Keystone
TECHNOLOGY CONSULTANTS

Cybersecurity Tips and Reminders

This Month's Focus- Your Bank Account has Changed

Recently, a local church was the victim of a wire fraud scheme that resulted in a loss of $1.7 million. Unfortunately, I do not have the technical details of this particular scheme, but I am pretty confident I know what happened. Over the years, I have investigated many of these wire fraud or payment diversion schemes.

Here is how the scheme works:

1) Hackers gain persistent access to a victim's email account. This is typically done through a phishing email asking the victim to log into their email account online. The victim clicks onto the phishing link, they enter their email address and password, then it appears to the victim that nothing happens. They move on with their day and think nothing of it. In many cases, now the hackers can log into the victim's email from anywhere in the world.

Send me more info

Be Suspicious. Something is not Right.

2) The hackers then search the victim's email for any valuable info they can find. They are looking for passwords to other accounts, banking information, patterns of communication with recipients that they could somehow take advantage of. The whole time they are doing this without the victim knowing someone else is looking at all their emails

.

3) Eventually they find a few different aspects of the victim's email history that they can exploit for financial gain. If they find that this victim is involved in an ongoing conversation with a customer or vendor that involves the transfer of funds, they will find a way to exploit this.

4) In the scheme involving the church the hackers likely gained access to the mailbox of the vendor who SHOULD have received payment. The hacker would then create mailbox rules that would hide their correspondence with the people they are trying to get payment from. Using the vendor's actual email account, they tell the payor that their banking information has changed and please send payment to the new account.

5) The payor sends the money to the hacker's bank account. The hacker quickly transfers it to an offshore account that is anonymous because of privacy laws protecting accounts in certain countries. The payor thinks all is well because they paid their bill and the vendor is wondering why they have not been paid yet.

6) Weeks go by and the vendor asks where is their money? By the time anyone realizes they have been

scammed, the money is long gone. The payor and the vendor put the pieces together and eventually the email requesting bank change is found. Depending on the insurance and/or banking safeguards, this money may or may not be recoverable by the victim.

In my experience, this sort of man in the middle attack could be carried out for weeks or months. If the hackers feel they have gained access to someone who will send and/or receive large amounts of money, they will monitor email conversations waiting for the right moment to insert themselves into the conversation and divert the money to their account.

There are several ways to protect yourself and your money from this sort of attack:

1) Implement multi factor authentication for as many of your online accounts as possible.
2) Have unique passwords for your online accounts and change them frequently. Use a password manager like LastPass to help organize these passwords.
3) Implement best of breed spam filtering services and policies.
4) Implement suspicious account activity alerts to take quick action when hackers access your email account.
5) Participate in continual cybersecurity training to help detect phishing emails.
6) If someone emails asking to change their account for payment, look up their phone number in your records (don’t call what is in the email), then call to confirm this request.

Any Questions?

Please respond to this email if you have questions, comments, or desire more information.