SMALL BUSINESS
BIG THREAT

Cybersecurity Covid-19 Cyberscam Tip Sheet

Phishing Emails

Cybersecurity researches have reported an increase in phishing emails for both Covid-19 and business process related emails. These emails will likely ask you to click a link or download an attachment and may even appear to come from trusted sources, including local medical organizations, your employer, health insurance companies, and local, state, and federal governments.

Covid-19 phishing emails will typically say “Covid-19” or “Coronavirus” in the subject line. They may proclaim a vaccine, a cure, or other important updates.

Business process emails may look more normal and appear to come from a coworker or your organization.
Here are some questions to ask yourself:

- Do you know the sender?
- Are they urging you to open an attachment or to click the link?
- Did the email come after standard business hours?

Vishing Phone Calls

With the rise of Covid-19 phishing emails, it is also expected to get an increase of vishing phone calls. These are scam phone calls that use really similar methods as phishing emails. The calls typically apply pressure and urgency. The caller may ask you for your name, address, and Social Security number to confirm who you are or they may ask for your credit card or debit card numbers for payment.

Here are tips if you receive a vishing call:

- Ask the caller for their full name, the organization they represent, and the purpose of the call.
- Inform the caller that you will call the organization back to inquire about the call.
- Search for the legitimate organization online or in a phonebook and place a call to them.

Fake Websites

Cyber criminals are making websites imitating legitimate organizations. These fake websites can look identical to the legitimate ones. You may see these if you clicked on a link in a phishing email. Typically, these phishing emails will ask you to click the link and login to your account.

Here are tips about fake websites:

- Always check and verify the URL in the address bar of your web browser
- Check for the use of numbers for letters or letters for numbers, for example a capital “I” (eye) looks like a lower case “l” (EL) or maybe they used a Zero instead of an “O” (OH).
- Instead of clicking a link, especially from an email, type in the URL of the website you normally use and login that way.

Small Business, Big Threat is a program of the Michigan SBDC, developed with support from the Michigan Economic Development Corporation and the U.S. Small Business Administration.