INSIGHTS

Cyber made simple.

one brightly cyber

PHISHING IS ONLY THE BEGINNING PART 2

BY JAY BORDEN

Last week we looked at phishing and the variations that require no technical skill.

This week we look at the ones that require some technical skill. However, the skills of many cyberattackers are quite good so this is not a deterrent.

SEO, Search Engine Optimization, is how companies legitimately get their site to rank higher on any search engine's list of results. In a technique known as SEO Poisoning or SEO phishing, the attackers use the same techniques as legitimate sites to get a counterfeit site they created to rank higher than the real site on the search results. The hope is that you will not notice it is a fake site, click the link, go to the site and have malware downloaded on to your device. Victims of these attacks often blame the company they wanted to go to, not realizing they fell for the scam and actually went to a fake site.

Another technique using social media is called Angler phishing. It targets people who complain about a company on social media. The attacker replies to the complaint saying they are from the customer service department of the company. They request personal information to confirm your identity and resolve the complaint.

If cyber attackers can steal an email you already received, they can replace attachments and links in the email with their own and send it back to you. You will recognize it, recognize the sender and probably click the link. This is known as Clone phishing.

If these attacks were as dated and simple as the Nigerian prince, they wouldn't succeed as often as they do.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

PHISHING IS ONLY THE BEGINNING PART 2

Continued

What are some new attack messages? Phishing emails may arrive posing as a potential new client. The email will include attachments of prior files that appear to be relevant. For instance, for a medical practice, attachments of test results, for products, attachments of the desire product specifications or an RFP or a purchase order. The attached files may look real but will download malware.

Quishing – this scam focuses on people implementing a new phone or a new computer. Access to sites and applications must be confirmed for the new device. QR codes may be used to confirm identity of the user and grant access. But the forged QR code will steal credentials and highjack session keys and sessions needed to reset MFA, Multi-Factor Authentication. This gives the cybercriminals ongoing access to all the sites, data, and applications that the real user can access.

Fake password reset messages trick people into entering the old and new password that is then in the hands of cybercriminals. Once they have that they can log into the systems and not set off any alarms.

A variation on the fake password reset is to send emails that appear to come from vendors used frequently such as Dropbox and others requesting password resets. The credentials are then stolen and used to steal all the information.

What do they all have in common? They only succeed if people fall for the scam.

The best defense is educating people about all these and testing to see if they take the bait.

Remind users that reputable vendors and companies will not request personal information in an email or a text. If an email or text or voice call arrives requesting this personal information, hang up immediately and report it to your CISO or head of IT.

Clicking or copying links in emails can be very risky. It is better to enter the url directly by typing it into your browser. For a phone call requesting information, provide nothing, hang up and call the supposed person using a number you know or find on the official website.

Visit onebrightlycyber.com to learn all the ways we help protect you.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920