DIGITAL FIRE.CA
MANAGED TECHNOLOGY

HOW TO AVOID "PHISHING SCAMS"

What is a "Phishing Scam?"

Phishing scams are usually presented in the form of spam emails or pop-ups in web browsers and they are often difficult to detect. The purpose of phishing is to collect sensitive information with the intention of using that information to gain access to otherwise protected data, networks, etc.

Various Phishing Techniques

- Embedding a link in an email that directs you to an unsecure website that requests sensitive information.
- Installing a Trojan vial a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain company information over the phone by impersonating a known company vendor.

How to avoid "Phishing Scams"

- Do not click on links, download files or open attachments in emails from unknown senders. It is best to only open attachments when you are expecting them, even if you know the sender.
- Never email personal or financial information. You never know who may gain access to your email account.
- Never enter personal or company information into a pop-up screen
- Check your online accounts and bank statements regularly
- Always treat your email password like the "keys to the kingdom," because that is what it is to spammers/hackers.
- Don't make passwords anything personal. If the spammer/hacker has your name, it is easy to find out those details from social media.
- If you know the sender of an email, be hesitant. If you don't know the sender, delete the email or check it with your IT department.

How to detect "Phishing Scams"

- Spelling and bad grammar
- Links in an email

  Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below it shows that the real web address is not the same as the one that was typed.

- Threats – Cybercriminals often use threats that your security has been compromised. They use this as a tactic to scare you into opening your email to "protect" your account from further breaching.
- Spoofing popular websites or companies – Scam artist will use graphics or wording that appear to be associated with well-known legitimate websites, but will take you to phony scam sites or look-a-like pop-up windows.