Cybersecurity Tips and Reminders

This Month's Focus- Display Name Spoofing

Email is a very common means of communication inside and outside of the organization; it is so routine, we just read and reply quickly. Sadly, it is also a common way attacks occur. The screenshot below is an example of a very well-crafted attack message. The attacker used a common technique called “Display Name Spoofing,” in which they made it look like I came from someone the receiver would trust. Spoofing is defined as a situation in which a person or program successfully masquerades as another by falsifying data.

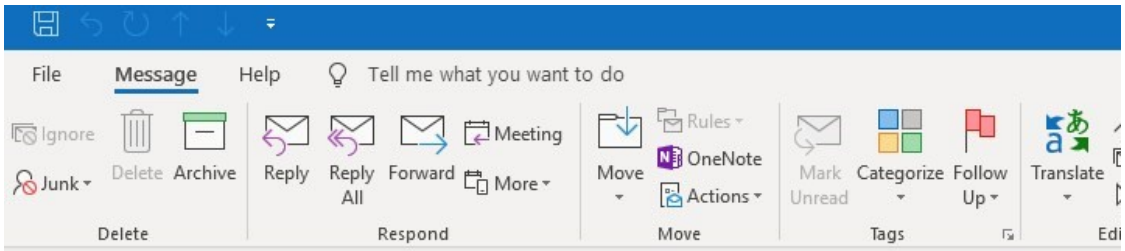
Send me more info

Be Suspicious. Something is not Right.

As you can see highlighted below, this email appears to come from David Howard and the email address displayed is correct. But it isn’t from David. It isn’t difficult to change the Display Name to whatever you like, which is what happened here. Unfortunately, a non-technical administrative employee (We will call her Janine) in our office fell for the scam and opened the attachment. Fortunately, it was immediately blocked by the installed anti-virus product. This raised Janine’s suspicion, so she looked closely at the original email. A few details in this message allowed her to determine it was likely a scam. First, the tone of communication wasn’t a way David typically writes. Second, the email signature did not look like his, and the phone numbers were not phone numbers he uses. Third, the file type is not something they ever used for invoicing. Janine then called me to review this email and make sure her computer was not infected.

I checked and quickly determined the anti-virus prevented the possible infection. When the properties of this message are analyzed, I found this email came from address khamkeo@easia-travel.com, and the country source is China. I opened the attachment file on a testing computer I call “Crash Test Dummy” which does not have anti-virus software installed. When I opened the Word document, it asked me to “Enable Content” which I did. Soon after that, with logging software, I saw a background process connect to a command and control server in Turkey. This downloaded more malicious files. Quickly it encrypted all Microsoft Office files and PDFs on the computer. Crash Test Dummy had just been infected with ransomware.

Lesson to learn here: analyze the totality of the email before you click on an attachment and/or link. If anything looks off to you, call the sender at a phone number you have called them at. Discuss the validity of the email before you click on anything. Better yet, send it to Keystone for review and we will help you determine whether it is safe or not.



Wed 11/14/2018 3:49 PM

David Howard <DavidH@keystonecorp.com>

October Invoice David Howard

To [redacted]

Invoice_No_5164133.doc
.doc File

Good Afternoon all.

Please find attached copy of your latest invoice.

Thanks in anticipation.

-

David Howard
Direct #: 836-032-2447
871-546-3893 x337
e:DavidH@keystonecorp.com

Any Questions?

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