AIRD BERLIS

SPOTLIGHT
MEDIA, SPORTS AND COMMUNICATIONS LAW BLOG

Mar 26, 2020

Beware of Preying Cyber Criminals During the COVID-19 Pandemic

By Paige Backman

Cyber criminals are parasitic, so the fact that they are using COVID-19 as a backdrop to increase their attacks should not be a surprise. It is, nonetheless, disappointing and irritating. IT teams are stretched to capacity managing en masse remote working conditions and the stability, security and training/help desk issues resulting from this new environment. Increased cyberattacks can stretch IT teams to or beyond their capacity. For the rest of us, we're trying to keep business running, conference calls moving, and maintain service standards while ensuring a germ-free and often a child-managed (educated and happy?) environment.

What are we trying to protect? Cyber criminals will try to get you to send them information and will try to access information about you from your computers. They can use information on your laptop and home computers, including documents, photos and videos to steal your identity and possibly for extortion. Depending on the virus or malware used, once on your computer or laptop at home, it can betray key strokes and passwords to get access to secure information such as banking and work networks. Their access to this depends on your less robust IT security at home as well as your attention being diverted.

We want to provide a few quick tips on what to look for and, hopefully, relatively easy ways to manage those challenges.

Cyber criminals prey on natural human behaviour and emotions such as anxiety, fear and the instinct to want to help. With COVID-19 being front and centre, emails could include offers relating to face masks or hand sanitizer. They can use the business disruption to send misleading communications to change internal business processes, particularly those involving the flow of funds and payment. You may receive emails from the World Health Organization. Of course, you may also get emails asking you to help financially. The email may ask you to take an action such as sending information, clicking on a link or downloading an app.

If you receive an unexpected or unusual email, even from people you are supposed to know (including the IT Department or management), or an email from any third party that you don't know, take a pause. Just a few seconds.

Hover your mouse cursor over the email address to see what the sender's true email address is. Often email addresses are purposely camouflaged to look like a legitimate name, but when you look at the email address itself, it doesn't match what it should be. Does the body of the email address accord with the organization it is supposed to be sent from? Email addresses that purport to be from reputable organizations that end in "gmail.com" should be a warning sign.

Do not open emails, click on links or open attachments unless you are comfortable you know who sent it. If the email is coming from someone you should know, but you think the request is odd or just unusual, simply send a separate email to the person (not replying to the email you received) to confirm the question or request. As well, as we're all finding ways to combat the loneliness that inevitably comes with physical distancing, use the opportunity to pick up the phone and confirm the request or communication. If the email is from an organization asking for help or money and you are potentially interested in what the organization has to say, independently (not through links in the email) and after hours search the organization on your own. If they are reputable, they won't be hard to find. Call or email them through verified phone numbers and email addresses, and not the contact information in the email you received.

We will be following up with more detailed information on this topic. If there's an issue you want us to

address or a question you have on this topic, let us know. We hope you stay safe during these interesting times.

Author

Paige Backman
Partner
T 416.865.7700
pbackman@airdberlis.com