Articles + Publications | March 8, 2021

WTF (Wire Transfer Fraud)?! – Steps to Reduce Risk

Privacy & Cybersecurity Newsletter

WRITTEN BY

Molly McGinnis Stine | Andy Sawyer | Matthew Murphy

Business email compromise (BEC) threats are soaring. Huge amounts of money are at risk. We share some practical tips to reduce the chances of being swindled — and to try to recover amounts if you are.

In BEC and related scams, the threat actors trick unsuspecting targets into sending money to the perpetrators, often either by fraudulent wire or ACH transfer instructions.[1] These scams, which target organizations from multinational corporations to small churches, rely heavily on the art of deception to defraud targets or to dupe them into desired action.

The Schemes

Generally, BECs involve communications with the target organization that are designed to appear legitimate. Threat actors have developed certain variants of BEC scams.[2] This article focuses on those schemes that look to trick people into sending funds to a fraudster by posing as a reliable figure (such as a manager, a vendor, a customer, or a client) to request payment for a real or seemingly real transaction.

We described the mechanics and pitfalls of some of these schemes in our last article. These threat actors rely on the recipient's faith in known relationships, desire to help, and interest in taking on new business or keeping commercial deals going. The scams might involve emails from addresses that appear legitimate but in fact are slightly different, contain enough real information to seem trustworthy, or urge immediate action for seemingly valid reasons. No matter the method, BECs mean big bucks. The Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3") tracks and analyzes BEC complaints and reports. They have reported that, between June 2016 and July 2019, global victims suffered losses of more than $26.2 billion, with the U.S. making up over $10 billion of that total.[3]

The Protections

Technical Measures

Your technical environment defends you against a number of BEC attempts. The FBI[4] and others encourage you to:

- Ensure that both desktop and web applications run the same software versions to allow appropriate syncing and updates.
- Consider the necessity of legacy email protocols, such as POP, IMAP, and SMTP, that can be used to

circumvent multi-factor authentication.

- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Enable security features that block malicious email, such as anti-phishing and anti-spoofing policies.
- Enable multi-factor authentication for all email accounts.
- Prohibit automatic forwarding of email to external addresses.
- Frequently monitor the Email Exchange server for changes in configuration and custom rules for specific accounts.
- Create a rule to flag email communications where the “reply” email address differs from the “from” email address.
- Add an email banner to messages coming from outside your organization indicating they are from an external sender.

Policies to Consider

You can bolster your technical defenses by anticipating the possibility of BECs. You stress the importance of being prepared to your management, employees, and business partners by proactively establishing practices. These policies should be revisited for updates as needed. You can consider the following:

Your Bank

- Ask your bank about steps you and they agree to take to verify transactions: (1) made to new accounts before funds are sent, and/or (2) above a designated threshold amount.
- Ask your bank about steps you and they agree to take in the event of a misdirected electronic payment.

Your Customers/Clients/Vendors

- Consider written agreements with customers, clients and vendors to establish agreed protocols to verify changes in account details, to deal with “rush” requests for funds, or to verify requested payments above an agreed threshold amount. Such protocols could include identification of agreed methods of verification and contact names for verifications.
- Consider including in contracts (with customers, clients and vendors) an allocation of responsibility in the event of a misdirected electronic payment and indemnification provisions related to such payments.

Your Payment Processes

- When you receive payment details for a new account, a change in payment details, or for any transaction with a “red flag” (funds to a new bank, a new account, a new payee name, an unexpected country, etc.), contact the payee to confirm the payment instructions. It is important to use a means that is different than the way you were contacted and that is one you can verify from an independent source or exchange. For example, if you are contacted by email, reach out to the payee by telephone using a number you have from a website. Do not use a phone number provided in the email with the payment instructions.
- If you receive a check from someone you believe to be a genuine client or customer with instructions to make disbursements on the funds, wait until the check clears before making any payments on the funds.
- Consider regular audits and/or system alerts for amounts over certain thresholds, for an unexpected number of

transactions to same vendor over a period of time, or for new account details even for known payees.

Your Employees

- Provide relevant, engaging and frequent training to employees about how to identify and avoid BECs and why it is important to them and to the company.
- Learn to spot phony emails, knowing that bad actors are increasingly skilled at creating realistic fakes.
  - Read sender email addresses closely, including the domain name. In addition to spoofing an individual's name, threat actors use slightly misspelled domain names to commit fraud.
  - Consider the tone, grammar, vocabulary, and spelling of the message.
    - Read the email aloud. Does it sound like the sender if you know the sender? Is it consistent with prior phone conversations or email correspondence? Does it end with the sender's usual sign-off? Does the sender use the same names you'd expect (nicknames, initials, etc.)?
    - Be alert to misspellings of people or company names that a real sender would not likely misspell.
    - Many threat actors are English as a second language learners. Often, they converse in British English which has spelling, vocabulary and grammar differences from American English.
    - Problematic or improper use of parts of speech (including participles, pronouns, prepositions, conjunctions) often expose impostors.
- Empower your employees to follow the policies.
  - Do not pressure them to make exceptions.
  - Encourage them to resist the schemer's pressure to act immediately.

Response Plan

Be ready to act quickly if you find you have been tricked into sending funds to a threat actor's account. Your chances to recover any funds are more likely if you discover the fraud very soon after it is perpetrated. Once discovered, even if some time has lapsed after the scheme occurred, you are better off if you deploy a response plan immediately.

- Create a response plan in the event of a BEC that results in misdirected funds.
  - Create contact list: internal contacts, your bank, the bank receiving the funds, the local FBI office, filing an IC3 report (www.ic3.gov), the police, and, as appropriate, your insurance professionals.
  - Make clear who is to take specific steps.
- Be ready to execute the response plan and to authorize those with responsibilities to carry them out.
- Review the plan regularly and update as needed.

Conclusion

You need both a strong offense and a quick defense against the insidious threat of BECs. Awareness of the problem is key and action to combat it imperative. We encourage you to consider the types of steps discussed in this article along with others you may employ or may assess for your particular circumstances.

___

[1] Wire transfer and ACH fraud are just two ways in which threat actors try to profit from BECs. Others include, for example, diverting direct deposit of payroll by seemingly changing account information or encouraging recipients to buy gift cards and then share the card codes with the threat actor. Notably, bad actors may also use BECs to try to gain access to an organization's systems or data for financial purposes other than redirecting a specific payment.

[2] We note that successful scams may attempt business email compromise, but may successfully hijack funds whether or not the victim's email system is actually compromised. In fact, system compromise may not be the threat actor's goal, as the threat actor may hunt only for information to use as part of a larger scheme or to request certain actions by the recipient. While this article discusses all of this generally within the context of BECs, the distinction is important as the risks and solutions will differ for technological infiltrations and for social engineering efforts.

[3] https://www.ic3.gov/Media/Y2019/PSA190910 (last accessed February 21, 2021).

[4] https://www.ic3.gov/Media/News/2020/201204.pdf (last accessed February 21, 2021).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber