CYBERSECURITY AND DATA PRIVACY

PHISHING LURES: WHAT TO DO IF YOU'VE TAKEN THE BAIT

by Justin L. Root, Sara H. Jodka and Wendy G. Hulton

Sometimes, it's easy to know you're being phished. There's little chance that a bank administrator in a country you've never heard of really needs your help to get the unclaimed money of a deceased, rich foreigner out of the country before the corrupt government steps in to seize it. Other times, though, it's not so easy. Modern scammers don't just phish, they spear phish. The difference is in the amount of research that goes into the scam and how narrowly the attempt is directed.

Imagine this scenario: Your company pays several invoices each month. Many come by email and include the account information to which payment can be directed. So when an invoice shows up from a known vendor for work actually done by that vendor, no red flags go up. After you make the payment, though, either the vendor contacts you and tells you the payment was never received or another invoice arrives for the same service. A little investigation shows that the invoice you paid was from a scammer and that the money is now gone.

How could this happen? There are a couple of ways. Maybe your systems have been compromised, the real invoice was deleted before anyone saw it, and a scam email (from a similar domain name) was sent in its place. Or maybe your vendor's systems have been compromised and what was only a draft invoice was used to create the fake email that was sent to you from the vendor's real email account. Similar scams abound: real estate closing scams attempting to divert funds to scammers at the last minute; internal emails from "management" ordering a wire transfer or requesting employee W-2 information; targeted messages with links to infected sites hoping to install malicious software on the victim's computer system.

Between professional social media platforms, personal social media platforms, and company websites, scammers can learn more than enough about you, your colleagues, and your company to craft a highly sophisticated, uniquely tailored scam to swindle you out of thousands, tens of thousands, or even hundreds of thousands of dollars.

Of course, an ounce of prevention is worth a pound of cure. Utilizing multi-factor authentication options, implementing internal and external verification procedures for large money transfers, training employees to recognize risks, and limiting the information available on social media platforms can go a long way toward avoiding the dangers of phishing attacks. But what can you do if you've fallen victim?

1. If you've transferred funds by wire, time is of the essence. As soon as you realize the money has been improperly sent, you should contact your financial institution and local law enforcement or the Canadian Anti-Fraud Centre and/or the Royal Canadian Mounted Police (RCMP). In some instances, it may be possible to reverse the transfer, although this often is not the case. If transferred money cannot be clawed back, contact your insurance provider. (And if you do not already have an appropriate cybersecurity insurance policy in place, now is the time to get one. It is also important to understand the limitations of that policy and to know what will and will not be covered.) Depending on your policy, the loss may be covered by insurance.

2. If you've transferred money or sent out sensitive information (employee T-4s or other personally identifiable information, trade secrets or intellectual property, or other confidential content), immediately identify the situation as a data security matter and implement your Incident Response Plan by notifying the appropriate people on the Incident Response Team. (If you don't already have an IRP and designated members of an IRT, now is the time to develop both.) You will need to identify your company's legal obligations – including state-level notification laws, law enforcement reporting obligations, regulatory reporting obligations, contractual obligations, etc. – and begin taking steps to satisfy those obligations. The retention of competent legal counsel who can serve in a breach coach capacity is critical for this phase.

3. File a report with law enforcement. Even if law enforcement cannot track where the money or information went, reporting the incident is a good idea. In some jurisdictions, it may be required by law. It may also be the case that the perpetrators are tracked down later, and having the report on file can help substantiate that you are entitled to some of any recovery that might occur. Also, reporting the incident may draw attention to a specific industry or sector that is being targeted by scammers and could help prevent others from falling victim as well. When making this report, however, it is important to be mindful of any regulatory obligations that might be implicated by the incident and to be cautious with information that could be misconstrued in subsequent regulatory investigations. You should determine whether you are subject to reporting obligations to either the Federal or Provincial Privacy Commissioner. Again, competent legal counsel is important at this phase.

4. Investigate how the incident occurred. Were the perpetrators able to gain access to your network to send fraudulent emails? Were they able to glean information from social media accounts or your company website that facilitated the fraud? Did improper employee training or inadequate policies and procedures lead to the incident? This phase may require an in-depth policy review and the retention of a qualified computer forensics company.

5. Finally, fix the problems that allowed the event to occur. This may require changing policies, changing protocols, resetting passwords, utilizing multi-factor authentication options, and implementing ongoing employee training sessions (among other efforts).

Obviously, implementing appropriate procedures in advance can help reduce the likelihood of data security incidents occurring, decrease the

time spent investigating and responding to an incident, reduce the costs associated with a breach response, and help to identify legal rights and obligations more quickly. Proper preparation, although necessitating some up front effort and expenditures, will ultimately result in overall cost, time, and energy savings should a data security incident occur, and allow affected entities to return to normal operations as quickly and efficiently as possible. If you are not sure when you last reviewed and updated your applicable policies, Dickinson Wright's cybersecurity and data privacy attorneys encourage you to do so today.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Cybersecurity and Data Privacy law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Justin L. Root is Of Counsel in Dickinson Wright's Columbus office. He can be reached at 614.591.5465 or jroot@dickinsonwright.com.

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.

Wendy G. Hulton is a Partner in Dickinson Wright's Toronto office. She can be reached at 416.777.4035 or whulton@dickinsonwright.com.