RLI PROFESSIONAL SERVICES GROUP

ARTICLE:

WIRE TRANSFER FRAUD: VIGILANCE IS THE BEST DEFENSE

STATISTICS

Business email compromise (BEC)* scams represent nearly half of the total losses of the top 10 internet crimes. In 2018 alone, over $1.3 billion in losses were reported to the FBI's Internet Crime Complaint Center (IC3) due to fraudulent wire transfers by victims of BEC schemes. These figures do not even account for the lost time, wages, files, equipment and losses associated with remediation services used by victims to minimize their damages (such as the cost of forensic investigations, cost of restoring lost data or hacked systems or the damage to the company's reputation and brand).

**Business email compromise, or BEC, is the term used describe the impersonation of executives or a trusted business contact (such as a client or bank) to obtain the transfer of funds or sensitive information. Most BEC attacks include some sort of email account compromise (EAC) that targets the individuals, such as the executives, administrative assistants, attorneys, etc. responsible for performing wire transfer payments,*

HOW CRIMINALS ATTACK

Criminals seek information to aid their wire transfer fraud in a number different ways. One wrong click can cause a variety of problems, including:

1) *Malware* — installing computer viruses, ransomware, spyware or other malicious software to gain access to your computer and steal private information, such as your passwords, credit card numbers or other financial information.
2) *Email hacks* — gaining unauthorized access to your email accounts.
3) *Phishing, vishing, smishing* — impersonating a reputable source and making phone calls, sending emails or texts to persuade you to reveal private information, such as your passwords, credit card numbers or other financial information. Often the emails and text messages include a link that takes you to a fake website as a way to collect this information. The link may also install malware on your computer. With vishing, criminals can "spoof" a legitimate phone number to make a seemingly valid contact appear on your caller ID, and with the aid of voice synthesizing equipment, impersonate an actual person.

Using these methods, criminals study company procedures (such as billing and invoicing) and relevant individuals. This allows them to mimic the appropriate format and syntax, adding credibility to their fraudulent requests and minimizing their likelihood of raising suspicion.

CASE STUDIES

Example 1: An executive assistant received an email from the CEO of the company, requesting a wire transfer of $3.2 million to one of the company's vendors as payment on an invoice. The request was sent on Friday at 3:00 p.m., a common time for the firm to make payments, and included

a personal remark: “I’m going to be offline this weekend because I’ll be coaching my daughter’s soccer game on Sunday, so don’t try to reach me; just make sure this is done today.” The criminal had studied the company’s procedures and accessed the CEO’s Facebook page, which publicized that the CEO coached his daughter’s soccer team, to add details that would lend credibility to the fraudulent request.

Example 2: An accountant received a wire transfer request from the CEO of the company while the CEO was out of country on vacation. The request asked for a wire transfer of $737,000 for a “time sensitive acquisition” and specified that the transfer be completed by close of business. A subsequent email containing instructions for the transfer included a letter of authorization, with the CEO’s signature over the company seal, as was consistent with company procedure. It was later discovered that the request was fraudulent. A closer examination revealed that the CEO’s email was missing one letter — instead of .com, it read .co. Additionally, it appeared that the CEO’s signature had been forged, and the company seal had been cut and pasted from the company’s public website.

Example 3: Bank of America customers in the Houston, Texas area received a text message alleging issues with their bank account and urging customers to call the supplied number. Customers who called the number were directed to the following automated message: “Thank you for calling the Bank of America. A text message has been sent to inform you that your debit card has been limited due to a security issue. To reactivate, please press one now.” After pressing one, customers were prompted to enter the last four digits of their Social Security number, then the full debit card number and expiration date — information criminals can use to access the customers’ accounts.

RED FLAGS

Here are some common signs of a fraudulent wire transfer request.

1. Incorrect email address. A seemingly legitimate email, with very slight changes.
2. The use of bad grammar, poor punctuation, awkward phrasing or odd capitalizations.
3. Request for personal information, such as a password or PIN.
4. Request that is out of the ordinary or deviates from the established pattern for the person or business requesting the transfer.
5. A sense of urgency. A rush request or demand that the transfer occur immediately.
6. An inability to reach the person requesting the funds.

PROTECTING YOUR FIRM

1) **Education and awareness training —** Train your employees and clients to protect sensitive information and to spot scams.

   a. **Be web wise.** Train employees not to post private or sensitive information, such as internal protocols, on publicly accessible sites.

   b. **Don’t open anything unfamiliar or suspicious.** Train employees to verify email address accuracy when checking mail on a cell phone or other mobile device, and to steer clear of any emails or links that are unfamiliar or suspicious.

   c. **Don’t rely too heavily on caller ID.** Caller ID can be easily “spoofed” to display exactly what the scammer wants it to show.

   d. **Verify payment changes with the intended recipient.** If it involves the moving of money, make sure employees and clients know what additional steps should be taken before proceeding.

   e. **Regularly update security software.** Make sure reliable security software is installed and regularly updated on all devices.

   f. **Stay up-to-date on fraud schemes.** See the ADDITIONAL INFORMATION section below for common resources.

   g. **Implement a cybersecurity protocol policy.** Have a policy outlining who employees should call or notify if they suspect a suspicious request.

2) **Wire transfer protocols —** Implement wire transfer protocols to verify the authenticity of each wire transfer request. If the request originates from someone in your office, such as the company CEO, consider confirming the request with them in person. If the request originates from a client or someone outside of your office, consider using a call back verification process – call the person using a number you have previously used, not the one from the current request, in order to verbally verify the request.

3) **Test vulnerabilities —** Test the effectiveness of your training and protocols. Make adjustments as necessary.

4) **Fraud response**

   a. **Contact the bank.** As soon as the fraud is recognized, request recall or reversal.

   b. **Notify the authorities.** File a detailed complaint with the proper authorities such as the FBI. Go to www.ic3.gov for more information.

   c. **Document what happened and reassess.** Evaluate the effectiveness of your employee training and wire transfer protocols, and adjust them if appropriate.

5) **Insurance —** Review your insurance policy. Does it cover losses due to cyber security fraud? If not, you may be paying out of pocket for these costs.

ADDITIONAL INFORMATION

1. **Federal agencies,** such as the FBI and the FTC, update their websites on popular scams that are being perpetuated (visit https://www.fbi.gov/scams-and-safety/common-fraud-schemes or https://www.consumer.ftc.gov/features/scam-alerts).

2. **Internet Crime Complaint Center (IC3)** releases a report every year identifying cybercrime trends and what those trends may represent in the coming year (visit https://www.ic3.gov/media/default.aspx).

3. **State agencies,** such as the State of California Department of Justice, release their own warnings of common scams residents should be aware of (visit https://oag.ca.gov/consumers/common-scams).

4. **Cybersecurity firms** may also blog about scams that are emerging (visit https://securingtomorrow.mcafee.com/category/consumer/consumer-threat-notices/).