STRADLEY RONON

Client Alert

A Publication of the Stradley Ronon
Cyber & Privacy Practice Group

WWW.STRADLEY.COM

MARCH 18, 2020

Stradley Ronon Stevens & Young, LLP
2005 Market Street
Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
New York
New Jersey
Illinois
Delaware

Please click here to visit our COVID-19 RESOURCE CENTER

Cybercriminals Increase Attacks Amid COVID-19: Here's What You Can Do to Strengthen

With COVID-19 and a resulting increase of employees remotely working outside of normal office IT infrastructures, cybercriminals have increased their attacks. Numerous reports have already been made of cybercriminals across the globe leveraging COVID-19 to attack systems, steal money, encrypt or steal personal and confidential data, or wreak other havoc.

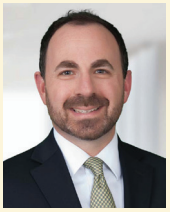
However, businesses and their remote workforces may act right now to strengthen resistance against these attacks, with the following tips:

- For remote users, only access the internet through trusted, secure, password-protected home Wi-Fi or hotspots.
- Avoid the use of public Wi-Fi and Bluetooth. Hackers may easily use these networks to connect to your device.
- If you must use public Wi-Fi, connect only through a VPN or a similar solution. Be sure you recognize the network you are entering into as your business's network. Hackers will try to mimic secure networks, so evaluate closely to ensure that you are joining your legitimate network.
- Stay alert and on the look-out for phishing emails disguised as security updates or as updated company policies. Any non-employer emails should include a reflexive "THINK BEFORE YOU CLICK" mentality, and an actual pause and evaluation, e.g., review senders' email addresses to confirm they are from your actual business contacts and not an imposter.
- Be extremely wary of any request for your personal and/or confidential information, such as login and password credentials. Report these requests to your IT team before responding.
- Keep work-related communications and documents within your trusted business network. Avoid downloading or saving work-related materials to personal devices, thumb drives, personal webmail, or unsecure file-hosting sites in the cloud.
- Carefully verify and confirm any change in payment instructions or verification protocols. Be wary of other requests to send payment, purchase check cards, or follow non-routine payment or transactional instructions. Collaborate with your IT team and accounting department to evaluate all such requests.

- Report lost or stolen devices immediately to your IT team.

COVID-19 requires us all to be hyper-vigilant and practice safety in our routine life. Our online life is no exception. Cybercriminals count on pressure, fear and urgency to succeed. Do not rush. Always take the time to think and evaluate. If you believe you have encountered a cyber threat, contact your IT team for further evaluation, and practice these tips to increase resistance to cyberattacks.

Be proactive. Have open lines of communication. Above all, be safe.



Jeffrey D. Grossman

Sara P. Crovitz

For more information, contact Jeffrey D. Grossman at 215.564.8061 or jgrossman@stradley.com or Sara P. Crovitz at 202.507.6414 or scrovitz@stradley.com.