Coronavirus: Cyber hygiene practices

During a crisis, bad actors often seek to take advantage by exploiting an already stressful and demanding situation. Leaders and those responsible for risk management are encouraged to proactively and regularly consider and address other potential hazards that could arise and further complicate response and recovery efforts to the initial crisis.

While the world is responding to the coronavirus disease 2019 (COVID-19), and individuals are increasingly focused on personal hygiene and social distancing, augmenting cyber hygiene efforts at home and at work are increasing in importance too. Social distancing is not possible when it comes to technology . . . we are connected and, indeed, inextricably intertwined through email, the internet, social media and the like.

A surge in cybercriminal activity is expected to occur, taking advantage of the global COVID-19 threat. Cybercriminals are seeking to leverage the threat through, among other tactics, “clickbait” aiming to spread malware and steal valuable commercial and personal information. Some suspicious emails contain links purporting to provide urgent updates about COVID-19, government-issued statements, or the ability to purchase items that are in short supply (*e.g.*, hand sanitizers, personal protective equipment).

Certain cybercriminals are openly taking advantage of the situation. The Maze cyber-extortionist group issued a “press release” on March 18 advising that they “decided to help commercial organizations . . . [by] starting exclusive discounts season [sic] for everyone who have [sic] faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get discounts our partners should contact us using the chat or our news resource. In case of agreement all the info will be deleted and decryptions will be provided.”

Companies are encouraged to frequently remind their employees about the basics of cyber hygiene, which often include:

- Reporting suspicious emails to the IT or other appropriate department, and checking emails to make sure that the sender’s email really is a proper company email address.
- For emails sent to a personal account, examining the full email header and paying close attention to the language in the body of the email to ascertain whether it could be a phishing attempt.
- Not sharing personal or financial information via email unless it is sent to a verified recipient through secure email.

- Being aware of social engineering (*e.g.*, a phone call or email from someone purporting to represent the government or technical support).
- Backing up your data.
- Using strong passwords and changing them frequently.
- Using trusted sources for information.

Cyber distancing is impossible; as such, hyper-vigilance at work and at home remain necessary to respond to and recover from cybercriminal activity.

Please contact your DLA Piper relationship partner with any questions or for more information.

By: Scott Weber & Edward J. McAndrew

Article originally appeared here.