CORONAVIRUS CYBERSECURITY CHECKLIST

COVID-19 presents a prosperous opportunity for Cybercriminals. Phishing emails, calls and texts are a few of the tools being used to take advantage of the coronavirus and people's fears.

To protect yourself and your employer, please don't be fooled. We encourage everyone to perform due diligence above and beyond to minimize cybercrime opportunities.

Here is a checklist of guidelines to keep in mind as you maneuver through this difficult time.

_____ **Do not share information that is personal, about employees or other internal details via unsolicited phone calls, visits, email or text messages.** Details being requested range from network structure, passwords, login ids, social security numbers, or network via unsolicited phone calls, visits, email, or text messages. If an individual claims to be from a legitimate organization, verify his or her identity directly with the company. (Do not use contact information provided via the caller, visitor, email or text to verify.)

_____ **Pay attention to a website's URL**. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g. .com versus .net). (For example, www.bssi.biz is a valid website URL. www.BSS1.biz is not. www.bssi.com is not.)

_____ **Hang up on robocalls.** Don't press any numbers. That may cause the robocall volume to increase.

_____ **Do not click on links in emails and texts or open attachments.** These techniques are used to lure you into sharing valuable personal information — like account numbers, Social Security numbers, or your login IDs and passwords. This information is used to steal money, steal identifies, gain access to the company network and spread ransomware. Often times familiar company names are used or the scammer is pretending to be someone you know.

_____ **Do not click on links or open attachments even from people you know.** Many viruses can "spoof" the return address, making it look like the message came from someone else. Check with the person (ISP, Software Vendor, etc.) who supposedly sent the message.

_____ **Do not send sensitive information over the internet before checking a website's security.** Look for URLs that begin with "https" and a closed padlock icon—a sign your information will be encrypted.

Do not use public WiFi, secured or otherwise, to access work accounts unless using a VPN. Connect to a secure network and use a company-issued Virtual Private Network to access any work accounts. Home routers should be updated to the most current software and secured with a lengthy, unique passphrase.

Be alert to "investment opportunities." The Securities and Exchange Commission (SEC) is warning people about online promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus and that the stock of these companies will dramatically increase in value as a result.

Do not perpetuate misinformation and rumors. Before you share information, confirm the facts.
https://www.usa.gov/coronavirus
https://cdc.gov
https://coronavirus.ohio.gov

Look up or report COVID-19 scams. The Better Business Bureau has developed a scam tracker that you can use to search reported scams. Enter "covid-19" into the keywords section to see if you are encountering a known scam. However, just because your situation does not appear in the results does not mean it is not a scam. If you are still suspicious, report it to the BBB and they will investigate. Your diligence could help others. You can access the tracker at https://www.bbb.org/scamtracker/.

Trust your instincts. It is human nature to be curious, trusting and helpful. We need to resist those temptations. Attackers use those characteristics to trick us. If something about the email or the attachment makes you uncomfortable, there may be a good reason.

If you have any questions, please feel free to contact us at 740.475.1700.