RECOGNIZING PHISHING EMAILS

What is a phishing scam? **Phishing is an effort to obtain confidential information by disguising as a trustworthy source and is typically used in emails.** Phishing scams are becoming alarmingly more prevalent in modern society and are happening in the North Country. Protecting your network with multiple barriers is imperative.

What to look out for

1. **Does it ask for personal information?**
   a. If you are asked to enter your credentials (username and password), take a moment and ask yourself the following question: Does this individual, or company usually request my personal data? If the answer is no, then the email should not be trusted.

2. **Does the email have a suspicious attachment?**
   a. Were you expecting this attachment? Don't be click-happy! Keep a close eye on URL's as they can contain a malicious virus or malware and can be installed once clicked infecting your computer. It doesn't hurt to be too cautious.

3. **Does the email address look authentic?**
   a. It is important to check the email address that it was sent from. If the email address contains a long string of characters, then it more than likely is not legit. On the other hand, it may appear to be from a specific company but upon closer look, it raises some suspicion. For example, you may receive an email with a domain with @mail.dell.biz but should really appear as @dell.com.

   b. Be aware of the actual content in the email. Are there a lot of grammatical errors and misspellings? Emails from a legitimate source pay close attention to language and professionalism. If the email is sent from an allegedly authentic company, but it has numerous mistakes and odd jargon or structure, it is more than likely a phishing email.

Other things you can do

1. **Create strong passwords:** Passwords should contain at least 8 characters, have an uppercase and lowercase letter as well as a number and symbol.

2. **Set up 2-factor authentication:** After your password is entered, 2-factor authentication prompts you to enter a code that is sent to your cell phone.

3. **Have a good backup in place:** Can your business recover from a ransomware attack where your data is held hostage? Having a reliable backup will significantly reduce down-time and could save your business.

4. **Upgrade your router:** It may be time to consider upgrading your router to a commercial-grade firewall with enhanced security. This can allow you to enable content filtering and lock-down your computer network to prevent malicious incoming traffic from coming in.

Bottom Line: Be vigilant. It doesn't hurt to be too cautious. Get into the habit of analyzing your emails and the content in them.

Cybercriminals are getting more sophisticated in their attacks. If there is a link, don't click on it! If you're asked to verify your password, don't enter it!

If you know the individual or company that sent you an unusual email and you're not sure if it is trustworthy, call them and verify it's them. Or you can contact us at support@icllc.co to validate the authenticity of the email.

illuminating**concepts**

support@icllc.co | icllc.co | 518-418-5103