HAND ARENDALL HARRISON SALE

CYBERSECURITY
Alert

10 Tips to Minimize Cyber Threats on Your Business

In this unprecedented time of social distancing, businesses across the globe must rely on their employees working remotely. In this environment with unique business challenges and the focus of everyone's attention on the Coronavirus, the risk of cyber threats is grave as businesses rely more extensively on electronic communications, business transactions, and isolated employees to continue to function during this pandemic. Numerous cyber breaches and scams have proliferated in this environment. The HAHS cybersecurity team cautions all businesses and employees to remain vigilant of these evolving cyber threats. Below are ten tips businesses and employees should consider during this unusual time:

1. **Continue to follow policies and procedures.** To the extent the business has cybersecurity and technological policies and procedures in place, they should not be cast aside simply because of the new work environment. Established steps for safeguarding credentials, logging in to VPN, limitations on email and social media use, changing of password, verification for email messages, standards for use of personal devices, and other similar security protocols should be adapted to current business operations. If the business does not have any policies, procedures, limitations, or guidelines on these and other areas for remote operations, they should be developed and implemented immediately.

2. **Dual-factor authentication and extra layers of verification remain crucial, especially now.** Bolster the security of electronic financial transactions and login credentials with the use of dual-factor authentication. Use layered and redundant levels of verification to confirm EFTs, wire instructions, and payroll details. Urgent requests for immediate action or requests outside of established procedures should be a red flag and investigated thoroughly before any response is made or action taken.

3. **Remain vigilant for phishing emails**. With the wave of COVID-19 updates email traffic, and dependence of email communications for those working remotely, cyber criminals have capitalized on the opportunity to trick unwary email recipients to click on malicious links or attachments to infect the computer with malicious content. Do not trust auto-populated sender names, and hover over the sender to confirm the email address is legitimate. Do not click on links or download attachments in emails that are unexpected or unverified. With the increase in the amount of conference and video calls, extra precautions should be taken to authenticate invitations or connection instructions before clicking a link. Verify emails by speaking to the sender directly on the phone to confirm unexpected or suspicious emails are legitimate.

4. **Be on the lookout for fake websites with COVID-19 related content.** There have been widespread instances of fake domains and websites formed to draw internet traffic and unsuspecting victims, mimicking legitimate websites. For example, a phony website mimicking the Johns Hopkins University's map of confirmed COVID-19 cases was created and infected users with malware. Other fake websites spoofing government, healthcare, and insurance providers have become prevalent.

5. **Investigate what impact the change to business operations has on commercial insurance, in particular, cybersecurity coverage.** As more businesses have employees working remotely, the question should be raised to insurance professionals how coverage may be impacted by the change in business operations. Some coverage issues may involve whether commercial coverage extends to personal devices used by employees working remotely, the impact on cybersecurity coverage by the modified working environment, and what exclusions or limitations may be triggered in this new business environment.

This alert was prepared by Hand Arendall Harrison Sale's Cybersecurity Practice Group. For further information or assistance, please contact Chris Williams or the Cybersecurity Group attorney with whom you normally work.

Christopher S. Williams
Author
cwilliams@handfirm.com
251-694-6233

Practice Group Members:

Roger L. Bates
Joseph L. Cowan
Kelly Thrasher Fox
Christopher M. Gill
C. Dennis Hughes
Robert C. Jackson
Sarah Outlaw McLaughlin
R. Benjamin Reardon
J. Burruss Riis
George M. Walker
Christopher S. Williams

6. **Home devices must be secure.** Ensure passwords, firewalls, virus protection, patches, and other safeguards are current and regularly updated on home routers, computers, and wifi. Many routers and other devices come with default passwords that can be located searching the internet so be sure to change and update all passwords.

7. **Children should not use business devices.** With children out of school, avoid the temptation to allow children to play games and watch videos on business devices. While the peace and quiet of a distracted child may seem like a good idea, that tranquility will be destroyed if a virus or malware infects the device due to the child accessing unsecure websites, popups, links, or videos. The more unnecessary website searches and internet traffic to your business device, the greater risk of picking up malicious content, especially if the child is allowed unfettered access to the device.

8. **Working remotely does not excuse violations of privacy, security, or consumer protection laws.** While this business environment is like nothing we have ever experienced, it does not justify violation of privacy, security, and consumer protection laws. The legislature may enact certain exclusions and limitations to address this current business environment to some extent, but expediency or efficiency cannot replace common sense and information safeguards. Emails with sensitive business or protected information should be encrypted and transmitted in accordance with applicable standards and laws. Individuals' PII, PHI, and financial and confidential information must continue to be safeguarded. Global pandemic or not, liability and regulatory penalties could follow those that cut corners or ignore mandatory requirements.

9. **Avoid public or shared wifi.** Even though people are likely avoiding coffee shops and other public locations with free wifi, some individuals will continue to use public or shared wifi, even for business matters. When at all possible, use company supported VPN and secured sources of internet to conduct business and financial matters.

10. **Remote working does not mean zero communication.** Vigilance and immediate communication with IT professionals are of the utmost importance, especially for unusual activity. Report any phishing emails or other questionable activity to your IT professional so they can verify, notify other users, and/or block the sender if possible.

While the COVID-19 pandemic has interrupted the usual method of business operations, remote working, conference and video calls, and the use of technology will help businesses continue to operate and function. With a little extra attention and caution, employees working remotely can thrive and continue to be productive during this new age of business operations. If our cybersecurity team can provide any assistance in the implementation of policies and procedures, conduct presentations or trainings (remotely) on best practices, or assist in the investigation or response to a cyber breach, please do not hesitate to contact us.