Email Hijacking, A License to Hack

By Danny F. Dukes, CPA, CFE, MBA

Some would argue that the advent of email has revolutionized personal and business communication. Who would ever criticize being able to write short or lengthy messages or full letters that are delivered in seconds? Then, when you attach documents or files, both word processing, PDF, and spreadsheets, you can expedite the delivery of vital business and personal data to intended recipients. As a matter of fact, you can include multiple recipients and not only avoid printing/postage/shipping costs, but also avoid multiple costs without any delay in delivery. What could possibly go wrong? As with every convenience for the good of mankind, there are those who strive to do us harm, financially or otherwise. Since the old firewall penetration trick used to access systems is now mostly prevented with monitoring and protection, email has become a computer hacker's best friend, making their efforts to penetrate company computer networks much easier. Unfortunately, email can now be our worse enemy, as it can fall in the hands of unintended recipients, wreaking havoc and costing us extensive loss of productivity and cash.

Numerous attempts to filter SPAM and junk email, which can be a key source of outside computer and network infiltration, have lacked complete reliability, because inevitably legitimate items get filtered to SPAM and junk folders. So then we loosen these filters which allows more rogue email items to make it to our "protected" inbox. Some believe we all can readily identify the rogue, potentially harmful email. At one time, this may have been somewhat the case. However, now email senders who wish to do harm have become more sophisticated, extremely sophisticated. It's not just rogue email with Chase Bank's logo asking you to login to your internet banking, while later you discover that you just gave your user ID and password to a criminal who now has access to your account and money is now missing. Maybe you don't bank with Chase and readily discount that email and others with Amazon, etc. Even if you do give up your bank login and password, banks like Chase have now established multiple ways to authenticate users trying to access financial information, such as sending you a code to your cell phone and/or asking you personal questions for which only you should know before granting access. The bad actors now

want to access your email so that they can read through your correspondence, find out where they can focus on defrauding you or record your login information when you log in to systems. We all get those emails telling us what are user name and passwords are right?

In a recent court case, a CPA firm would wire transfer funds for a client's investment interests to the client's chosen investment sources. The CPA firm would act after receiving a simple client email. They were authorized to initiate wire transfers at the client's bank taking the funds from their bank account(s) and sending it to these third parties. The client clicked on unsuspecting links in email(s) which allowed the unauthorized bad actor to have access to this client's email. The bad actor reviewed email history discovered these emails requesting wire transfers were a standard practice and knew who to email to initiate the wire transfers. They even knew locations that the client discussed with others, including the CPA firm, where the client considered making investments.Taking it one step further, the bad actor hijacked the client's email address so that the CPA firm emails would no longer show up in the client's email in box. Then, this bad actor began to communicate with the CPA firm by sending the CPA emails with instructions requesting wire transfers to other third parties in locations where the client considered investing. After 2-3 unsuccessful attempts to wire funds, the bad actor finally got the recipient account information correct and absconded with over $600,000 of the client's cash. Who is at fault is not at issue here. What's at issue appears to be innocent email was converted to lost cash. This prompted a law suit and an extensive lengthy investigation. Meanwhile, the client is missing $600,000 with no immediate resolution and lost productivity.

The second example of bad acting is when the actor obtains access to a victim's employee's computer from one of these previously described rogue emails and discovers through observation that large sums are being invoiced by a vendor and subsequently paid by this employee. How much trouble would it be to call the company and find out who the accounts payable clerk is and what their email address is? It's not difficult. By knowing their name, penetrating their computer, they can discover the vendor's name, maybe even discovering the names of the vendor's employees through emails, the bad actor calls the victim's accounts payable area, cordially asks for the correct employee(s) by name, informs this (these) employee(s) that the vendor bank information has changed and provides the new bank information. Then, when the authorized vendor invoices the victim, the invoice is processed and the funds go to the bad actor, not the vendor. This happens multiple times and the vendor calls to find out where their funds are and tells the victim that they are past due demanding payment. Again, the bad actor has out maneuvered the system for unauthorized fraudulent benefits.

Recently, I received an email from a Houston law firm that I did not recognize. I interact and do business with law firms from many states. So, at this point, not recognizing the law firm was my only hesitation. The email had a hypertext link that supposedly took me to files for a court case shared on Microsoft One Drive. Usually, I can click on the sender's email address and see that the email domain and even the letters before the domain are not authentic and they do not match the law firm's domain. However, this time the domain on the email was the website for this valid law firm and it was a legitimate email address of an employee that coordinates file sharing for the firm. After calling the firm, the receptionist asked if I was calling about the email and informed me that it was not authentic. The email had been hijacked. The remaining unanswered question is how was my email address chosen since I had never worked with this firm. Usually, the bad actor uses the emails in the individual's address book, which would have interacted with this person before and would have been more likely to click on the link provided, which would have given this crook more access to continue their crime spree. Remember how easy I said it would be to find out the names and email of appropriate company personnel? Well, they

did so in this example and had I clicked and not questioned, who knows what my exposure would have been?

Email is much like a postal mail box and postal address. Anyone can mail to your address and anyone can send you email if they know your email address. Email lists can be bought or email addresses for key employees can be discovered through inquiry. So they are not any more confidential than postal addresses. Think about how much junk mail you get from the US Postal Service. Then, consider all the junk email you receive in your inbox. Now, email that looks legitimate and authentic can do much more damage than the junk postal mail that is quickly tossed in the trash. Clicking links or downloading attachments on email can result in the misallocation of real cash. One simple click or one simple download can be costly. Email recipients should be more diligent in determining the legitimacy of email received just to avoid losses, conflict with vendors and others affected. The potential loss and aggravation has been and can be real and extremely disruptive. However, vendors and third parties relying on email to authenticate monetary transactions should be more cautious and use more reliable methods to likewise avoid these misallocations. Ironically, something as simple as a phone call or further analyzing transaction legitimacy before processing can save thousands of dollars and hours of unnecessary tasks.