WILMINGTON TRUST

MEMBER OF THE M&T FAMILY

Seven Steps to Protect Yourself from Fraud

Protecting yourself—and your business—from email and wire fraud scams

Key points

- Business impersonation scams are a large and growing risk for high-net-worth individuals, closely held business owners, and institutions
- Scams have claimed victims in all 50 states and throughout the world
- Learn seven steps that can help you protect yourself and your business from impersonation and other types of fraud

One afternoon, a hypothetical comptroller at a mid-sized company got an email that appeared to be from the CEO, instructing him to wire $400,000 to an attorney the CEO was working with to acquire an overseas company. After several email exchanges, the comptroller initiated the wire transfer. A few days later, the CEO noticed the transfer and asked the comptroller about it. The CEO had never authorized the transfer. Instead, the CEO's email account had been hacked by a fraud ring, who then engaged in a crime called "executive impersonation fraud." The money was never recovered.

This example of an executive impersonation scam is part of a larger group of growing business impersonation scams, which also includes email compromise and wire transfer fraud. The FBI estimates that business email compromise, in which a criminal compromises a legitimate business email account in order to conduct unauthorized transfers of funds, has cost individuals over $12.5 billion in the four and a half years from October 2013 to May 2018. Scams have claimed victims in all 50 states and more than 100 countries. And there is every reason to believe the threat is growing. Between December 2016 and May 2018, there was a 136% increase in identified exposed losses, the FBI says.[1]

[1] Business E-mail Compromise The 12 Billion Dollar Scam, FBI. July 12, 2018, Alert Number I-071218-PSA.

Continued

Stay alert to these scams

In addition to executive impersonation scams, the FBI reports that cyber threats can take a number of different forms. Some of the most common include:

Employee email compromise

After hacking an employee's personal email account, a criminal requests invoice payments to vendors on the employee's contact list. Payments are directed to the perpetrator's bank account. The business may not know about the fraud until vendors contact them to follow up on payment status.

Criminals may also target individuals, redirecting regular payments for mortgages, insurance, or other expenses to their own accounts.

Attorney or personal representative impersonation

Emails purportedly from attorneys or other representatives demand speedy, confidential payment. Often these demands are timed to coincide with other authorized payments—at the end of the week or other billing cycle.

Vendor/supplier impersonation

With this business scam, fraudsters will hack into a company's email database and look for customers. They then create a realistic invoice from a known vendor and email the non-suspecting customers, telling them an invoice is due, but the payment information has changed. They'll then give ACH or wire instructions to their own fraudulent account.

Phishing schemes to obtain private data

In businesses, human resources departments receive fraudulent requests for W-2s and personal information, which can be used for identity theft and credit card fraud. Individuals may also be targets for phishing schemes via emails and phone solicitations asking for personal information like bank account numbers and Social Security numbers.

Wire transfer fraud

As in the example above, a company or individual receives a fraudulent request for a wire transfer, which is made to look as if it came from someone within the company or a trusted friend or relative.

Seven steps to help protect against impersonation fraud

STEP 1:

Keep business and personal information safe

It's best to start with good basic computer security—not reusing the same username/password across systems you access, changing your password regularly and using hard-to-guess combinations of letters and numbers, not opening email attachments from unknown senders, keeping your virus software up-to-date, and being careful about posting personal and business information on social media. Be cautious, too, about offline requests for information by phone or even in person. Many fraud perpetrators use a combination of hacking and social engineering to infiltrate systems.

STEP 2:

Beware of email-only requests for payment

Scrutinize requests for payments, whether they are directed to you personally or to your business. Be attuned to any unusually large invoices or those that must be processed quickly. If you own a business, train your staff to flag suspicious requests for payment, especially those that come into your company solely through email. Poor use of English or badly copied company logos can also be indicators of fraud.

STEP 3:

Confirm payments with vendors

Any emails requesting the creation or change of wire payment instructions should be verified by phone. Verify the phone number by using the company's website. Often, hacked emails contain fraudulent contact information.

STEP 4:

Check invoices and emails for errors

Spoofed emails and invoices often differ in small, hard-to-identify ways from the real thing. For instance, an email address ending in .com might be shortened to .co. Checking the bank routing numbers against previous invoices can also turn up fraudulent requests for funds.

Continued

STEP 5:

Set up dual authorization and verification

Many organizations unknowingly take on fraud risk related to executive impersonation by giving a single individual, usually the comptroller, sole authority for disbursements. Regardless of size or employee tenure, companies should always require dual authorization and separation of duties to mitigate outside risk from penetrating the organization. If you rely on an accountant or family office to pay your personal bills, make sure that they have dual authorization and verification procedures in place.

STEP 6:

Educate yourself and your employees

Fraudsters prey on people and organizations with a lack of fraud knowledge. Keeping yourself and all of your employees educated on the most current fraud trends is key to possibly preventing fraud before it occurs or recognizing it quickly to reduce potential losses.

STEP 7:

Choose a financial advisor who can help

Partnering with a financial institution that keeps you informed of fraud developments and is invested in helping to protect your organization from fraud is also key. As a partner in fraud prevention, your financial advisor could:

- Keep you informed of relevant fraud industry data
- Provide help on identifying fraudulent activities early to reduce organization losses
- Advise you on fraud prevention best practices
- Offer necessary fraud protection products and procedures, such as dual authorization and separation of duties, to reduce your risk of becoming a fraud victim
- Help you to reconcile account activity daily
- Encourage out of channel verification of any payment

What if you've already been hacked?

If you've been the victim of executive impersonation, business email compromise, or wire transfer fraud, it's important to act immediately.

1. Contact your own bank. Very large wire transfers can take several days to process. If you notify your bank immediately, they may be able to stop or unwind a transfer.
2. Contact the authorities in the jurisdiction your funds were transferred to. For example, police in hubs for fraudulent activity like Hong Kong and China may be familiar with the criminal rings who defrauded you. In some cases, they can help to freeze and recover assets that have been fraudulently acquired.
3. Review your insurance policies for potential coverage and contact your insurance advisor or attorney, who will be able to determine whether corporate insurance will cover your losses and can begin the process of filing a claim. If your personal accounts have been attacked, contact your regular family attorney for guidance.
4. In some countries, you may need to hire local counsel in the jurisdiction where your funds were directed. Local counsel can work with police and the court system to recover your money. They can help you navigate language barriers, different legal systems, and even time zone differences that can make it hard to pursue your claim yourself.

Wilmington Trust's advisors have the experience and knowledge to help you reduce your exposure to certain types of fraud, including executive impersonation, business email compromise, and wire transfer fraud. For more information about how we can assist you in helping to prevent fraud in your personal or business accounts, contact your relationship manager or visit Cybersecurity and You.