Cyber Security:
Avoid These COVID-19 Scams

During this outbreak, employees are working from home and conducting more business over email and video conferencing. Be aware that cybercriminals are using the coronavirus outbreak to deploy dangerous malware including ransomware on your organization.

Share the following information with your colleagues and your customers to reduce their chances of being victimized.

One of the biggest threats are coronavirus-related phishing emails which entice you to click on malicious links or attachments. Don't be fooled!

- **Any coronavirus-related email with an attachment or link should be treated as highly suspicious and verified using known contact information before responding.**
- Never give out **company credentials** in response to a coronavirus-related email.
- Watch for coronavirus-related scams purportedly from the Centers for Disease
- Control and Prevention (CDC) or experts promoting the latest information. The emails may look authentic and include logos or branding for the **World Health Organization** or other government or public health agencies. Don't trust them!
- Common scams relate to **potential vaccines, other cures, prepaid tests, local infection maps**, etc. Be extremely skeptical of any email related to these subjects.
- Treat any email related to potential government checks as suspicious. Scams include those asking for your Social Security number, bank information and a form of pre-payment or fees to collect the check.
- If you are donating money, research the charity thoroughly.
- Scams are by email, phone call, or text.

Don't visit untrusted websites related to COVID-19. There has been a significant rise in website registrations related to COVID-19 that are being used to either steal information from visitors or infect them with malware. Use only trusted sources for authoritative information on COVID-19 such as www.cdc.gov and www.coronavirus.gov

Tips to Detect a COVID-19 Scam

- **Don't trust any request for personal information.** If the coronavirus-related email asks for personal information like your Social Security number or login information, it's a phishing scam.

- **Check all email addresses.** Don't just look at the name associated with the email. Look at the actual email address. Using the below phishing email as an example, the name on the email is Doctor Anthony Fauci. But the actual email address is "no-reply@collaborative--login.com." Because these don't match, this should be treated as suspicious and confirmed before proceeding.

- **Check all links before clicking.** Inspect a link by hovering your mouse cursor over the email link to see what URL the link points to.

- **Analyze the tone.** Does it create urgency or fear? If so, then it's likely a scam.

- **Bottom line.** Treat all coronavirus related emails as suspicious until verified by IT.

Working from Home

- Use extra-long passwords and two-factor authentication for remote access to your organization.

- Protect all mobile devices with passwords/biometrics and never leave them unattended.

- Diligently follow all company rules related to remote working and re-read all relevant company policies on working remotely.

- Never use public WiFi to transact sensitive business unless through a Virtual Private Network (VPN) or other secure means.

- Securely dispose of all sensitive information (including shredding any paper copies) in accordance with company rules.