AUTOBUILD NEWS

MiTek

GN GUIDELINES NO.247

ANOTHER MITEK ADVANTAGE – FEBRUARY 2018

By Daniel Heathershaw – IT Manager

Phishing, Spear Phishing and Whaling

Phishing. It's a strange word that's pronounced the same as fishing, which is apt because the term is used to describe a method employed by scammers to catch victims using bait. That bait comes in a variety of forms, such as email messages, phone calls or social media links. Phishing and some of its variations can be used to scam individuals and businesses out of large sums of money.

WHAT IS PHISHING?

Phishing has been around for a long time and the attacks come in a number of different varieties, but at its core it is a scam that is used to attempt to obtain money through deceit, or to obtain personal/private information that can be sold or used in identity theft.

Generally, phishing targets a large number of people simultaneously, with the aim of catching a few victims to exploit; kind of like throwing a net into the ocean. The results can vary but, depending on the sophistication of the scam, can be quite rewarding for the attacker.

However, phishing has evolved, and targeted phishing techniques – also known as Spear Phishing – have risen to the surface.

TARGETED PHISHING

Spear Phishing, has increased in frequency over the last year, as has a technique called CEO Fraud. Spear Phishing and CEO Fraud are generally accomplished when the attackers gain access to or spoof legitimate business email accounts with the aim of conducting unauthorised funds transfers.

Email accounts are an ideal target because they can be "spoofed", which is a when an attacker impersonates a legitimate business user by creating an email message with a forged sender address. To the naked eye these emails look legitimate and are often acted upon without much thought by the recipient.

Spear Phishing is a more targeted attack than plain phishing. Generally, a scammer will spend a significant amount of time studying his target to gather as much information as possible before launching an attack. The attack will target a particular person, or a small group and will include personalised details to make the attack look as legitimate as possible

Whaling or Executive Whaling is generally targeted at senior management or administration/finance staff. Again, attacks of this type are well researched, with the attacker often gaining intimate knowledge of internal payment processes or even business-to-business payment processes. In this example, a person responsible for bank deposits, or even the CFO, could receive an email from the 'CEO' asking them to immediately deposit an amount of money into a specific bank account. As the email looks like it has been sent by the CEO, there is an increased chance that the request may be acted upon.

> Phishing is a scam that attempts to obtain money, or information that can be sold or used in identity theft.

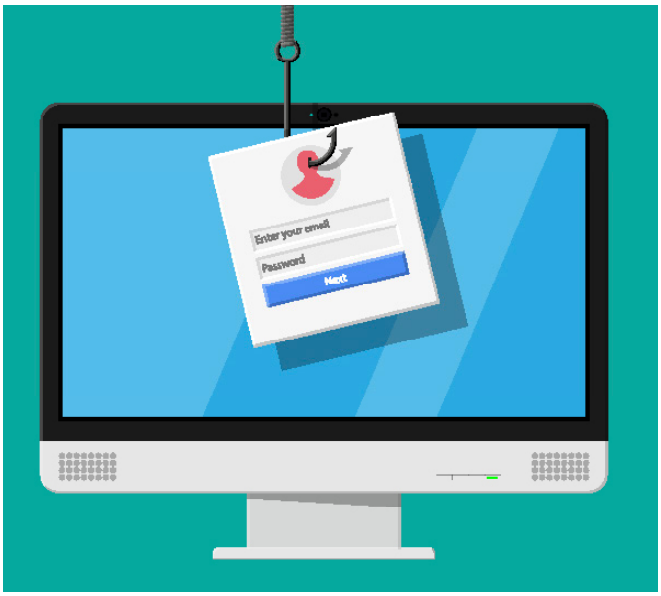

ILLUSTRATION: ABSCENT/SHUTTERSTOCK.COM

WHAT SHOULD YOU DO?

A number of methods can be put in place to protect your company from phishing attacks, such as implementing an email security system to filter out dangerous emails and protect your company from advanced threats. However, no technological solution is foolproof, and one of the best protection methods available is to invest in the education of your staff to help them identify fraudulent emails.

Another great idea is to review your internal processes to make it harder for a phishing attack to be effective. For example, you could require two or more forms of approval before a funds transfer can take effect.

As always, if you are unsure, contact your local IT Professional. T