CYBER THREATS – PHISHING ATTACK

Criminals love to deceive people especially during a pandemic. This kind of crisis, like the Coronavirus pandemic, give criminals the opportunity to tempt their victims into taking the **Phishing bait**. During this time, people are very vulnerable and would usually turn into their financial institutions, employers, the government and other relevant authorities for guidance. So, when a fraud email or any fraud communication from any of these entities with instructions or promises is received, the victim will not question it. A very impulsive click in the computer or on the phone and the victim's device is infected, then the bank account is compromised.

Phishing is an example of social engineering technique that deceive users. This cyber attack is a fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, credit card details and bank information. It disguises as a trustworthy entity in an electronic communication such as emails, instant messaging and text messaging. The goal is to trick the victim to believe that the electronic communication like an email is a request from the financial institution and to click a link or download an attachment.

Types of Phishing:

Spear Phishing

When attackers try to craft a message to appeal to a specific individual, that's called *Spear Phishing*. Phishers identify their targets (sometimes using information on sites like LinkedIn) and use spoofed addresses to send emails that could plausibly look like they're coming from co-workers. For instance, the spear phisher might target someone in the finance department and pretend to be the victim's manager requesting a large bank transfer on short notice.

Whaling

The term *Whaling* refers to spear phishing attacks directed specifically at the very big fish, namely senior executives like a CEO and other high-profile targets. Gathering enough information to trick a high-value target might take time, but it can have a surprisingly high payoff. Examples of the content of a whaling attack email may be an executive issue such as a subpoena or customer complaint.

Catphishing and catfishing

Catphishing is a type of online deception that involves getting to know someone closely in order to gain access to information or resources and to get control over the conduct of the target.
Catfishing, a similar but distinct concept, involves a person creating a social network presence as a sock puppet or fictional person in order to trick someone into a (usually) romantic relationship. This usually begins online, with the hope of it progressing to real-life romance. This is never the objective of the perpetrator though. In general, he is seeking access to money or resources, or to receive gifts or other consideration from the victim.

Clone Phishing

Clone Phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link, has had its content and recipient address taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version. This is then sent from a spoofed email address. It would appear as if it came from the original sender and it may claim to be a resend or an updated version of the original. Typically, this requires either the sender or recipient to have been previously hacked for the malicious third party to obtain the legitimate email.

Voice phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a financial institution would tell users to dial a phone number regarding problems with their bank accounts. Once the phone number (which is owned by the phisher and provided by a voice over IP service) is dialed, prompts would tell users to enter their account

numbers and PIN. *Voice Phishing or Vishing* uses fake caller-ID data to give the appearance that calls come from a trusted organization.

SMS Phishing

SMS Phishing or Smishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. Smishing attacks typically invite the user to click a link, call a phone number, or contact an email address provided by the attacker via SMS message. The victim is then invited to provide their private data; often, credentials to other websites or services. Furthermore, due to the nature of mobile browsers, URLs may not be fully displayed; this may make it more difficult to identify an illegitimate log-in page. As the mobile phone market is now saturated with smartphones which all have fast internet connectivity, a malicious link sent via SMS can yield the same result as it would if sent via email. Smishing messages may come from telephone numbers that are in a strange or unexpected format.

How to Prevent Phishing

1. Keep Informed About Phishing Techniques – New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one.

2. Think Before You Click! – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead? A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information, but the email may not contain your name. Most phishing emails will start with "Dear Customer" so you should be in alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.

3. Install an Anti-Phishing Toolbar – Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

4. Verify a Site's Security – It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar. Check for the site's security certificate as well. If you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites. Even search engines may show certain links which may lead users to a phishing webpage which offers low cost products. If the user makes purchases at such a website, the credit card details will be accessed by cybercriminals.

5. Check Your Online Accounts Regularly – If you don't visit an online account for a while, someone could be having a field day with it. Even if you don't technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements from your financial institutions and check each entry carefully to ensure no fraudulent transactions have been made without your knowledge.

6. Keep Your Browser Up to Date – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop. The minute an update is available, download and install it.

7. Use Firewalls – High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.

8. Be Wary of Pop-Ups – Pop-up windows often masquerade as legitimate components of a website. All too often, they are phishing attempts. Many popular browsers allow you to block pop-ups. You can allow them on a case-by-case basis. If one manages to slip through the cracks, don't click on the "cancel" button because such buttons often lead to phishing sites. Instead, click the small "x" in the upper corner of the window.

9. Never Give Out Personal Information – As a general rule, you should never share personal or financially sensitive information over the Internet. When in doubt, go visit the main website of the company in question, get their number and give them a call. Most of the phishing emails will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with "https".

10. Use Antivirus Software – There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes. Just be sure to keep your software up to date. New definitions are added all the time because new scams are also being dreamed up all the time. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly. Firewall protection prevents access to malicious files by blocking the attacks. Antivirus software scans every file which comes through the Internet to your computer. It helps to prevent damage to your system. You don't have to live in fear of phishing scams. By keeping the preceding tips in mind, you should be able to enjoy a worry-free online experience.

SOURCES:

https://en.wikipedia.org/wiki/Phishing
https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
https://www.phishing.org/10-ways-to-avoid-phishing-scams

IMPORTANT FRAUD LINKS

Canadian Anti-Fraud Centre – Reporting Fraud
http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm

Canadian Anti-Fraud Centre – Recent Scams and Fraud
http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

Royal Canadian Mounted Police
https://www.rcmp-grc.gc.ca/

Report a scam or fraud
https://www.ontario.ca/page/report-scam-or-fraud

Government of Canada – Questions and Complaints
http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00019.html

Kijiji Help Desk - Avoiding Reply Scams
http://help.kijiji.ca/helpdesk/safety/avoiding-reply-scams

Youtube Video – Get Cyber Safe
http://www.getcybersafe.gc.ca/cnt/rsrcs/vds/phshng-en.aspx