Dinsmore

Publications

Tips to Avoid Cyberattacks during the COVID-19 Pandemic

March 25, 2020 | Legal Alerts–

Kurt R. Hunt and Leanthony D. Edwards, Jr.

In this difficult and unprecedented time, it is important to stay informed not only to remain healthy but also to protect yourself against falling victim to cyberattacks.

We are familiar with common cyberattacks such as phishing schemes, ransomware, and the long-running Nigerian lottery email scam. We may even feel comfortable with our ability to spot these threats, and companies have adapted their policies and practices to help defend against them. Unfortunately, cyberattackers devise more elaborate attacks every day and often use specific information or current events to increase the efficacy and spread of an attack.

The Cybersecurity and Infrastructure Security Agency (CISA) has warned bad actors are now using the COVID-19 pandemic to, "send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to

RELATED ATTORNEYS

Kurt R. Hunt

RELATED SERVICES

COVID-19 Business Strategies Hub

COVID-19 Cybersecurity

COVID-19 Intellectual Property

Cybersecurity & Data Privacy

fraudulent charities or causes." A Johns Hopkins COVID-19 data map operating as an interactive dashboard of COVID-19 infections and deaths was used to spread malware.

U.S. Attorney General William Barr warns criminals have used the following scams to profit through the COVID-19 pandemic:

- Individuals and businesses selling fake cures for COVID-19 online and engaging in other forms of fraud;
- Phishing emails from entities posing as the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC);
- Malicious websites and apps appearing to share virus-related information to gain and lock access to your devices until payment is received; and
- Seeking donations fraudulently for illegitimate or non-existent charitable organizations.

Proactive steps to protect yourself and your organization

We recommend taking the following precautions to help prevent falling victim to a COVID-19 related scam;

- Avoid clicking on links and opening attachments in unsolicited emails;
- Stay updated on COVID-19 news and developments by using trusted sources including Dinsmore's COVID-19 Business Strategies Hub, the CDC, and WHO;
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information;
- Verify a charity's authenticity before making donations; and
- Exercise caution in handling any email with a Coronavirus or COVID-19-related topic.

If you have any questions or concerns about cyberattacks and their implications for your business, please contact your Dinsmore attorney.