SMARTPHONES - A GROWING TARGET

BY JAY BORDEN

When someone mentions cybersecurity or phishing or hacking or ransomware, people typically think of computers. But almost everyone has another device that is also vulnerable to all those attacks – their smart phones. After all, what makes them smart – a computer chip!

This means that the phones we carry are targets and cyberattackers are increasingly focused on the phones.

Research found that phishing is the most common attack type on phones as it is on computers. Why is it so common? Because no hacking is required, no credentials are required, nothing is required except the target's email address. The phishing messages are getting harder to spot due to the attackers getting smarter and the improvements made by the addition of AI.

Research also showed that almost one-quarter of respondents, 24%, said they were victims of a phishing attack on their phone.

All the popular phones, especially the high end ones claim to have anti-malware. But in tests none successfully blocked all the test messages. Certainly, keep the phone and its anti-malware up to date but don't expect it to keep you 100% safe.

Phishing is, after all, designed to fool people. Yes, it does have to get past the anti-malware. But the cybercriminals are getting better at sending messages that get through the anti-malware. Phishing emails often have a link to a compromised site. Anti-malware would examine that site and if malware was found, the email would be blocked. But now attackers direct you a clean site that then may direct you to an infected site and the anti-malware doesn't go that far.

The smart phone companies are working to block the phishing emails. But the cybercriminals are working to avoid the protections the vendors put in place.

SMARTPHONES - A GROWING TARGET

CONTINUED

The carriers and other tech companies have a stake in this and need to be working together to block a higher percentage of the phishing emails.

If the phones and the tech companies aren't catching all the phishing emails what can you do?

Educate yourself and your users. Education is an effective technique to protect against phishing on your phone and on your computer.

To be effective the training needs to catch and hold people's attention. If it is boring, it won't do anything. If it is too long, people will lose interest and start doing something else.

Be sure the training explains the real risks of phishing - for a small-medium enterprise a successful phishing attack can put the company out of business. Successful phishing will expose confidential information entrusted to the company by their customers. How will they feel if their information is exposed? If a ransomware is successful it may stop the company from processing orders, shipping orders, billing, etc. How long will the company survive in that state? Will the ransom be affordable or put the company in financial distress?

In addition to those costs, if you aren't properly protecting information you may be subject to fines and penalties. This is especially true in regulated industries.

Back to training, it needs to be more than once a year. Quarterly is good, more often may be better. That way people can be kept up to date on the latest attack techniques.

The partner of training is desktop exercises. These are phishing emails that are sent to employees to see who takes the bait. The emails have to look real. If they are obvious, everyone will identify them as phishing and feel they are good at spotting phishing emails. That plays right into the hands of attackers.

SMARTPHONES - A GROWING TARGET

Continued

If someone takes the bait, do not use punishment or public exposure. That will turn people off. It just means they need more training. Present it as an opportunity to learn how to protect themselves and the company.

People have been shown to be the cause of over 80% of breaches and phishing is the most common and successful form of attack. That is why training and desktop exercises can be so effective at keeping information safe and your company out of trouble.

Be sensible and protect your information.

Visit our site, onebrightlycyber.com to learn all the ways we help keep you safer.

Welcome to peace of mind.

onebrightlycyber.com
(888) 773-1920