Reinhart

Beware of Email Scammers During the Coronavirus Outbreak

As with any other crisis, the COVID-19 pandemic tends to bring out the best in most people but the worst in others. Scammers are even more active than ever, hoping that changes in our work environments and the enhanced distractions and stresses we now face will make us less diligent and therefore more susceptible to their schemes. As a result, we all need to stay more alert than ever to attempts to access our confidential or financial information.

There are increasing reports of hackers gaining access to a party's email account and then, posing as that party, instructing its financial institution, lawyer or customer to send a transaction or settlement payment to the hacker's account. Anytime you receive bank account or funds transfer information for the first time, or worse, a change to such information, it is imperative that you break the communication chain by speaking to the sender in person or by telephone.

Hackers are also using access to a party's email account to attempt to infiltrate the systems of the party's customers, vendors or other contacts. Their method is to use that person's email to send you an email that appears to legitimately come from your contact's account. The email will ask you to click on a link or invite you to download documents through a provided link.

Because the email comes from a recognized contact's email address, the hacker is banking on you clicking on the link to attempt to open and download the information. Hopefully, your security software will block such attempts as malware. But, your security software may not recognize the threat. So, it is important that you, and your employees, look for clues that will prompt an inquiry before clicking on the provided link.

Ask yourself if this is the type of message your contact normally sends. If not, then do not open the link. Even if the message is similar to a normal communication from that contact, if you were not expecting information from the contact at the time it was sent, do not click on the link. Instead, if you receive an unexpected email asking you to click on a link or to download documents, verify with the purported sender that they have indeed sent you information before attempting to view it.

It is imperative to call your contact at a number you have for that individual in

POSTED:

Mar 25, 2020

RELATED PRACTICES:

Corporate Law
https://www.reinhartlaw.com/practices/corporate-law

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Steven P. Bogart
https://www.reinhartlaw.com/people/steven-bogart

your contact list, *not* at a number provided in the email or by a reply to that email. Using a number provided in the email or responding to the email itself will only connect you to the scammer who will, of course, verify the attachments contained in their message are legitimate.

If you have any questions about how to thwart the efforts of scammers during the coronavirus outbreak, please contact a member of our Data Privacy and Cybersecurity Team, or your Reinhart attorney.