ARE YOU BEING PHISHED?

How to know if your business is a victim of social engineering

At first everything looks safe.

As the FTC¹ explains, “Phishing emails...may look like they’re from a company you know or trust.” You’re more likely to follow instructions from “Equifax” than you are from a random organization.

But you are a bit surprised to get the email.

If the email is a surprise, beware! There’s a reason you weren’t anticipating an email from your boss while he’s on vacation.

TIP! **Double-check the sender’s email address.**
Remember that this can be misspelled to mimic a legitimate address and that the “from” field can be spoofed.

You read the email. There’s a negative situation.

Many times, scammers create negative situations to trick you. Your CEO needs your help, but is in a meeting and can’t talk. Or a vendor claims your company owes a payment.

TIP! **A phishing email can lure in you with a faked refund or security alert.**
No matter the bait, the goal is to steal your login credentials.

Your information/money is needed to solve the problem.

After setting up a negative situation, the phishing email will present the solution: sharing your information or resources. This might involve logging in your “account” or sending a wire transfer.

TIP! **If the email comes from an organization, log in to your online account and check your message center to verify the email.**

There is a deceptive link.

If an email directs you to click a link, hover over it before clicking through. If the link doesn’t look reputable or contains errors, beware!

TIP! **Your computer should display a URL when you hover over a link.**
Better still, visit the website of the organization directly.

There are grammar mistakes.

Don’t give your “sender” the benefit of the doubt. Missing punctuation, subject-verb disagreements, or other grammatical issues should raise your suspicions.

There are spelling mistakes.

Misspelled words often spell P-H-I-S-H-I-N-G. If your name is spelled wrong or if there is another spelling error, suspect a malicious email!

There’s an .EXE attachment.

If the email has an .EXE file, beware of malware (i.e., malicious software). However, other file extensions--including .DOC extensions--can be dangerous, too. If you’re in doubt, call the person or organization who supposedly sent the attachment to confirm it’s a safe file.

TIP! **Making a phone call can prevent cybercrime.**
If an email demands money, simply call the person who emailed you to confirm whether the message is legitimate.

Cybersecurity is important because phishing scams happen daily.

Contact Proactive IT for a free cybersecurity evaluation.

704-464-3075

Proactive IT
weareproactive.com