INSIGHTS

Cyber made simple.

one brightly cyber

PHISHING IS ONLY THE BEGINNING PART 1

BY JAY BORDEN

Phishing has been in the news for years as a popular scam. Remember the Nigerian Prince who promised to send money if you would send some to him as a good faith gesture? That was an early version of phishing.

It would be surprising if some variant of this isn't still out there, given how successful it was, or still is. However, the scams are getting much more believable, especially with AI, Artificial Intelligence, being used to create or improve them.

Phishing is quite common but has given rise to a number of variations. Knowing about them is the first step in staying safe. What are they?

Phishing is the biggest. In phishing an email is sent that appears to come from a trusted source and asks for confidential information such as username and password. Or it could ask for your social security number, or bank account number. Another variation asks you to initiate a wire transfer or purchase gift cards to pay an outstanding bill and prevent account closure or service disruption.

A form of phishing called spear phishing targets you specifically. To help improve its believability, the email may address you by name, mention the name of a colleague or an executive, a project you are working on, or even a client/customer. This is all to make you think it is legitimate and get you to click the link or send the requested information.

At times the spear phishing targets are executives. This has been named whale phishing as the executives are the big fish.

PHISHING IS ONLY THE BEGINNING PART 1

Continued

Communications have moved beyond just emails, and cybercriminals now use those also. Instead of emails the scam message may be sent by text. This is termed smishing, a combination of SMS, the formal name of texting, and phishing. The intent is the same, to get you to send credentials or money. Just the means of delivering it have changed.

Cybercriminals don't forget phone calls and voicemail. Then it is called vishing, a combination of voice and phishing. Again, with the same intent, getting you to believe the message comes from an authorized party and clicking a link or sending confidential information.

QR codes are the boxes with all the squiggly lines that you can scan with your phone to go to a site or get an offer or other things. QR codes are being used in many ways such as on websites, in ads, in restaurants to view menus and more. Quishing is a variation of phishing using QR codes. It replaces the real QR codes with fake ones that direct users to bad sites to steal credentials, download malware or both.

These are the attack types that target users directly. They take little to no technical expertise by the attacker. All that is needed is a list of names and email addresses or phone numbers of people at target companies. These can be bought relatively inexpensively on the Dark Web. Quishing does require creation of new QR codes that direct people to the fake website, creation of the fake website, and placing the new QR codes over the original ones. This does take some technical knowledge.

A bit more complex are phishing messages sent over social media platforms. On these the attackers need to find the target's social media account and then send the message. Not much more complex but a bit. It can be sent as a comment on a site or as a direct message to the user of that social media platform.

Next week we will continue looking at attack methods.

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

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