Cybersecurity and Data Privacy

TOP CORONAVIRUS CYBER SCAMS TO WATCH FOR NOW

Now more than ever it is crucial to be aware of potential cyber threats. Cyber criminals are taking advantage of the current pandemic to propagate numerous types of cyberattacks. Following are some of the scams that are making their rounds – very quickly. In all instances, if you are ever in doubt about the validity of a communication, err on the side of caution.

Public Health Scams: Hackers are sending messages that claim to be from the Centers for Disease Control (CDC), World Health Organization (WHO) and other public health offices. The scam comes in the form of a phishing email aimed at stealing confidential information or installing malware.

- *Do not download or click on any links in suspicious emails.*

Government Check Scams: As part of the recently announced stimulus package, it is expected that the U.S. Government will be sending money to qualifying households, either via direct deposit or physical check. However, threat actors are calling and emailing people, and asking for personal information or money up front in order to process the alleged government payment.

- *The government does not ask you to pay anything to get this assistance (no fees, charges, interest, etc.).*
- *The government does not call you asking for personal information, such as social security number, bank account or credit card number.*

Business Email Scams: Although not a new threat, the economic upheaval caused by the pandemic crisis has created an increase in legitimate and not-so-legitimate financial communications. Hackers know that an urgent request for payment or change in wire instructions today may not raise eyebrows like before. Also, teleworking employees are unable to verify a questionable directive as quickly.

- *Educate employees again about these types of scams and designate a central in-house contact where they can verify requests.*

IT Scams: Instead of coming from a CEO, the suspicious call allegedly comes from a member of the IT department, asking for a user name and password or requesting that certain software be downloaded while working remotely.

- *Again, warn employees about this type of scam and designate a central in-house contact where they can verify all technology requests and directives.*

Supply Chains: The COVID-19 crisis is creating a high demand for supplies. Scammers have created websites that mimic the look of online retailers. These websites are not legitimate.

- *To be safe, type in the URLs (web addresses) that you believe are genuine. If the supplier is unfamiliar to you, confirm its legitimacy with industry colleagues before placing an order.*

Roboscams: Remote workers more than likely are receiving a high volume of robocalls while working from home. Some of these calls are pitching COVID-19 test kits, cleaning supplies, medicine, ventilators and masks.

- *Warn employees about these coronavirus-themed sales calls and instruct them to hang up.*
- *According to the FTC, one recording targets small businesses that may be affected by the coronavirus, warning them to "ensure your Google listing is correctly displaying. Otherwise, customers may not find you online during this time."*

Data Scams: With an increase in the number of remote workers comes increased security risk. Hackers are hoping that at-home workers and companies are lowering their online defenses, making it easier to attack and steal personal information.

- *Follow your employer's security practices while at home.*
- *Educate all work-at-home personnel to protect devices and personal information with basic cybersecurity practices, including keeping software up to date and systems patched, and using strong passwords and multi-factor authentication.*
- *Secure the home network by starting with turning on the router's encryption.*
- *Never leave your laptop unattended and make sure it is password-protected and not shared by family members.*
- *Securely store sensitive data; any sensitive data should be shredded before discarding it.*
- *Do not use public Wi-Fi without proper protection.*

For more information, please contact:
Karen Painter Randall
Chair, Cybersecurity and Data Privacy Group
krandall@connellfoley.com
973.840.2423

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938