March 16, 2020

Coronavirus Privacy & Cybersecurity Health Precautions

Related Practices

COVID-19 Resource Center
Privacy & Cybersecurity

As the world adjusts to the new precautions required in order to stem the spread of the Coronavirus (COVID-19), companies are encouraging employees to work remotely and face-to-face interactions in nearly all fields are being moved online. This sudden and substantial shift raises enhanced cybersecurity threats for companies as employees access systems with remote connectivity with which they may not be accustomed or are tempted to use home technologies or personal accounts that are less secure. With this increase to the cybersecurity threat surface, companies and individuals should be vigilant in maintaining sound cybersecurity practices and remind their employees of best practices to mitigate cybersecurity risks and adhere to company policy.

Remind Employees of Company Policy

Employees should be reminded of company policy with respect to how to work at home and remotely in a secure manner, including which technologies to use and how to use them. These reminder instructions should be written plainly and be easy for the employees to understand and operationalize. If there are specific employees with access to high-risk company systems (e.g., because of the data those systems contain or the importance of those systems to mission critical business processes) those employees may require even more specific “high-touch” reminders in order to ensure that their use of the high-risk systems from remote locations does not introduce an unacceptable security risk.

Careful What You Click

The cybersecurity blogger Brian Krebs warned last week about cybercriminals disseminating malware through websites using the popular Johns Hopkins interactive live Coronavirus map. According to Krebs, these live interactive maps are being imbedded into links, and when a user clicks on the map, it disseminates malware onto the system. Accordingly, companies and individuals should be especially vigilant in opening attachments even if received from a known source. Similarly, individuals should have a heightened awareness for phishing emails that may be seeking to take advantage of people's need for information or desire to help during a crisis and purport to be from an official of their company or a vendor that request that the individual click on a link or provide the sender some kind of personal or sensitive information.

Maintain Sound Remote Working Practices

Avoid using personal or public WiFi networks, personal or shared devices, and personal email accounts.

Personal and public WiFi networks are more susceptible to hackers who can gain access to these networks because of their lower security measures or lack of passwords to gain access. Moreover, personal or shared devices may lack critical security updates and allow unauthorized individuals to access information that should be protected. Employers should offer employees a Virtual Private Network (VPN) to gain access to a company's system in order to mitigate against some of the risk created by public WiFi networks and personal computers and should require strong passwords to gain access. In addition, employees should be discouraged from using personal email accounts. Not only are such accounts less secure, but a company is less able to manage and monitor communications being made on its behalf if they take place on third party email platforms. If personal emails are used, no sensitive information should be transmitted through those emails and if possible, encrypt attachments relating to non-public company business.

Device Security

With the ability to conduct work in public spaces and on portable devices, companies should take and advise its workforce to take precautions relating to their devices. If possible, companies should issue laptops that are encrypted and can be remotely wiped. Laptops should be equipped with multi-factor authentication to gain access to company systems. With all portable devices, including USBs, smartphones, tablets, and laptops, individuals should be vigilant to ward off against losing or having the device stolen. They should not be left unattended in vehicles or unsupervised in public places. When using devices remotely, individuals should ensure that others cannot view their screen and that devices are locked when not in use.

Despite best efforts, however, cybersecurity issues may arise. Companies should encourage employees to report issues immediately and provide an easy means to do so.

The Michael Best Privacy and Cybersecurity team works regularly with clients to help develop and implement cybersecurity best practices and related policies and easy to follow employee training materials. For more information relating to cybersecurity or privacy issues, contact the Michael Best Privacy and Cybersecurity team.

Related People

Adrienne Ehrhardt
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Elizabeth Rogers
Partner

earogers@michaelbest.com
T 512.640.3164

Ryan Sulkin
Partner
rtsulkin@michaelbest.com
T 312.596.5836