The Key to Thwarting a Phishing Attack

While anti-spam filters are a great tool for eliminating the barrage of unwanted email messages, it should not be the only protection in the security toolbox. Technology is continuously improving and anti-phishing measures can filter out malicious email, but these should not take the place of good security training and education. Technology is a supplement to a security plan against phishing, not the plan itself.

Here are several reasons that training should be an integral part of any organization's arsenal when it comes to thwarting phishing attacks:

1. Malicious email messages often arrive from legitimate email addresses.

It's not difficult to create an email address from a well-known email service that will most likely pass through spam filters. Cyber criminals will make up several of these from free services from which to send their spam. It's also not too hard to compromise real accounts and send messages to all of the contacts in a particular person's address list. Considering the recent wave of attacks on Office 365® users and the recent hoards of Tumblr®, LinkedIn® and other email addresses for sale on the dark web, this is a very real possibility and it could be some time before these are flagged as spam and filtered out.

2. Spammers test spam filters before sending out their messages.

There are many free tools that analyze email to determine what is and is not spam. The phishers will use these same tools to test their messages before sending them out to their targets. They change the messages ever so slightly by modifying the text with substitutions until they don't get any red flags and then off the messages go.

3. Attackers take advantage of information they find on social media and other public places.

All of the information floating around on the Internet can be used against you. Spam filters will "learn" with whom users are corresponding and the attackers can harvest personal data off various social media like Facebook® and LinkedIn to make matches. If a message comes through addressed to a particular person from someone the spam filter has "seen" before, it may just get through. Unfortunately, these personalized messages are 40% more likely to get someone to click a link or open an attachment.

4. IP Addresses Can be Trusted by Spam Filters.

Email messages come from servers with specific Internet Protocol (IP) addresses. Spam filtering tools trust certain ones - those that come from Gmail®, for example. Others are not so trustworthy, such as those that come from university dorms, airports, and other public places. They are considered transient and are flagged by filters. However, ultimately IP addresses can be "warmed up" and become more trusted by the tools. So an attacker can use servers with warmed up IP addresses and be more likely to pass right through any defenses that are in place.

Phishing in all its forms (spear-phishing, whaling) continues to be very effective and can be quite lucrative for attackers. People continue to be the weakest link in an organization's defense strategy. That's why training is so important. All of the tools in the world will not work if a phisher is able to convince someone to wire large sums of money. It's exciting to ponder artificial intelligence and technology tools, but they simply will never be able to subvert human actions. So take time to properly teach your users how to avoid becoming a victim of phishing.

The use of trademarks is not intended to endorse any company, product or service. Trademarks are the property of their registered owners.

Get the lastest information from our website. Scan the QR Code to go directly to this page.