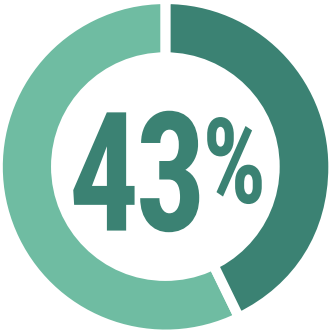
SpyCloud

Business Email Compromise 101

How these attacks work, why they persist, and what you can do to prevent them.



of internet crime losses in 2020 stemmed from BEC attacks

Introduction

According to the FBI's Internet Crime Complaint Center (IC3), losses from **Business Email Compromise (BEC)** surpassed $1.8 billion in 2020 – an average of $93,000 per incident. To put this into perspective, the average loss from a single bank robbery is around $3,000. BEC scams may not make headlines on the level of ransomware, for example, but they have remained one of the most consistent and common avenues of attack for many years.

BEC schemes are successful because they exploit the very qualities that make people good employees. For people in certain positions, receiving email requests for wire transfers, rerouting payments, or sharing sensitive financial information is part of an average workday. The trouble is, telling the difference between an authentic email and an impostor's scam is not always easy. What if illegitimate requests are literally coming from a trusted sender's email account, but the account owner is unaware their credentials have been compromised? **This is known as Account Takeover (ATO) and it is often a precursor to successful BEC attacks.** Once the ATO is underway, it's a matter of social manipulation.

THE U.S. TREASURY DEPT. ESTIMATES BEC SCHEMES COST U.S. FIRMS ABOUT $300M EACH MONTH

Understanding how to exploit human behavior during vulnerable times (i.e. the start of global pandemic or an economic recession) has allowed scammers to grow bolder, targeting not just large companies, but executives as well. Anyone can be a target – and subsequently, a victim. How can organizations protect themselves from a problem that is rooted in our very nature as humans? As we'll explore in this paper, just because the problem exists between "the keyboard and the chair" doesn't mean it's unpreventable.

GLOBALLY, BEC HAS LED TO NEARLY $30B IN LOSSES SINCE 2016

ATO and the Anatomy of BEC Attacks

To give you an idea of why BEC scams are so successful, think about the number of emails that land in your inbox on an average day. Now, think about the number of emails ***everyone*** in your organization receives daily. If your organization as a whole receives 1 million emails per year and even just 0.1% of those emails are illegitimate and make it past filters, that leaves 1,000 potential scams waiting to be activated by their recipients.

To be fair, falling for a BEC scheme isn't always a matter of employee/victim gullibility. In many cases, it begins with a successful ATO in which the criminal has fully assumed the identity of a legitimate company executive, network administrator, employee, or third-party vendor by acquiring the victim's account credentials. Obtaining those credentials is easier than you think. Thanks to a robust dark web marketplace, criminals can simply leverage reused or similar passwords from previously breached sites to gain access to existing accounts. They wait patiently, watching the activity and trends of key company employees and vendors until they have a sense of who, when, and where they should strike to have the biggest impact and generate the greatest gains from their BEC scam.

As stolen credentials have become more accessible on the dark web, so has the ability to compromise legitimate email accounts. This has allowed BEC to evolve into much more intricate and personally tailored attacks. In 2020, the IC3 saw more BEC victims targeted with different types of scams: extortion, tech support, romance scams, and work-from-home scams, among others. In these scenarios, the victim provides an attacker with a form of sensitive personal identification (PII) and financial information, which is then used to create a bank account and receive stolen BEC funds that are later transferred into a cryptocurrency account or gift cards, both of which are difficult (if not impossible) to trace.

BEC attacks generally fall into two categories: **phishing** (with emails or texts containing malicious links and/or attachments) and, more commonly, **social engineering** attacks. At the height of the pandemic, the surge in BEC attempts offered examples of how potent merging the two attack types could be. In strictly "social engineering" attacks, the victim is often "groomed" with vague-but-urgent questions from someone who may appear to be a high-level co-worker ("Are you in the office today? Can you do me a favor..."). Once the rapport is established, the criminal starts making urgent requests and may solicit funds distribution through direct deposits, payments, or gift cards, and may ask for banking details. These attacks are especially tricky to detect; the most innocuous types come in the form of direct emails or texts and contain no questionable links or attachments. Because of this, they largely bypass traditional email gateway protections or go directly to unmonitored text messages. During the pandemic, criminals used aspects of social engineering by leveraging COVID-19 in phishing emails. These emails could ask vendors to provide information ("Because of the pandemic, we're switching billing software and need your updated payment information.") or ask employees to open a link or attachment containing malware ("Employees are required to review our updated COVID-19 office protocol.").

BEC Attack Order of Operations

Identify Target + Obtain Access

Once the criminal identifies its victim organization, they use ATO or **credential stuffing** to gain access to the email account of a desired target – ideally, the target is someone in a position of authority. Impersonating executives via email makes BEC scams easier to pull off since employees are inclined to trust and react quickly to messages from the C-level.

Intercept Communications + Monitor Transactions

The criminal's objective now is to observe legitimate email activity without being seen or heard. Often, they set up an auto-forwarding rule within the account. This allows the attacker to stealthily observe the target and monitor communications from partners or vendors, particularly those that involve financial exchanges.

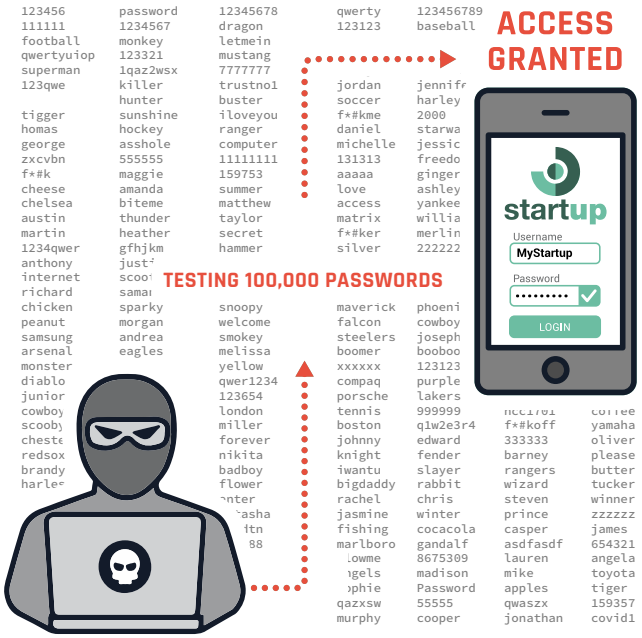


Illustration of a credential stuffing attack.

Dupe the Victim
Taking on the persona of their target, the criminal actively inserts themselves into an email conversation. The idea is to fool the victim into trusting that the criminal is who they are pretending to be. The criminal can carry out multiple parallel conversations posing as one entity to another.

Take the Money and Run
The attacker modifies a wire transfer or financial transaction details, routes payments to themselves, and moves on to the next victim organization.

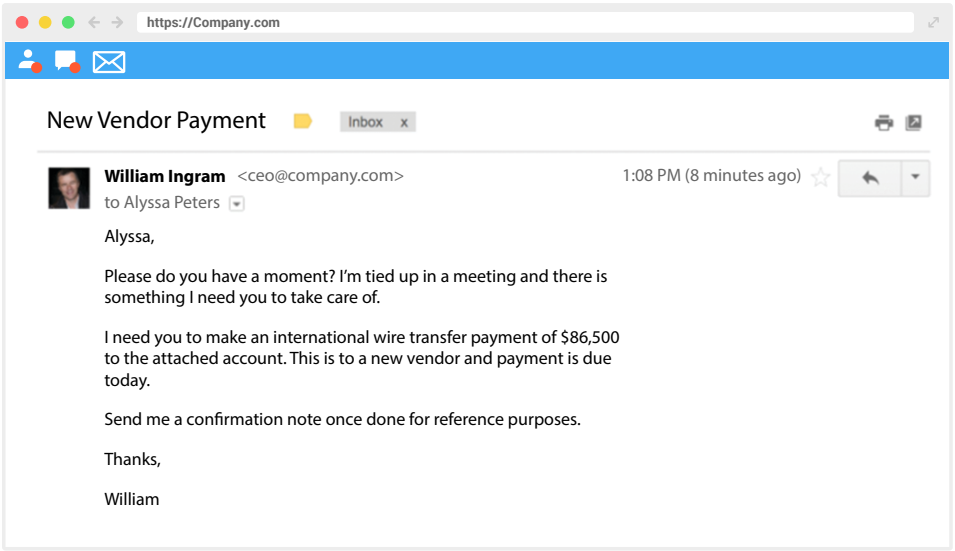
Primary Types of BEC Fraud

CEO Email Fraud

Posing as an executive is one of the more proven BEC methods for two reasons – for starters, it's human behavior for employees to immediately comply with executive requests, and executives happen to be as guilty of weak password hygiene as everyone else. In fact, **according to SpyCloud research, the credentials of 133,927 C-level Fortune 1000 executives are available for sale on the dark web.**

In CEO email fraud instances, attackers will impersonate a company CEO or other executive in an attempt to convince employees at any level into processing unauthorized wire transfers or sharing confidential tax information.

Usually, CEO fraud emails are social engineering attacks, but they sometimes can crossover into spear phishing. In these instances, the attacker impersonates a CEO asking an employee to click on a seemingly legitimate link. This tactic was prevalent during the start of the pandemic.

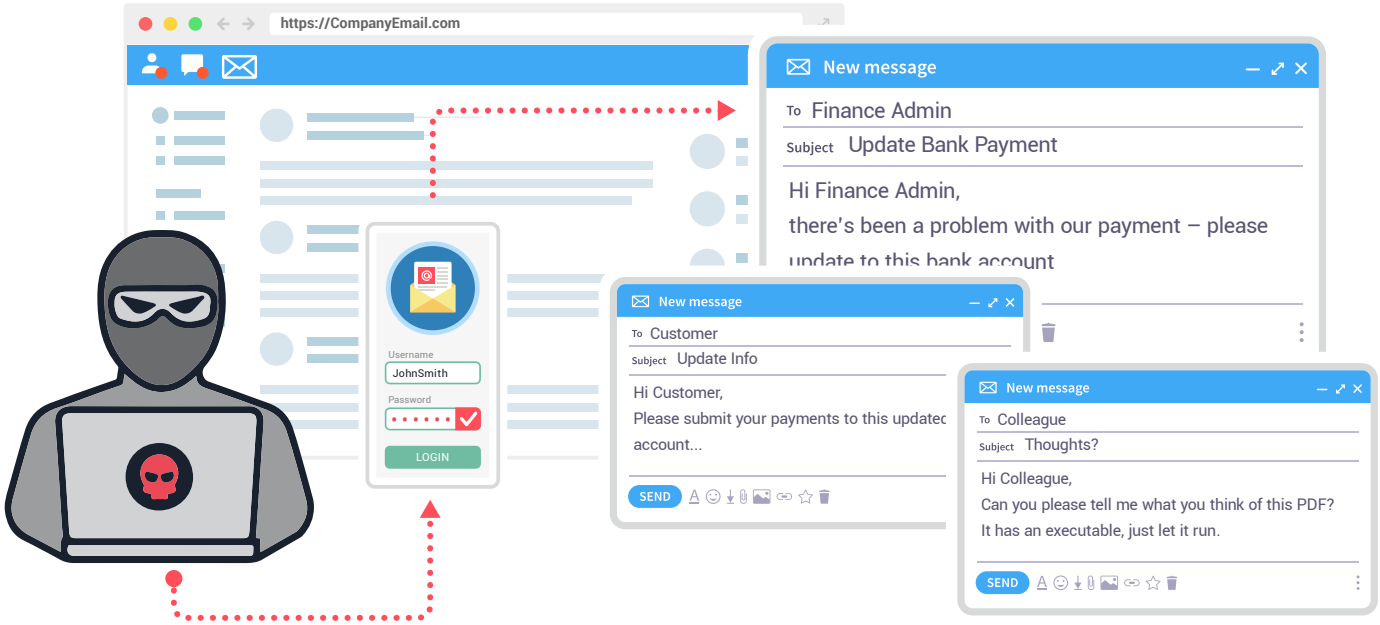


Example of an email used to commit CEO fraud.

Attackers can instruct the recipient of the email to siphon funds into threat actor-controlled mule accounts. Or, they can place a link in the email which leads to an attacker-controlled phishing page (*example: "We encourage you to **sign in** and review our company's updated COVID-19 office protocol."*). Attackers may also manipulate lower-ranking employees into initiating a bank transfer on behalf of an executive or to make certain adjustments from within an organization to make fraudulent wire transfers less detectable.

Vendor Email Compromise

While similar in concept to CEO email fraud, vendor email compromise (VEC) is a type of BEC that exploits vendor communications to control payments, most often in the form of **false invoice scams**. In typical VEC scenarios, criminals tap in to vendor emails or business systems to observe how transactions are processed. They collect information on invoice structures and communication idiosyncrasies. These details enable them to assume communication with the victim without raising suspicion.



While the financial impact from any type of BEC scam can be significant, the stakes for VEC are much higher, netting $125,000 on average. According to the US Securities and Exchange Commission in 2018, at least nine publicly-traded companies were swindled out of $100 million because of such scams.

The FBI lists **false invoice schemes** as one of the top types of BEC scams. These attacks usually target someone who works in a business's financial department. Savvy attackers will alter a legitimate invoice's bank account numbers, but leave the rest of the invoice unchanged – making it difficult to detect that it's fraudulent. However it happens, the false invoice scheme involves using phishing emails to impersonate the accountant, the vendor, or both.

Protect Your Enterprise: Addressing the Human Attack Surface

Defending against schemes that utilize sophisticated social engineering methods is easier said than done. Experts agree that humans could very well be the weakest link in any organization's security posture, particularly because of the prevalence of poor password hygiene. When passwords are reused between employees' work and personal accounts, credentials that have already been exposed in a data breach are fair game for use in BEC campaigns. Employees unwittingly enable attackers inside the organization to take note of its billing systems, vendors, and even the communication styles of employees before launching a campaign. So what can you proactively do as a security team to stem the tide?

Clear & Constant Education

Ongoing training programs arm your weakest links to become human firewalls. Reinforce learnings in an easily accessible way, such as a company-wide cybersecurity chat channel or wiki. Share specific examples of BEC attempts when you come across them and let people ask questions during regular SecOps "office hours."

In 2020, BEC costs increased from $54,000 in Q1 2020 to $80,183 in Q2, *and accounted for half of all losses in the previous year and the majority of cyber insurance claims.*

Monitor for Exposed Employee Credentials

Two factors make BEC easy to perpetrate: the enormous amount of stolen credentials available on criminal forums, and our habitual password reuse. SpyCloud's database of exposed user credentials reveals an all-time password reuse rate of 57% – and a 60% password reuse rate for breaches collected in 2020. The problem is only getting worse. The ability to know which of your employees' credentials have been exposed and force them to do a password reset observing NIST guidelines is a critical preventive measure for keeping email accounts secure.

Know Which Vendors Are Susceptible

The far-reaching consequences of BEC scams cannot be overstated. When third-party email accounts are compromised, criminals are able to monitor email communications and connect the dots from one business to the next. In fact, some of the biggest data breaches in recent memory were the result of a third-party account compromise, such as the 2013 incident in which retailer Target's systems were breached via an HVAC vendor's compromised credentials. Target was just one example; more than 56% of organizations report falling victim to a breach that was caused by a third party.

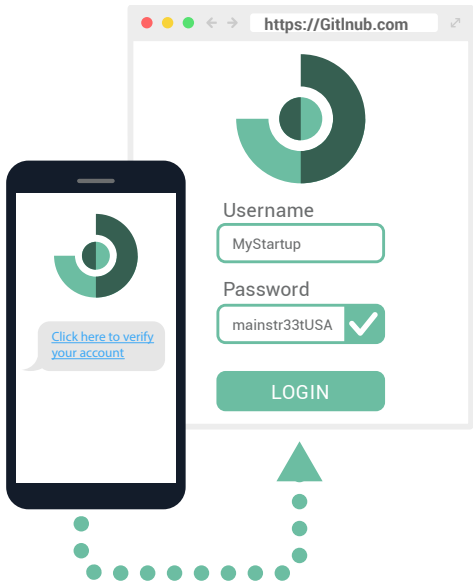
Your business does not function as an island in and of itself, nor should your approach to cybersecurity. Monitor for vendor and partner credential exposure – and even better, help them remediate. You're helping them as much as you're helping yourself.

Conclusion

Business email compromise is a bit more challenging than your average cybercrime. Worse yet, it's not going anywhere and it's not getting any less costly. In 2020, BEC costs increased from $54,000 in Q1 2020 to $80,183 in Q2 alone, and accounted for half of all losses in the previous year and the majority of cyber insurance claims.

To prevent being victimized, it's critical that organizations remain on high alert to identify BEC scams and other attacks. Beyond employee education and proactive monitoring, there are day-to-day measures everyone can take:

- **Do not share login credentials with unknown or suspicious providers (there is never a legitimate reason for a third-party to require your login credentials).**
- **Be alert to hyperlinks in emails and texts that may contain misspellings of the actual domain name, and do not click suspicious links.**



- **Verify the email address (ensure the sender's email address appears to match who it is coming from).**
- **Check in with vendors personally about updated payment details.**
- **Implement multi-factor authentication and use a unique password for every online login to protect against account takeover.**

Remember, a single compromised email account is all that a criminal requires in order to steal from your business.

The SpyCloud Difference

SpyCloud offers early detection solutions that stop ATO and BEC before it happens. Our solutions identify vulnerable employee and vendor accounts by checking them for compromise against the world's largest database of recaptured breach assets. Automated remediation scales your protection efforts without requiring additional resources, ensuring you can prevent attacks on a workforce of any size. Protect exposed accounts before criminals have a chance to use them for business email compromise and other targeted attacks.

See Your Account Takeover Risk →

Discover how many breach records are associated with your email address and your domain as a whole. Once you know, you can take action.

Employee ATO Prevention

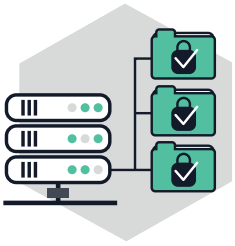
Protect your organization from breaches and BEC due to password reuse.

Learn More →

VIP Guardian

Protect your highest-risk executives from targeted account takeover.

Learn More →



Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More →

Third Party Insight

Monitor third party exposures and share data to aid in remediation.

Learn More →

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized purchases.

Learn More →