CORPEX

IT SERVICES

IT Security – Phishing Best Practices

Attackers are very smart and know how to trick you. They get to know how they can adjust legitimate website names so you think they are real. Take this one for example:
www.Ameracainepxerss.com
If you are not careful, you would think this is for American Express. But notice the miss-spelling?

It is critical to ensure the URL's are spelled correctly. Safe websites should include http**S**://www.name.com or https://www.name.ca. Misspellings, design flaws, urgent offers, pop-ups, and spoofing are all sure signs something could be wrong.

People setup fake sites to lure you into providing your personal information. They can clone a legitimate site to make their fake site or emails look real. Once they get you on their site, they will lead you into a process to keep you entering personal information or launch malicious software on your device.

Phishing involves asking you click on anything that could temp you such as:

- Complete the survey so you don't miss out.
- Open the attachment to read the details.
- Verify an activity like a shipment delivery.
- Verify or update password information.
- Accept a special offer.

But watch out. It can be a total scam. Only open sites once you have checked the following features:

- Are you expecting the email and is it usual to get this email or text from this sender?
- Ensure the attachment is not an executable.
- Is the email from a real person and someone you recognize?
- Saying URGENT is a sign. Do they ask you to act right away?
- Hover over any offer to click to see if the domain name of the offer matches the sender.
- Is the signature from a generic sender?
- Known file types (eg. Adobe PDF's; zip, docx and xlsx files) can contain viruses or scripts that run when you open it, so be careful what attachments you open from senders.

Keep yourself safe by using caution. Think twice before you click or offer your personal information to anyone.