corsica technologies

9 SIGNS OF A PHISHING ATTACKS

Familiarize your company with these common signs to reduce your risk.

1) A GENERIC GREETING

Because phishing emails are sent out en masse, they often use generic greetings with no personalization, like "Dear Member." Sometimes your email address is the greeting or there is no greeting at all. These are all red flags, particularly if the supposed sender's standard greeting is different.

2) A DECEPTIVE EMAIL ADDRESS

You should always carefully review the sender's email address, because a phishing email address can be off by even just one letter. For example an email may be from "promotions@amazan.com" in an attempt to fool you into thinking it's a legitimate message from Amazon.com. Remember too that your brain will fill in missing letters for you - something these hackers count on.

3) REQUEST TO UPDATE OF VERIFY ACCOUNT

Hackers will often generate emails that prompt you to verify your account information, spoofing them as if they are coming from well-known, popular vendors or financial institutions. When you click the link, it goes to a fake login page that is actually stealing your credentials. If you receive one of these and are concerned about your account status, contact the service provider directly by phone or by typing the known URL into a fresh browser window.

4) SENSE OF URGENCY

The goal of a phishing attack is to trick the recipient into clicking on a bad link or attachment. Using social engineering tactics, hackers create messages that are designed to illicit an emotional, immediate response based on fear or excitement. This urgency is a major red flag.

5) DECEPTIVE URLS

The linked text in an email doesn't have to represent the true destination. To check a link without clicking on it, hover over the text and the actual destination URL will appear. In phishing emails, that still may be a URL that is close to what you would expect to see from that sender. Be on the lookout for even the slightest variation to the URL such as an extra dot or a missing letter.

6) AN ATTACHMENT

In the age of phishing, ALL attachments should be approached with caution. If you were not expecting an email with an attachment, or it is not the normal protocol for that sender, verify it directly with the sender before opening.

7) PRIZE OR AWARD NOTIFICATION

If it sounds too good to be true, it is. Don't let an emotional response to this type of claim cloud your judgment. Avoid clicking on links to claim a prize. If you want to confirm it, contact the supposed source directly through a clean browser window or by phone. This includes messages about refunds or credits that you weren't expecting.

8) MISSPELLINGS OR GRAMMATICAL ERRORS

Many phishing emails come from cybercriminals in foreign nations, and the result is misspellings or grammar or syntax errors. If the language in any email seems awkward or just not in keeping with the normal tone for that apparent sender, treat it with caution.

9) ANY MESSAGING THAT SEEMS ODD

With so many phishing variants in existence, the best way to defend against them is to remain vigilant and exercise extreme caution. If anything about an email or text seems "off" or abnormal, avoid clicking on any links or attachments. Instead verify the information with the supposed sender first.

REMEMBER TO ALWAYS THINK BEFORE YOU CLICK.