March 2017

Stay Ahead of the Email Scammers

Lookalike and hacked emails are helping fraudsters steal billions. Here's how to fight them.

Larry Zelvin
Director of the Citi Cyber Security Fusion Center (CSFC)

Law enforcement agencies around the world have been investigating a scheme known as a Business Email Compromise (BEC). BEC is a scam that cyber criminals use to steal money from businesses or wealthy individuals using wire-transfer payments. Since 2013, more than $3 billion in fraud losses have been attributed to this type of fraud globally, making it the most lucrative form of cybercrime to date.[i]

So how does a BEC work? In BEC scams, cybercriminals generally use social media sites – and particularly professional networking sites – as a tool to identify employees who have access to banking, financial or sensitive employee data. They then trick the employees into performing wire-transfers by sending them an email request that appears to come from an executive, such as a Chief Executive Officer or Chief Financial Officer. They try to make these emails appear legitimate so the employees perform the fund transfers to criminal accounts before they are identified as fraudulent. In some cases, cybercriminals have even hacked into the real email accounts of executives or other high-ranking businesspersons to send these illegitimate transfer requests.

Despite recent media coverage on this fraud scheme, and a sobering alert from the U.S. Federal Bureau of Investigation (FBI), cyber criminals launching these attacks continue to enjoy successes as many employees are typically not accustomed to saying "no" to requests from senior leaders in their firm. In 2015, cyber thieves stole over $46 million from one company alone using the BEC technique, although law enforcement officials managed to recover approximately $8 million in this case.

What might we do to protect ourselves in the face of this rising tide of BEC scams? The Cyber Security Fusion Center recommends that company leaders talk to their employees about BEC preventative and defensive measures. They advise them to be wary of emails requesting wire-transfer payments and closely scrutinize any orders deemed urgent by the sender. Whenever validity seems questionable, employees should pick up the phone to verify the transfer request. Likewise, they need to look closely for mimicked email addresses and closely review domain names (e.g. john.smith@gmail.com compared to john.smith@gmai.com).

In the case of "urgent" transfer requests, companies are encouraged to consider imposing additional authentication protocols. A further precaution is reducing the number of individuals that have the authority to approve or conduct wire transfers. To restrict the number of "leads" available to BEC scammers, caution should be exercised when posting financial and personnel information to social media and company websites.

If you suspect you have been targeted by a BEC, report the incident immediately to your Citi Client Relationship Manager and local law enforcement to aid in the recovery of funds.

[i] https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams?utm_source=hs_email&utm_medium=email&utm_content=28140297&_hsenc=p2ANqtz--f0buz9nDeHu9YAI5KYbMmCHIthkKaP7LIvZgOvaXQOuUOCJWXPSxi1TSIz5gdZ_ZF9OVTPnVsL2mGryCnumjJvUj