3 Facts About BEC Attacks

Wire transfer fraud is scary business—and probably more prevalent than you realize. Frequently referred to as business email compromise (BEC), this flavor of cybercrime is very difficult to stop with technical safeguards and frequently impossible to reverse should an attacker successfully trick a target into wiring money.

When it comes to preventing these attacks, vigilance on the part of employees and consumers is absolutely critical. The following three facts will explain the scope of the problem and help you avoid becoming a victim of these attacks.

## Fact #1: Billions of Dollars Have Been Lost Since 2013

The U.S. Federal Bureau of Investigation (FBI) has been tracking BEC—also known as email fraud and email account compromise (EAC)—domestically and globally since October 2013. The recent trends related to fraudulent wire transfers are alarming:

* Each year, there are tens of thousands of complaints about BEC scams, resulting in billions of dollars in damages.
* BEC scams have been reported in more than 150 countries and all 50 U.S. states.
* Businesses and organizations aren’t the only victims of these types of attacks—consumers can also be impacted. For example, the FBI has identified BEC scams targeting all points along the real estate transaction chain, including buyers, sellers, and realtors.

It’s also important to note that BEC attacks are not solely about wire fraud. For example, cyber-attackers use illegally obtained tax information (like W-2 statements of U.S. workers) to commit tax fraud and other crimes. In another type of BEC scam, fraudsters impersonate workers in order to trick payroll departments and payroll services companies into diverting direct deposits so they can steal employees’ wages.

**Bottom line:** BEC attacks are widespread and are affecting organizations and individuals alike. And even with billions in losses now calculated each year, the numbers are likely to be low because BEC attacks often go unreported. Don’t fall into the trap of thinking it could never happen to you—cybercriminals look up, down, and across org charts to find their targets, and they target consumers as well.

## Fact #2: BEC Attacks Take Advantage of the Familiar to Fool You Into Making Bad Decisions

Technical tools are often ineffective against BEC attacks because of the way these attacks are constructed. Emails generally don’t contain malicious links or attachments—two hallmarks of phishing attacks that email monitoring tools can identify and block.

In contrast, BEC attacks attempt to “fly under the radar,” using familiar names and details to disguise themselves as safe, legitimate communications. For example, attackers will mine social media and other sources of public information to get to know their targets, and they will often build rapport over multiple contacts—via phone and email—to lull the target into believing they are communicating with someone trustworthy. The wire transfer (or data) request isn’t made until the attacker is confident the target is comfortable enough to act on the request.

In some cases, attackers make messages appear to have come from a known source by using a technique known as “spoofing”; in these instances, the sending address looks like a trusted contact (though a hover over that address will reveal something different). In other cases, cybercriminals are able to steal email login credentials and send messages from a legitimate account, making it extremely difficult for an email recipient to spot a fraudulent request.

**Bottom line:** When it comes to a wire transfer or payment request (or an email asking for sensitive employee data), nothing should be taken at face value. Treat any solicitation of this nature with a critical eye—particularly if the requestor asks for a change to previously established banking processes or account details.

## Fact #3: You Have the Power to Stop BEC Attacks in Their Tracks

Cybersecurity awareness and understanding of email best practices are critical to preventing different types of fraud and to protecting personal and business data. In the case of BEC attacks, some relatively simple measures can make all the difference:

* **If you commonly request wire transfers or tax-related data ...** set up a private, “need to know” process for people to obtain face-to-face or voice-to-voice confirmation that the request is legitimate. Be sure to communicate that process outside of email, via a trusted channel.
* **If you commonly execute fund or data transfers …** you must protect yourself, your reputation, and your organization’s funds/data. Do not act on a request without obtaining confirmation of the request and approval to execute on it. This is particularly critical if you are pressed to act quickly and/or ignore established procedures. If there aren’t processes in place that can help prevent fraudulent transfers, approach your supervisor and ask that non-email-based approvals be established for these types of requests.
* **If you commonly approve fund or data transfers …** ensure you are not the sole source of approval. Work with other stakeholders to ensure your process is not prone to a single point of failure, and make sure that approvals happen via a channel (or channels) other than email. Be willing to make yourself available for approvals via phone or in-person meetings, and never undermine the approval chain by allowing transfers to happen outside of the agreed-upon process.

**Bottom line:** If you are part of the “chain of command” for fund and data transfers, you need to take your role seriously and do all you can to ensure that you prevent fraud. Awareness of the dangers and safeguards is critical. And even if you aren’t regularly involved in these activities at work, remember that you could experience a BEC attack in your personal life—particularly if you are involved in a real estate transaction. In reality, any wire or data transfer request—regardless of when it happens or where it appears to come from—should be thoroughly vetted before you act on it.