TECH CORNER

Dear Member

Following on from last week's article on Spoofing, this week we will looking at various forms of social engineering, there are many but this week we will focus on **Phishing**, **Spear Phishing**, **Vishing** and **Whaling**– no rods or nets needed! As other terms are used in the guide below that may not be familiar, I have created a link directly to Wikipedia to explain these words in further detail. These words will look like this - HYPERLINK. Hover over the word and Use Ctrl and Click to take you directly to the web page.

Phishing

Phishing is a cybercrime in which mass targets (not targeting individuals) are contacted by email, by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.

Common Features of Phishing Emails

1. **Too Good To Be True -** Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just do not click on any suspicious emails. Remember that if it seems too good to be true, it probably is!
2. **Sense of Urgency -** A favourite 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. When you come across these kinds of emails, it is best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organisations give ample time before they terminate an account and they never ask customers to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.
3. **Hyperlinks -** A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different, or it could be a popular website with a misspelling, for instance www.bankofemgland.co.uk on first glance looks genuine but - the 'n' is actually an 'm' so look carefully.

4. **Attachments -** If you see an attachment in an email you were not expecting or that does not make sense, do not open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
5. **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!

Though hackers are constantly coming up with new techniques, there are some things that you can do to protect yourself:

- To protect against spam mails, spam filters can be used. Generally, the filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it is spam. Occasionally, spam filters may even block emails from legitimate sources, so it is not always 100% accurate.
- The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked, or an alert message is shown. The settings of the browser should only allow reliable websites to open.
- Many websites require users to enter login information while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis, and never use the same password for multiple accounts. It's also a good idea for websites to use a CAPTCHA system for added security.
- Changes in browsing habits are required to prevent phishing. If verification is required, always contact the company personally before entering any details online.
- If there is a link in an email, hover over the URL first. Secure websites with a valid Secure Socket Layer (SSL) certificate begin with "https". Eventually all sites will be required to have a valid SSL.

Spear Phishing

Phishing in its generic form is a mass distribution exercise and involves the casting of a wide net. Phishing campaigns do not target victims individually—they are sent to hundreds, sometimes thousands, of recipients. Spear phishing, in contrast, is highly targeted and targets a single individual. Hackers do this by pretending to know you. It is personal.

A Spear Phishing attacker is after something in particular. To connect with you in a convincing way, the attacker may engage in social engineering to impersonate people you know, such as colleagues or business acquaintances. The attacker can accomplish this by researching you on the Internet and social media or getting information about you from data breaches.

Prevent Spear Phishing Attacks:

As well as the above tips for preventing phishing attacks also consider:

- Do not be swayed just because the sender seems to know a lot about you-

Someone who has never met you, and never will, can nevertheless easily project themselves as an "insider" – a friend-of-a-friend, perhaps, or a colleague you've worked with electronically but never met face-to-face.

With a mixture of information collected from already-public data breaches, social media profiles and historical emails that you sent or received, even a modestly funded crook without much technical savvy can sound a lot more convincing than "Dear Customer."

- Do not rely on details provided by the sender when you check up on them-

You would think that scammers would try very hard to discourage you from checking up on them – but sometimes they'll not only welcome it but actively urge you to call or message them back, or visit their website, as part of the scam.

If you call them back on the phone number they gave you, or message them via the website they provided, you are simply offering them an opportunity for them to tell you the very lies they want you to hear.

- Do not be afraid to get a second opinion

If you have ever asked colleagues to proofread your documents or emails, they will often have found mistakes that you cannot believe you missed yourself.

That is because a second opinion goes an awfully long way.

In fact, that is the main reason why crooks urge you not to tell anyone what you are up to – to stop you getting a second opinion and thereby catching them out.

Voice phishing = Vishing

A cyber criminal will contact you by telephone impersonating someone in a position of authority. Vishing is similar to phishing, but the attack is delivered by telephone instead of email. Automated messages may also be used.

Prevent Vishing:

- Verify unexpected phone requests in ways that are not connected to the incoming phone call. For example, use an official directory and another telephone to call the company's main office and ask to speak with the caller who is making the request.
- Be very suspicious of any caller who asks you to share login information over the phone.
- Companies will not call you to request that you change logins, passwords or divulge any personal information or account data. Any caller who makes this type of request is probably a scammer - Refuse the request.

Whaling:

Whaling is a highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email. Whaling is digitally enabled fraud through social engineering, designed to encourage victims to perform a secondary action, such as initiating a wire transfer of funds or requesting additional information about the business or an individual in order to conduct further attacks.

Initially whaling emails were not much harder to identify than their less targeted phishing counterparts. However, the adoption of fluent business terminology, industry knowledge, personal references and spoofed email addresses have made sophisticated whaling emails difficult for even a cautious eye to identify. Highly targeted content is now combined with several other methods which executives should be aware of to reduce their chances of falling victim to a whaling attack. Crucially all these developments either exploit existing trusted relationships or combine a cyber-attack with non-cyber fraud tactics.

Whaling emails are more sophisticated than generic phishing emails as they often target chief executives and usually:

- contain personalised information about the targeted organisation or individual
- convey a sense of urgency
- are crafted with a solid understanding of business language and tone

Nicholas Spike
Assistant Secretary