COVID-19 Legal Digest: The COVID-19 Pandemic Leads to New Cyber and Data Breach Threats

Client Advisories

04.14.2020

The COVID-19 (coronavirus) pandemic has led online scammers to launch new, and too often successful, ways to hack into computers and steal people's information and money. The vast increase in people working remotely has compounded the risks of data breaches through technological vulnerabilities and human error. Scammers are focusing on social engineering and any schemes they can come up with that will make people open attachments, download apps, or enter their confidential information.

As experts have reported significant increases in the frequency of cyber attacks of all kinds, now is a good time for businesses and individuals to take stock of their defenses against such unauthorized intrusions, which include:

- Solicitations by fake charities, gofundme campaigns, etc. set up by scammers to try to get people to give them money.
  Offers from products online (toilet paper, hand sanitizer, etc.) that get paid for, but never arrive.
- Phone apps that supposedly track infection and death rates in neighborhoods across the world in real time, but are actually just ways to infest mobile phones with malware.
- Callers purportedly from Medicare of Medicaid, and/or websites offering COVID-19 testing kits, so long as the person pays for shipping.
- Emails from "spoofed" email addresses that look like legitimate company addresses and try to fool workers to send or wire money to an account or provide confidential company information.
- Emails that try to fool workers into clicking on links to malware that infects computers or to trick people into entering their usernames and passwords for their email or computer systems, such as:

- Emails targeting people working from home or college students back from school that purport to be from their work/college and contain a link to a website (work-related website or DropBox, etc.) and prompt the user to log in remotely, then exports the login credentials to the scammer.
- Emails purportedly from the World Health Organization claiming to contain attachments with important health information.
- Emails purportedly from the government and asking for credentials so the person can receive a stimulus check.
- Emails purportedly from local hospitals offering for people to pay up front and schedule a time in the next few days for COVID-19 testing.
- Emails offering COVID-19 testing that include a link that supposedly goes to a map of nearby test centers.
- Emails or advertisements for free streaming services in light of the COVID-19 situation once the user enters personal information.
- Emails disguised as coming from an electronic signature company (DocuSign, etc.) indicating they have a document that requires their signature and encouraging recipients to open link, .xls spreadsheet or a .doc file containing the important document. However, the .doc file is not a document at all-it's malware that immediately infects your computer and could potentially spread to your entire network.

It is of course prudent for everyone-businesses and individuals alike-to take measures to prevent data breaches at all times, but the increased vulnerabilities brought on by the COVID-19 pandemic make it especially important. Not only do you want to stop cyber criminals from stealing your information, getting into your financial accounts or tying up your computers for a ransom, but you have ever-expanding legal obligations to take reasonable measures to protect the privacy of other people's data and information that you possess.

Some laws require certain types of businesses to adopt specific security measures. More generally, per the American Bar Association's *ABA Cybersecurity Handbook*, the emerging legal standard requires all businesses to engage in a process to "assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments."

For those businesses whose cybersecurity practices consist of offhand measures adopted without a strategic evaluation of risks and alternatives, the cyber threats emerging from the COVID-19 crisis should be a motivation to engage in a deliberate assessment process. In addition, those businesses who have already undertaken a formal assessment should take this opportunity to determine if any changes in their approach to cyber security are warranted by the increased threats, or at least to remind their management and workforce of the best practices to minimize their cyber and legal risks.

No matter where a business stands in its cybersecurity program, there are a few, relatively inexpensive things that it can do at this juncture.

- Alert its workforce to the nature of COVID-19-related email scams.
- Implement or reiterate effective company policies concerning passwords; the identity, handling and disposal of confidential information and information security, including hard copy documents and electronically stored information and data; and those policies requiring verification of wire transfer requests.
- Give serious consideration to implementing multi-factor authentication for logins to company network systems.
- Follow the detailed advice available at the following link to the website of the Cybersecurity and Infrastructure Security Agency, which is part of the Department of Homeland Security.

If you have questions or would like more information, please reach out to your Archer contact or Robert Egan, Chair of Archer's Data Privacy and Cybersecurity Practice Group, at 856-354-3079 or regan@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

Subscribe to COVID-19 Advisories

To subscribe to the latest news and updates on COVID-19, click the link above, or copy and paste this address into a new browser: https://archerlaw.wpengine.com/news-resources/client-advisories/covid-19-legal-updates-subscription/

Related People

Robert T. Egan

Of Counsel

regan@archerlaw.com

856.354.3079

Related Services

- Data Privacy & Cybersecurity