Wisconsin Better Business Bureau: Study examines risk to businesses from business email compromise scams

Posted on Thursday, Sep 26, 2019

Milwaukee, Wis. – An in-depth investigative study by Better Business Bureau (BBB) finds that business email compromise scams are skyrocketing in frequency and have cost businesses and other organizations more than $3 billion since 2016.

Business email compromise fraud is an email phishing scam that typically targets people who pay bills in businesses, government and nonprofit organizations. It affects both big and small organizations, and it has resulted in more losses than any other type of fraud in the U.S., according to the Federal Bureau of Investigations (FBI).

The investigative study – **"Is That Email Really From 'The Boss?' The Explosion of Business Email Compromise (BEC) Scams"** – looks at the prevalence of BEC scams and the criminal systems that perpetrate them. It digs into the scope of the problem, who is behind it, the multi-pronged fight to stop it and the steps consumers can take to avoid it. Read the full study at bbb.org/becstudy.

BEC fraud takes many forms, but in essence, the scammer poses as a reliable source who sends an email from a spoofed or hacked account to an accountant or chief financial officer (CFO), asking them to wire money, buy gift cards or send personal information, often for a plausible reason. If money is sent, it goes into an account controlled by the con artist.

The FBI recognizes at least six types of activity as BEC or email account

compromise (EAC) fraud, which differ based on who appears to be the email sender – a chief executive officer (CEO) asking the CFO to wire money to someone, a vendor or supplier requesting a change in invoice payment, executives requesting copies of employee tax information, senior employees seeking to have their pay deposited into a new bank account, an employer or clergyman asking the recipient to buy gift cards on their behalf, even a realtor or title company redirecting proceeds from a real estate sale into a new account. These targeted email phishing scams are sometimes called “spear phishing.”

This serious and growing fraud has tripled over the last three years, jumping 50% in the first three months of 2018 compared to the same period in 2017. In 2018, 80% of businesses received at least one of these emails. From 2016 through May 2019, the Internet Crime Complaint Center (IC3) received 58,571 complaints on BEC fraud, with reported losses in the U.S. totaling $3.1 billion. BBB’s report finds that the average BEC loss involving wire transfers is $35,000, while the average loss involving gift cards is $1,000 to $2,000. However, the cost to businesses can be much higher: Google and Facebook lost more than $100 million to BEC fraud before the perpetrator was arrested in 2017.

An Edwardsville, Illinois, real estate agent told BBB that on the closing date for a house she helped sell, the buyer received an email appearing to come from the agent, requesting that the buyer wire funds to a specified account, contrary to the agent’s instructions that the buyer bring a certified check to the closing. While the agent did not send the email nor was it from her true email address, the amount requested was the actual closing price of the house, and an attached PDF showed the letterhead of the real company handling the transaction; the account to which the money was to be wired was fake. The buyer did not comply and brought a certified check to the closing. Since the agent reported the incident to her manager and the title company, her company now warns clients to call the title company or real estate agent if they receive instructions to wire real estate closing money.

According to BBB’s report, the majority of defendants who have been arrested or charged for BEC fraud in the U.S. over the last three years are of Nigerian origin. The report says 90% of BEC groups operate out of Nigeria, with other Nigerian fraud groups operating from the U.S., Canada and many other countries around the world. In breaking down the anatomy of a BEC scam, the report notes that fraud gangs need the names of people within an organization, their job function and their email username and password, often obtained with illicit open source tools or free trials or lead generation services; that they must send emails directly to people,

impersonating a trusted superior or partner and seeking money, which they can accomplish with a fake email address or domain name or by hacking a real person's email account; and that they need a way to obtain money sent by victims, often via money mules, as detailed in a February 2019 BBB study about romance scam victims who become money mules.

Active efforts are being made to fight BEC fraud. On August 22, 2019, 80 defendants, believed to be responsible for at least $6 million in losses, were indicted in Los Angeles for BEC fraud in a major effort led by the FBI. On September 10, 2019, a worldwide law enforcement effort yielded 74 arrests for BEC-related fraud in the U.S., 167 in Nigeria and 40 in several other countries, with nearly $3.7 million in assets seized from the fraudsters. The U.S. Justice Department has brought at least 22 cases in the last three years, many as part of a collective enforcement effort dubbed "Operation Wire Wire," named for BEC fraud's common name among Nigerian fraudsters.

The report recommends:

- BBB urges businesses and other organizations to take technical precautions such as multifactor authentication for email logins and other changes in email settings, along with verifying changes in information about customers, employees or vendors. The report also urges culture and training changes in organizations – namely, confirming requests by phone before acting and training all employees in internet security.
- There is a strong need for more international cooperation between law enforcement agencies.
- Email system providers should consider enabling additional features to help prevent BEC fraud, including default settings with more security.
- Law enforcement should recognize that BEC fraud gangs engage in many varieties of the fraud at the same time and focus on the key actors in the frauds, not just supporting actors such as money mules.

What to do if your organization has lost money to a BEC fraud:

- If an organization finds that it has been a victim of a BEC fraud, it needs to immediately call its bank to stop the payment and report it to the FBI in the U.S. or the Canadian Anti-Fraud Centre in Canada. If a report is filed within 48 hours, there is a chance the money can be recovered.
- Complain to the FBI's Internet Crime Complaint Center. IC3 also asks people to

report unsuccessful BEC attempts as well. Information from attempts may help establish patterns or identify mule bank accounts.
- Complain to the Canadian Anti-Fraud Centre: 1-888-495-8501.
- Report fraud to BBB Scam Tracker.

For an online version of this story, click HERE. For more information or further inquiries, contact the Wisconsin BBB at www.bbb.org/wisconsin, 414-847-6000 or 1-800-273-1002. Consumers also can find more information about how to protect themselves from scams by following the Wisconsin BBB on Facebook, Twitter, Instagram and YouTube.

ABOUT BBB: For more than 100 years, the Better Business Bureau has been helping people find businesses, brands and charities they can trust. In 2018, people turned to BBB more than 173 million times for BBB Business Profiles on more than 5.4 million businesses and Charity Reports on 11,000 charities, all available for free at bbb.org. There are local, independent BBBs across the United States, Canada and Mexico, including BBB Serving Wisconsin which was founded in 1939 and serves the state of Wisconsin.