DANGERS OF PHISHING EMAILS

THREATADVICE COURSE OVERVIEW

Hackers are constantly innovating new social engineering tactics to steal critical data from users. The most common method that hackers continue to utilize is phishing attacks. “Phishing” is the act of luring users into surrendering personal data or account access. Phishing is also used to damage systems, networks, and devices through dangerous links, downloads, and malware. The common occurrence of phishing emails makes them one of the most dangerous threats facing users today. In many cases, users overlook phishing emails because they are disguised so well. The success of these attacks is primarily linked to a lack of understanding regarding the level of danger.

The Danger of Reputable Source Imitation

Users form a level of trust with various message senders that appear in their inbox. These sources can be coworkers, family, friends, or well-known brands. Hackers are fully aware of the trust that is developed and use that against victims to formulate well-crafted phishing emails. Cybercriminals use fake links to download malware onto the victim's computer. These malware links will often be disguised as a reputable company offering a discount that can only be applied for a limited time through the link. The best way to disarm these malicious links is by hovering over the link’s button with the mouse cursor. This will display the destination of the link before the user clicks on it. The email should then be reported as a phish to allow IT security personnel to investigate the threat.

In other cases, the phish will resemble a message from a coworker seeking company information that is outside of their department or access privileges. Any message that seems out of place should be double-checked through direct communication with all parties that are involved.

The Danger of Spear Phishing

A dangerous misconception regarding phishing emails is that all phishing emails are identical and easy to spot. Some of the most effective phishing attacks are articulately designed to manipulate specific people. These attacks are known as spear phishing attacks. Spear phishing

campaigns take time to carry out because cybercriminals have to meticulously study members of an organization to learn names, titles, and operation-based tasks. Users who let their guard down can easily fall victim to spear phishing, surrendering personal or company data.

The Danger of Clone Phishing

There are many variations of spear phishing that hackers will use to steal data or infect a system with malware. One of the most dangerous variations is known as clone phishing. In a clone phishing attack, cybercriminals will create an email that is nearly identical to legitimate emails sent out by trusted organizations. Hackers find success using this method because the victim becomes numb to receiving emails from this source and they miss the danger in the clone. Organizations that hackers are most likely to clone include banks, security system providers, business vendors, and government institutions or agencies. Users must treat every email as a potential threat until they are confident that the message is legitimate. It's extremely easy to fall into the trap of believing that every email sent from a particular organization is always safe. Hackers prey on user assumptions.

The Danger of Whaling

No department or position in an organization is too high or too low for cybersecurity awareness training. In fact, cybercriminals are aware of the users that may avoid cybersecurity training and will seek them out first. Attacks on users with a high profile are known as whaling attacks. Whaling is a type of phishing attack in which hackers target senior executives or other members of an organization that have extensive access privileges. Successful whaling attacks deal a significant blow to an organization's stability. It can be much harder for a company to recover from losing its most critical assets. This is why all executives must set the standard for the organization by staying dedicated to practicing cyber awareness.

Summary:

"Phishing" is the act of luring users into surrendering personal data or account access. Phishing is also used to damage systems, networks, and devices through dangerous links, downloads, and malware. The common occurrence of phishing emails makes them one of the most danger-

ous threats facing users today. The success of these attacks is primarily linked to a lack of understanding regarding the level of danger. The primary dangers associated with phishing include spear phishing, clone phishing, and whaling.

For assistance in evaluating your strategies, technical requirements, staff evaluations and communications contact a ThreatAdvice professional to learn more.