Admiral/ADM Advisory

Monday, August 10, 2020

Cyber Threats-Phishing Schemes

A Focus on Phishing Schemes and Scams

A recent publication from one of Admiral Security's partners in law enforcement, The National Capital Region Threat Intelligence Consortium (NTIC), has provided relevant intelligence on the continued threat from cyber-related phishing schemes. In this publication, the NTIC lays out some common themes to the issue, as well as the recommended course of action for dealing with the threats.

As Admiral Security reported in its April 22, 2020, Admiral Advisory, these cyber threats have not slowed during the Pandemic but have actually increased using the COVID-19 problems as fodder for more schemes. According to the NTIC, "Phishing is a type of social engineering scheme in which an attacker tries to trick victims into revealing sensitive information such as their account login credentials (usernames and passwords), their banking or credit card information, or personally identifiable information (PII) such as dates of birth and Social Security numbers. The attackers then use this information to gain unauthorized access to email, social media, and financial accounts, steal victims' money and data, conduct financial fraud, or commit identity theft."

There are a variety of different postures that attacks take:

- Phishing is the overarching definiiont for any of the campaigns utilizing email to obtain personal and sensitive information.
- Spear Phishing is an attack geard toward a specific group of people, usually within one organization to obtain information to be exploited.
- Whaling is defined by the targeting of high level members of an organization, such as CEOs, politicians or celebrities.
- Smishing is the utilization of text messages or SMS to target the cell phone users.
- Vishing is when the attackers use phone calls or voicemails to target an individual user, by pretending to be from a government agency or other legitimate organization.

While phishing has become more advanced, with a multitude of tactics being used, the trend continues because the schemes are successful. Bad actors will "spoof" a domain of a legitimate organization to trick an individual into thinking the email is legitimate. Or some emails are from compromised IT systems of real organizations; more tactics are the use of official company or agency logos in the email signature and may even address targets by name. The table to the right shows some ways to identify a phishing attack and avoid becoming a victim.

Six Ways to Identify a Phishing Email:

1. **The email creates a sense of urgency or tries to cause an emotional response.**

Emails that uses words or phrases designed to grab your attention and encourage you to act quickly should be a tip to a scam. Take time to read the email and weigh its real importance. Ask yourself what is the urgency of the request?

2. **The email contains some type of threat if the recipient does not act on the request.**

Similar to above, if the email in question threatens you with some type of negative consequence, usually monetary, it is likely a phishing email and you should not act on it.

3. **The email asks you to provide or confirm personal or sensitive information.**

Any email that asks you to provide any personal or sensitive information such as a date of birth, Social Security number, financial account information, or a password, either by responding to an email or clicking on a link contained in that email, should be regarded as a phishing email and reported to your IT department.

4. **The email contains a lot of misspellings or grammatical errors.**

Look for careless or improper use of language. Check the salutation and signature block for words that are not commonly used by a sender.

5. **The wording in the email is vague or unclear but includes a link or attachment.**

5. **The email asks you to change an established process or procedure.**

This tip is especially important for employees who are responsible for maintaining an organization's finances.

If you are still unsure about any of these scenarios, ask someone from your IT department for help to determine if the email is legitimate before responding to it, clicking on any links, or opening any attachments. Even with legitimate requests, never provide sensitive information over unencrypted, unsecure email or text messages. Also, you should never provide your password to anyone, regardless of the reason provided.

Think Before You Click.