click on any of the links that may be embedded in the message.
- Double check phone numbers that appear in an SMS - you can do this via the Internet or by referring to any marketing material. For ease of reference, store banking phone numbers on your mobile phone, along with email and website addresses.
- Contact the sender directly to determine if they sent you a legitimate request.
- If unsure whether or not something is a scam, always take the time to investigate it.
- Contact your cell phone provider and forward a copy of the SMS so that they may investigate it.

Protect Yourself From Fake Wireless Networks

- Avoid using hotspots that are run by people you don't know or trust.
- Understand that public WiFi hotspots or wireless networks are not secure.
- Use a Virtual Private Network (VPN) when accessing free wireless hotspots. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted.
- If you can't connect securely using sending confidential email. You should also avoid any site VPN, and online banking or shopping and sites that require you to enter passwords.
- When you connect to a WiFi network, many devices will prompt you to enter a network type ('home', 'work' or 'public'). Always connect as 'public' when you connect to a public WiFi network, as this will lock down the connection more securely.
- Disable wireless networking when you are not using it.

Protect Yourself From Tabnabbing

- Make sure you always check to be sure the URL in the browser address page is correct before you enter any login details. A fake tabbed page will have a different URL than the website you think you are using.
- If the URL looks suspicious in any way, close the tab and reopen it by entering the correct URL again.
- When banking online, don’t open multiple tabs. Open a new window instead.
- Never leave your computer unattended when logged into your online accounts or when you’ve provided credit card information on a shopping site.
- Don't log in on a tab that you have not opened yourself.

Other Methods of Defense

- You need a multi-layered defense to protect yourself:
- Protect your computer with spam filters, anti-virus, anti-malware, and anti-spyware software, and a firewall, and keep them up to date.
- Keep your operating system, web browser, and software up to date, as they provide the latest security updates (patches).
- Use strong passwords. An ideal password is at least eight characters in length and contains letters, punctuation, symbols and numbers.
- Use different passwords for different sites. Never use your online banking password for any other purpose.
- Never share your PIN number or password with anyone, especially someone you don't know.
- Backup your music, pictures and other files regularly.
- Protect yourself against eavesdroppers and freeloaders by using encryption on your wireless network.
- When disposing of your computer and mobile devices, use software to erase and over-write data on your hard disk to ensure that it is not recoverable.

Mitigating an Attack

Defense Against Phishing

Mitigating an Attack

- What to do if you suspect you've become a victim of a phishing attack
- Act immediately if you've been hooked by a phisher. If you provided account numbers, PINS, or passwords to a phisher, notify the companies with whom you have the accounts right away.
- Change all your passwords and pin numbers immediately, even if you suspect that your any one of your passwords has gone to the wrong hands.

Mitigating an Attack – Report It

- If you are unsure of how a company received your number, or are suspicious about an email, phone call, or SMS that you have received, you should contact the company and report your concerns.
- Report phishing, whether you're a victim or not. Tell the company or agency that the phisher was impersonating.
- Report frauYou can also report the problem to law enforcement agencies through NCL's Fraud Center, www.fraud.org, the Anti-Phishing Working Group, the U.S. Federal Trade Commission (FTC) and the FBI through the Internet Fraud Complaint Center, all of whom work to shut down phishing sites and catch those responsible. The information you provide helps to stop fraud.

Staying Alert

- Phishing is one sphere of activity where ignorance is never bliss.
- As long as there are gullible people around, there will be crooks to take advantage of human vulnerabilities like carelessness, laziness, greed, and ignorance.
- Aided and abetted by technology, these attacks are increasing by the day.
- A little alertness will go a long way in fighting these cybercriminals.

CONGRATULATIONS

This concludes the Employee Security Awareness Training on “Phishing”