

IS THAT EMAIL *REALLY* FROM YOUR CLIENT?

A new breed of cyber threat aims to impersonate your clients. Here's how you can minimize the risk to you and your clients.



Sponsored by:





Advisors face a new category of cyber threat: email account compromise (EAC), a tactic that involves using clients’ email accounts to initiate fraudulent wire transfers or otherwise steal funds. To fend off the new wave of attacks, advisors should familiarize themselves with how EAC works and the best practices for preventing it.

“Even if you think you’re protected, you may not be,” says Rob Fernandes, chief investment security officer at the Investment Center. “That’s because cyber threats are evolving continuously in response to the precautions people are taking. As fraudsters continue to become more sophisticated in their methods, it’s crucial to respond to the latest tactics before you become a victim.”

A False Sense of Security

For years, one of the main cybersecurity threats for advisors has been business email compromise (BEC). BEC schemes target the email accounts of high-level employees, such as CEOs or CFOs, to gain access to sensitive information and ultimately misappropriate funds.

This type of cyberattack has happened to a broad array of companies, not just financial institutions. One prominent example occurred in 2015, when criminals targeted the multinational toy company Mattel. They mined social media and other digital sources for sensitive information about high-level company employees and succeeded in compromising the email account of the CEO. After that, they spent time familiarizing themselves with Mattel's procedures, particularly regarding money transfers. Finally, they sent an email from the CEO's account to a Mattel finance executive requesting a \$3 million payment to a new vendor in China. The executive saw nothing suspicious in the request and approved the transfer, only realizing her mistake when she mentioned the transaction to the CEO later that day.

The FBI estimates that BEC of this sort accounted for more than \$12 billion in losses around the world between October 2013 and May 2018.

Of the nearly **80,000 incidents** worldwide, more than half — about **41,000** — occurred in the U.S.¹

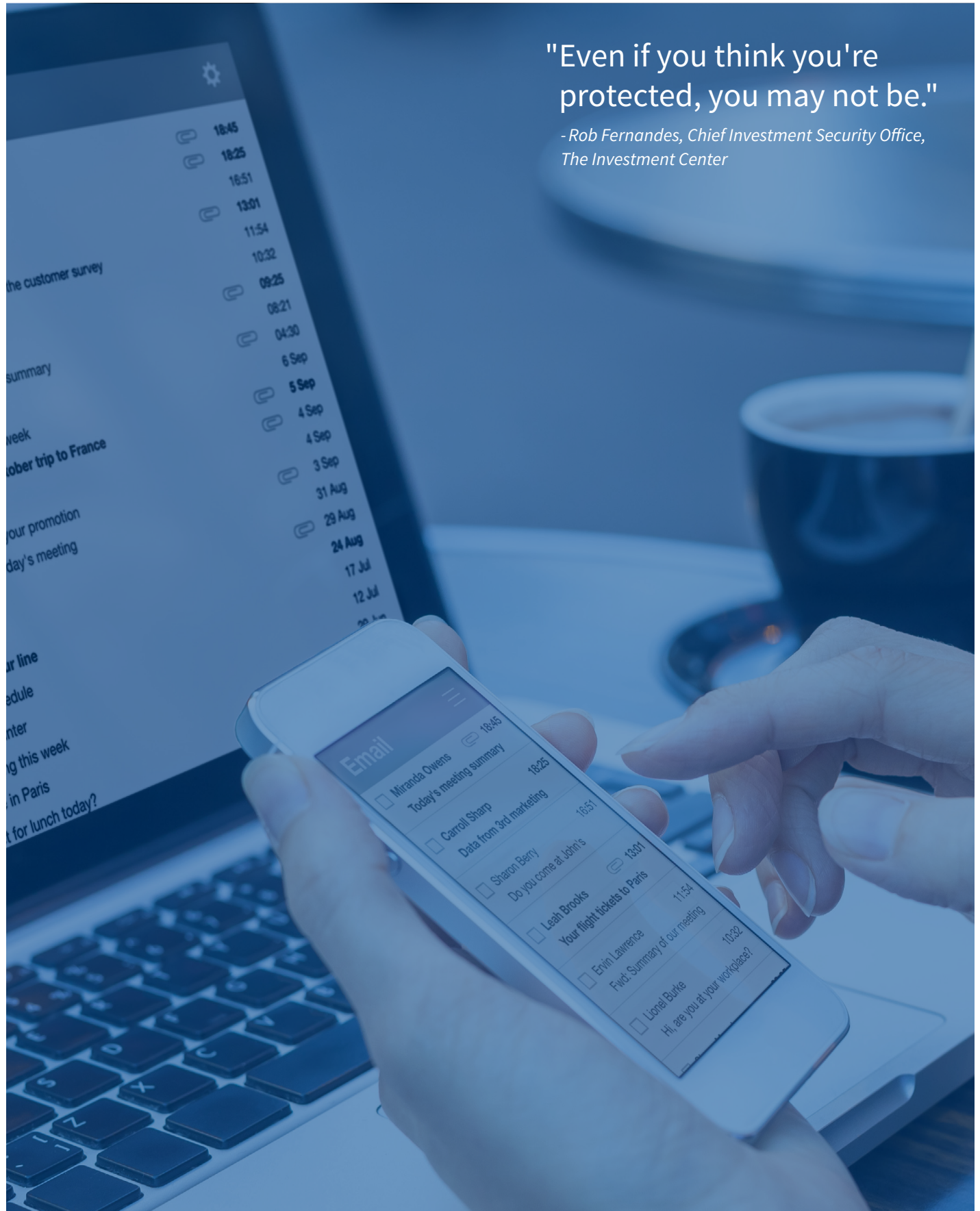
The prevalence of BEC has spurred the financial industry to develop safeguards and employee educational measures to counter it. The industry's robust response has helped tamp down BEC — though it's still a serious threat — but it may give some advisors a false sense of security regarding cyberattacks.

¹ FBI, "Business E-mail Compromise: The 12 Billion Dollar Scam," July 2018 (<https://www.ic3.gov/media/2018/180712.aspx>)



"Even if you think you're protected, you may not be."

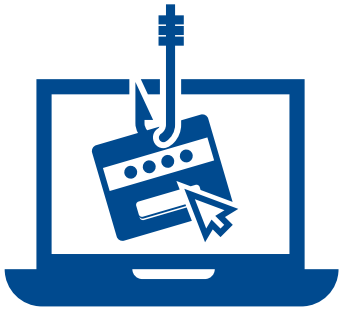
- Rob Fernandes, Chief Investment Security Office,
The Investment Center



The Rise of EAC

Hackers have developed new, more sophisticated approaches in recent years. EAC is among the most notable of these new strategies.

EAC has elements of BEC. It also draws on traditional phishing scams, in which criminals send emails purporting to be from reputable sources to entice individuals to click on links or download attachments. The goal of these scams has traditionally been to steal personal financial information or to demand a ransom to restore access to the individual's computer system. Phishers tend to cast a wide net, in some cases targeting millions of individuals at once, and many take little care with the quality of their writing and messaging. Most recipients of phishing emails may detect the malicious intent, but it only takes a handful of victims for the scheme to succeed.



EAC attacks tend to be more focused and sophisticated than traditional phishing scams. In an EAC attack, crooks use individuals to gain access to the ultimate target: typically businesses such as advisory firms that the individual deals with on a regular basis. EAC scammers may send out emails to many individuals, as in traditional phishing schemes, but tend to use more polished language and messaging. In some cases, they don't use email at all; one common tactic is to hack into email accounts using programs that help guess individuals' passwords, leaving no evidence for the account owner to detect the breach.

Once a criminal has gained access to an individual's email account, he can conduct surveillance on the person's emails and on social networks and other accounts. He may lurk undetected at this stage for several months, waiting for the right opportunity to strike. At that point he can send emails from the individual's account and reply to emails that were sent to the individual; delete emails to and from the account to hide evidence of the attack; and have all emails forwarded to another account.

He can also change the account's security settings, **including passwords**, security question answers and associated phone numbers.

How Advisors are Targeted

Financial advisors present an ideal end-target for EAC criminals, since they manage large sums of money and frequently direct substantial money transfers. Here's how a hypothetical EAC scam directed at an advisor could play out.

The scam begins with the advisor getting a call from a client requesting a **\$30,000 wire transfer**.

The advisor agrees to email the client the appropriate forms to initiate the transfer. Shortly thereafter, the advisor receives the completed forms with the client's signature. All seems to be going according to protocol.

Minutes later, the advisor receives a follow-up email from the client. The note informs the advisor that the client is having problems with the usual bank account and asks to make the transfer to another account. The advisor agrees, and a few minutes later receives a new form with the new bank and routing information, again with the client's signature. The advisor then initiates the wire transfer and replies to the client telling them it's been initiated.

A few hours later, the advisor receives a call from the client inquiring about the wire transfer. The advisor informs him/her that the transfer was completed and that a receipt was sent. The client tells the advisor they never received the email or the funds.

With a racing heart, the advisor questions the client about the day's events. The advisor quickly realizes that after the request was initiated, the advisor was communicating with someone else — a thief who injected him or herself into the communication chain and excluded the client. Now the advisor must deal with the fallout.



How to prevent EAC


Advisors can take a number of steps to prevent EAC. First and most important, advisors should never process a client's request based on digital verification alone. Rob Fernandes says the message is simple: "Never trust anything coming from email."

Two-factor authentication at every stage in the process is crucial in ensuring the identity of the client. Most often, this requires a simple phone call. For example, in the above scenario, the theft could have been prevented if the advisor had called the client after each new email to verify that the information was correct, and the new request was legitimate. Advisors may be concerned that frequent phone communication of this sort could annoy clients. Fernandes' response: "If the cost of preventing fraud is a slight inconvenience for you and your client, that's an acceptable price to pay." Moreover, he says, the inconvenience can be minimized if advisors make clients aware of the two-factor authentication protocol before there is a need to use it and communicate the importance of such safeguards in preventing fraud.



Advisors can also look for red flags in emails requesting fund transfers. These include urgent requests of any type, errors in the language of the email and requests for secrecy around the interaction. Many organizations have begun sending employees test emails that exhibit some or all of these red flags, then following up with conversations about how they responded.

“By far **the most important safeguard is education** throughout the entire communication chain,” says Fernandes. “Advisors, broker/dealers and clients should all be on the same page about cyber threats and security protocols.”



"If the cost of preventing fraud is a slight inconvenience for you and your client, that's an acceptable price to pay."

*- Rob Fernandes, Chief Investment Security Office,
The Investment Center*

To this end, advisors should consider educating clients about how to secure their email accounts properly and reminding them periodically to do it. Best practices include using a password manager to avoid password redundancy; creating a long passphrase for the manager; enabling multifactor authentication; and subscribing to a breach notification service, such as the one offered by the identity theft protection company LifeLock.

In the unfortunate event that an advisor falls prey to EAC, they should immediately alert their supervisor and the firm's cybersecurity or compliance department. The federal government's Financial Crimes Enforcement Network, or FinCEN, can help fraud victims recover some or all of the stolen funds, but it's important to act quickly, as there is a much a greater chance of recovering the funds if the crime is reported within 24 hours.

Cyber crime techniques are constantly evolving, so advisors' defenses must also continue to adapt. By remaining vigilant about the threat of EAC and implementing the practices outlined above, the financial industry can work toward reducing this risk and safeguarding clients' assets.



Resources

FINRA Report on Cybersecurity Practices

- www.ic3.gov/media/2018/180712.aspx
- www.sec.gov/spotlight/cybersecurity
- www.sec.gov/litigation/investreport/34-84429.pdf

About the Investment Center

For over 30 years The Investment Center has had one focus — the success of every advisor who partners with us. By joining The Investment Center, an advisor has full access to a diverse team of highly accomplished experts in the fields of finance, marketing, technology, and practice management. Our product selection coupled with an infrastructure designed to meet an advisor's needs in a timely manner ultimately results in an enhanced advisor-client relationship. Our practice management experts offer proven strategies in client acquisition and retention to help our advisors reach their specific goals and objectives.

To hear how The Investment Center can help you meet your goals, visit our website www.investmentctr.com/genx