Shumaker

JUNE 11, 2021 | PUBLICATION

Client Alert: The Risk from Phishing

Download Client Alert: The Risk from Phishing

INDUSTRY SECTOR

Health Care
Technology

SERVICE LINE

Data Breach Response Team

RELATED PROFESSIONALS

Grant P. Dearborn

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

We are all well aware of the risks that cyber-crime presents to businesses now. On a weekly basis, we see stories about virus attacks, hacks, and ransomware. But, how do we avoid being the victim?

Of course having appropriate Information Technology (IT) safeguards and the qualified personnel to fortify the castle walls is part of the solution. However, based on information in the industry, security events are also likely to occur because of the errors of staff.

In order to mitigate this risk, we have to make sure that our staff understand some of the pitfalls of being linked to the worldwide web.

First, it has been apparent to many that staff do not realize that a major vector of attack for hackers is to infiltrate and co-op the email of another person. In some cases, we see hackers mock up email addresses, but in phishing we also see hackers take control of a real person's email account. At times, the hacker will remain in the account and use it as a vehicle to phish other accounts or to harvest other information. This means that when someone receives a suspicious email and the receiver emails the email account owner regarding whether the named sender actually sent the suspicious email, the response may come from the hacker. We have even seen a case where the hacker hijacked a wife's account and corresponded with her husband. Luckily for him, he did recognize a problem in the communication.

Moreover, staff has to understand that phishing is a domino effect type stratagem. Phishers probe an email account by sending an email with an attachment to a particular account. It is also a numbers game, as the phisher may send a hundred such emails. The phisher wants the receiving individual to open the attachment, and the receiver finds the attachment will not open without the receiver inputting his/her email account credentials (password, email address, and/or account name). Once the receiver inputs this information, the hacker will then use those credentials to hijack that former receiver's email, will access address books, and send the same or similar attachment to the hijacked account holder's peers. This is the domino effect, and it may be a great way to alienate all of your peers.

We have to know the enemy's purpose. The hacker has one of two purposes. The phishers seek to either harvest email credentials and sell those on the Dark Web, or alternatively, phishers seek to research accounts

for information that can be monetized. This researching of information in email accounts may also include targeting accounts related to finance in an attempt to route fictional invoices. Likewise, phishers may also seek individual specific information, such as social security numbers or credit card numbers, which are often then sold on the Dark Web.

Phishers take control of one email account, and then seek to replicate the process by using that account's address book to continue to replicate the process. The phishers are relying on human nature to cause the receiver to be less on guard due to the familiarity with the sender. This can cause individuals who receive an email attachment, even one out of the ordinary, to not question the request for credentials. The founding principles in the art of phishing is the understanding of human psychology.

Finally, we offer some avenues to help reduce the risk of human error. As a point of emphasis, entities need to conduct area specific training for those who utilize sensitive information. Also, the staff needs to know that generally he/she should not be inputting their email credentials into third-party requests. The organization should train those who may have such a request due to a particular third-party software, and all other staff should be specifically trained to not provide such information with an explanation of the danger. Moreover, we need to not retain sensitive information in our email unless absolutely necessary and even then, only the minimum necessary. Staff need to be reminded that generally, email is a dangerous vector for sensitive information. When possible, use alternatives, such as the last four digits of a social security number instead of the entire social security number. Please remember that a hacker who has control of your email account can search your sent box, inbox, and deleted box for sensitive information. Any search you could perform, the hacker can as well. Additionally, all staff need to be trained that each individual has an obligation to report security events and that a failure to report will be considered a further violation of your policies. IT professionals need to be aware of the need to react quickly to cut off outside access to a phished email account.