8 WAYS TO IDENTIFY PHISHING ATTEMPTS

BRAXTON-GRANT TECHNOLOGIES

REQUESTS FOR SENSITIVE INFORMATION

A legitimate organization will never ask you enter any information that is sensitive by following a link. Usually, you will be asked to go to the official website or app to enter your credentials and any other information that is required.

GENERIC SALUTATIONS

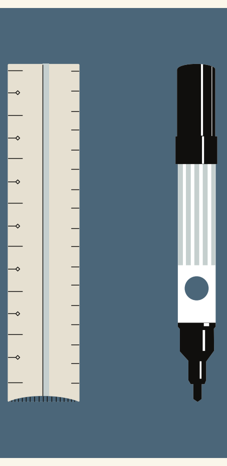
Most hackers will greet you with a "Dear Valued Customer..." or "Dear Account Holder...". Sometimes, ads will not even include a greeting. A genuine organization will use your name.

CHECK THE DOMAIN

Don't check the name of the sender. Check the email address attached by hovering over the "from" address. If you see any changes from what you were expecting, like numbers or letters added, this might be a phishing attempt.

BAD GRAMMAR

Legitimate organizations will send emails that are professionally written, with no spelling errors or bad syntax. Hackers believe their prey is less observant and easier to target, so they tend to have grammatical mistakes.



FORCING YOU ON TO A SITE

If in doubt, don't open the email. Many times, emails can be coded entirely as a hyperlink so any accidental click in the email can lead you to a malicious site or start a spam download on your computer.

UNSOLICITED ATTACHEMENTS

Authentic organizations will seldom send you attachments. They will usually direct you to their website to download what you need from there. It's not foolproof because there are times when they will send you information that you need download, but this isn't common.

HYPERLINKS

Always hover over any links in the email. When you hover over the link, it will show you the actual URL it will direct you to.

SENSE OF URGENCY

One of a hacker's favorite methods to hook a victim is asking them to act fast, either by offering a one-time deal or stating that your account has been compromised. It is usually best to ignore these communications.

WWW.BRAXTONGRANT.COM II 443-545-2052 II SALES@BRAXTONGRANT.COM