Shumaker

MARCH 20, 2020 | PUBLICATION

Client Alert: Beware of COVID-19 Cybersecurity Scams

Download Client Alert: Beware of COVID-19 Cybersecurity Scams

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Breach Response Team

RELATED ATTORNEYS

Jarrod J. Malone
Douglas A. Cherry
Andrew J. Mayts, Jr.

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Opportunistic cybercriminals are taking advantage of the COVID-19 pandemic to dramatically increase cyberattacks. Malware and phishing campaigns are especially prolific, where hackers are sending out emails disguised as helpful advice from employers and official organizations, such as the U.S. Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO). Counterfeit emails about health advice are prolific and designed to steal login credentials and other personal financial information.

Network security is more important than ever with so many businesses encouraging their employees to work remotely. We encourage individuals to remain vigilant and take the following precautions:

- Avoid clicking on links in unsolicited emails (even those that look official). For instance, if you receive an email that appears to be from the CDC, rather than click the link, simply go to the CDC's official website directly through your web browser.
- Don't open suspicious email attachments.
- Be suspicious of unsolicited phone calls or emails seeking information about employees or other internal information. For instance, if you receive a call from a credit card company reporting that your account has been compromised, don't provide any requested information. Instead, hang up and call back the official phone number located on your credit card to verify.
- Do not reveal your personal or financial information in an email.
- Don't send sensitive information over the Internet before checking a website's security.

What you should do if you think you're a victim:

- If you think you may have revealed sensitive information about your organization, report it to the appropriate personnel quickly.
- If you believe your financial accounts have been compromised, contact your financial institution immediately to verify and determine next steps.
- Immediately change any passwords that you might have revealed.
- Be vigilant for other signs of identity theft like unusual charges, communications related to accounts or services that you do not recognize, or strange accounts appearing on your credit report. Check credit

reports and online statements periodically.

- Consider reporting the attack to the police and file a report with the Federal Trade Commission.
- Consult qualified legal counsel when in doubt.

Shumaker