Spear Phishing: Top Threats and Trends

March 2019

Best Practices to Defeat Evolving Attacks

Spear phishing is a threat that's constantly evolving as cybercriminals find new ways to avoid detection. This report takes an in-depth look at the three most prevalent types of attacks: brand impersonation, business email compromise, and extortion.»

Barracuda
Your journey, secured.

Table of Contents

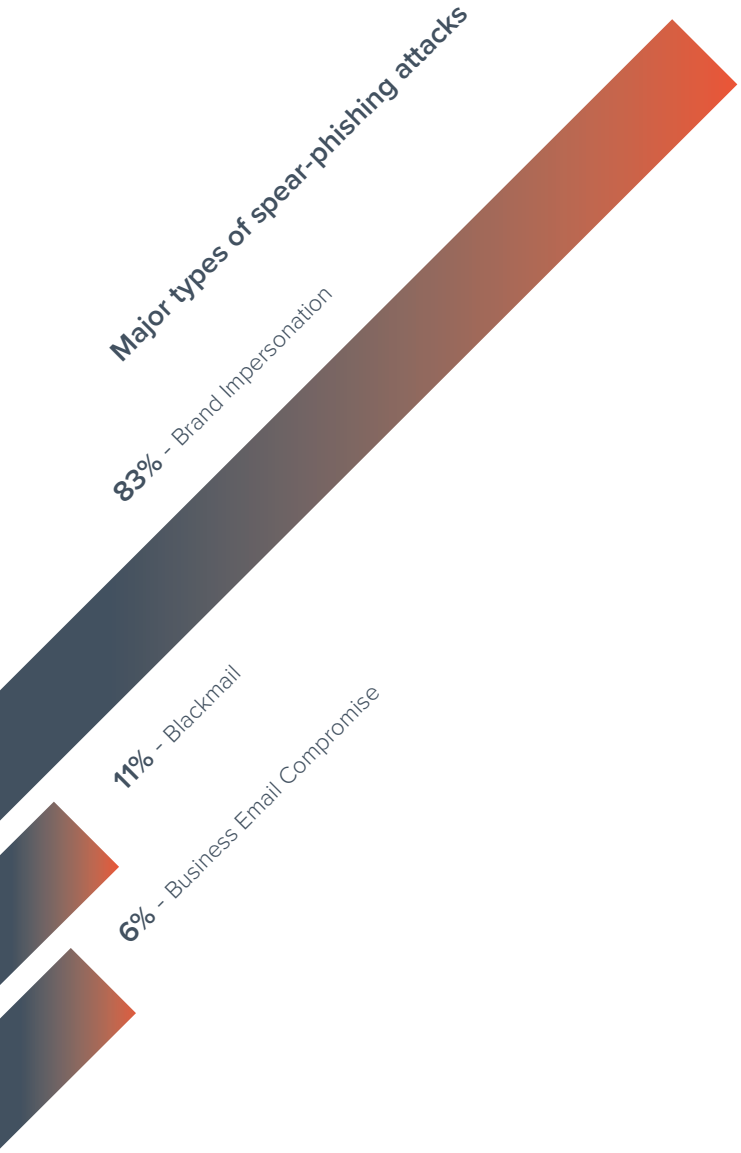
Spear Phishing

Protect your business from sophisticated, targeted and costly attacks.

Spear phishing, a highly-personalized form of email attack, is increasing in popularity with cybercriminals. Attackers research their targets and craft carefully-designed messages, often impersonating a trusted colleague, website or business. Spear-phishing emails typically try to steal sensitive information, such as login credentials or financial information, which is then used to commit fraud, identity theft and other crimes.

Designed to evade traditional email security, including gateways and spam filters, spear-phishing attacks are often sent from high-reputation domains or already-compromised email accounts. Spear-phishing emails do not always include malicious links or attachments. Since most traditional email-security techniques rely on extortion and reputation analysis, these attacks get through. Attacks typically use spoofing techniques and include "zero-day" links, URLs hosted on domains that haven't been used in previous attacks or that have been inserted into hijacked legitimate websites; they are unlikely to be blocked by URL-protection technologies. Cybercriminals also take advantage of social-engineering tactics in their attacks, including urgency, brevity and pressure, to increase the likelihood of success.

Attackers research their targets and craft carefully-designed messages...»



Social-Engineering Tactics Continue To Evolve

Barracuda researchers evaluated more than 360,000 spear-phishing emails in a three-month period, identifying and analyzing three major types of attacks:

Brand impersonation

These types of spear-phishing attacks, designed to impersonate well-known companies and commonly-used business applications, are by far the most popular because they are well designed as an entry point to harvest credentials and carry out account takeover. Brand impersonation attacks are also used to steal personally-identifiable information, such as credit card and Social Security numbers. Microsoft and Apple are the most-impersonated brands in spear-phishing attacks.

Business email compromise

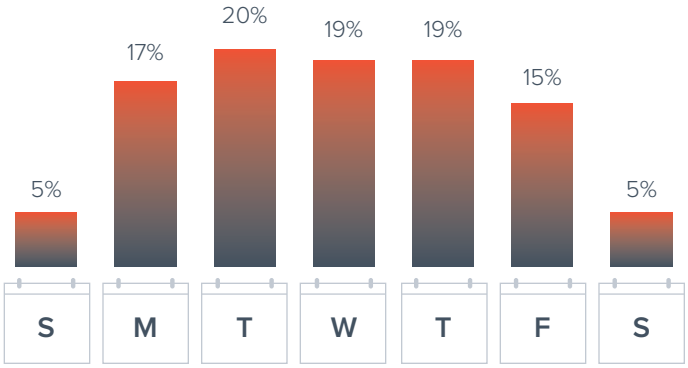
Also known as CEO fraud, whaling and wire-transfer fraud, business email compromise makes up only a small percentage of spear-phishing attacks, but has caused more than $12.5 billion in losses since 2013, according to the FBI. Scammers impersonate an executive, partner or another trusted person in an email, requesting a wire transfer or personally-identifiable information from finance department employees or others with access to sensitive information. Gmail accounts are used to launch 30% of business email compromise attacks.

Extortion

In most extortion scams, which includes sextortion attacks, cybercriminals claim to have a compromising video, images or other content allegedly recorded on the victim's computer, and threaten to share it with all their email contacts, unless they pay up. With about 1 in 10 spear-phishing emails being a sextortion attack, employees are twice as likely to be the target of extortion than business email compromise.

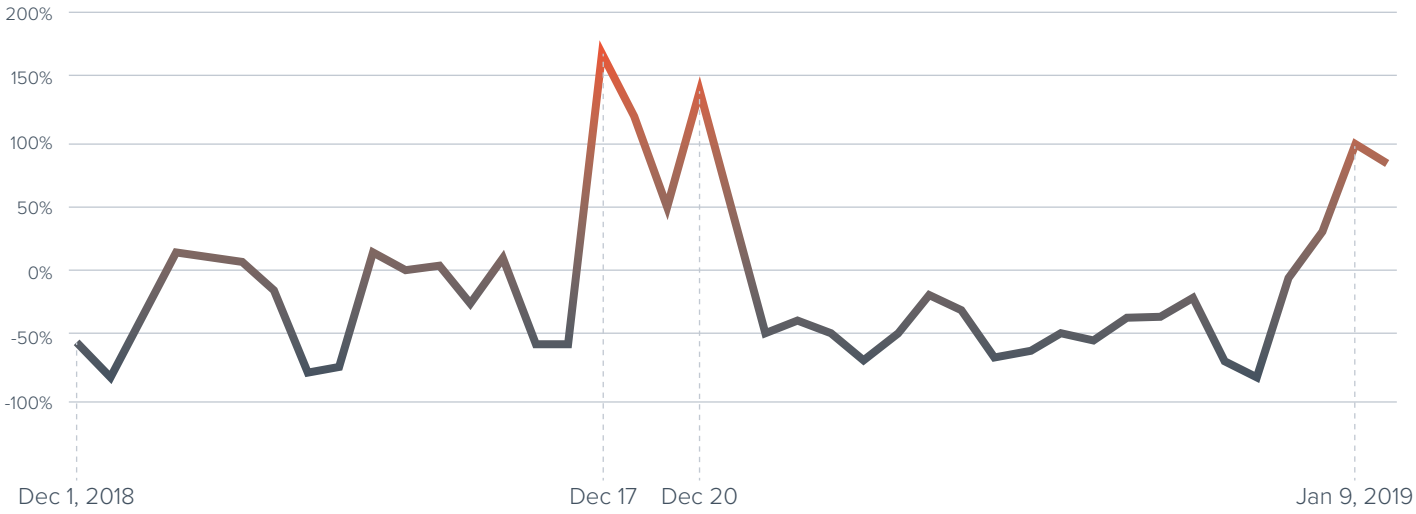
Cybercriminals Carefully Time Attacks

While malicious emails can arrive any day of the week, spear-phishing attacks peak between Tuesday and Thursday, with 1 in 5 emails being sent on Tuesday. Given the fact that businesses are the typical targets, it's not surprising that weekend days make up the lowest percentage of attacks. Scammers send the majority of emails on business days to make the attacks more convincing.



Spear phishing attacks peak mid-week

Spear-Phishing Attacks Spike Around Holidays



Seasonality dramatically impacts the number of spear-phishing attacks. Cybercriminals try to exploit security weaknesses and other potential vulnerabilities around holidays and other events, such as tax season. The week before Christmas, the number of spear phishing attacks spiked to more than 150% above average. The number of attacks dropped significantly in the weeks after the holiday.

Cybercriminals know the end of the year is flooded with a lot of activity, including email communications, and try to take advantage by launching attacks at distracted and busy employees. IT and security staff resources are typically stretched at the holidays, as many people take vacation time, and they may not be as vigilant or have as much time to monitor potential phishing attacks. Cybercriminals try to exploit this temporary weakness in security. Scammers deliberately target seasonal workers, contractors and other temporary employees, who can be less familiar with company business practices and security policies and more likely to fall victim to an attack.

Staying Ahead Of Attacks

This report takes an in-depth look at brand impersonation, business email compromise and extortion, including providing detailed information about how the most popular spear-phishing scams work, the reasons traditional email security can't stop the attacks and the latest targets and techniques being focused on by cybercriminals. Best practices and prevention measures that every business should consider to protect against these sophisticated, targeted and costly attacks are also recommended, including a combination of purpose-built-technology and user-security training.

Brand Impersonation

Top brands at high risk for attacks.

Key Findings

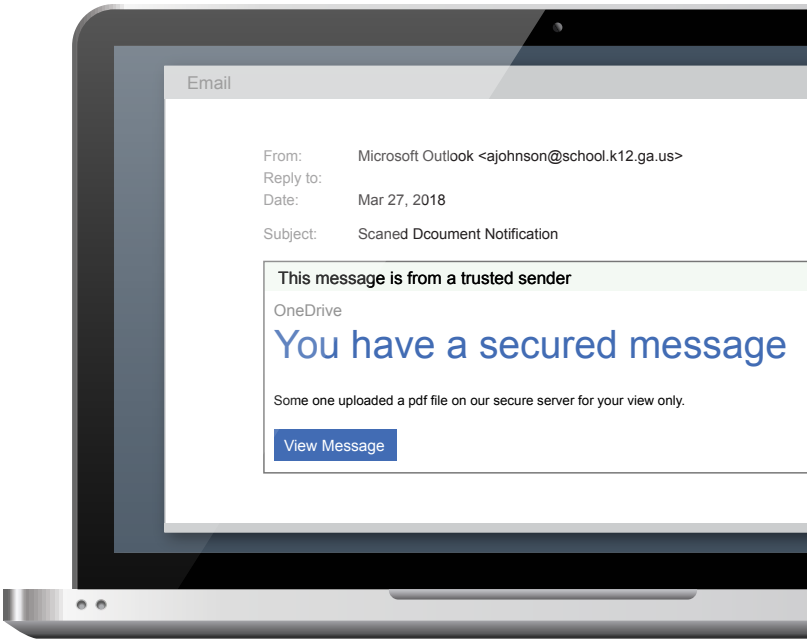
- 83% of spear-phishing attacks involve brand impersonation.
- Sophisticated spear-phishing attacks are used to steal account credentials.
- Nearly 1 in 5 attacks involve impersonation of a financial institution.

Nearly 1 in 5 attacks involve impersonation of a financial institution. »

How Brand-Impersonation Attacks Work

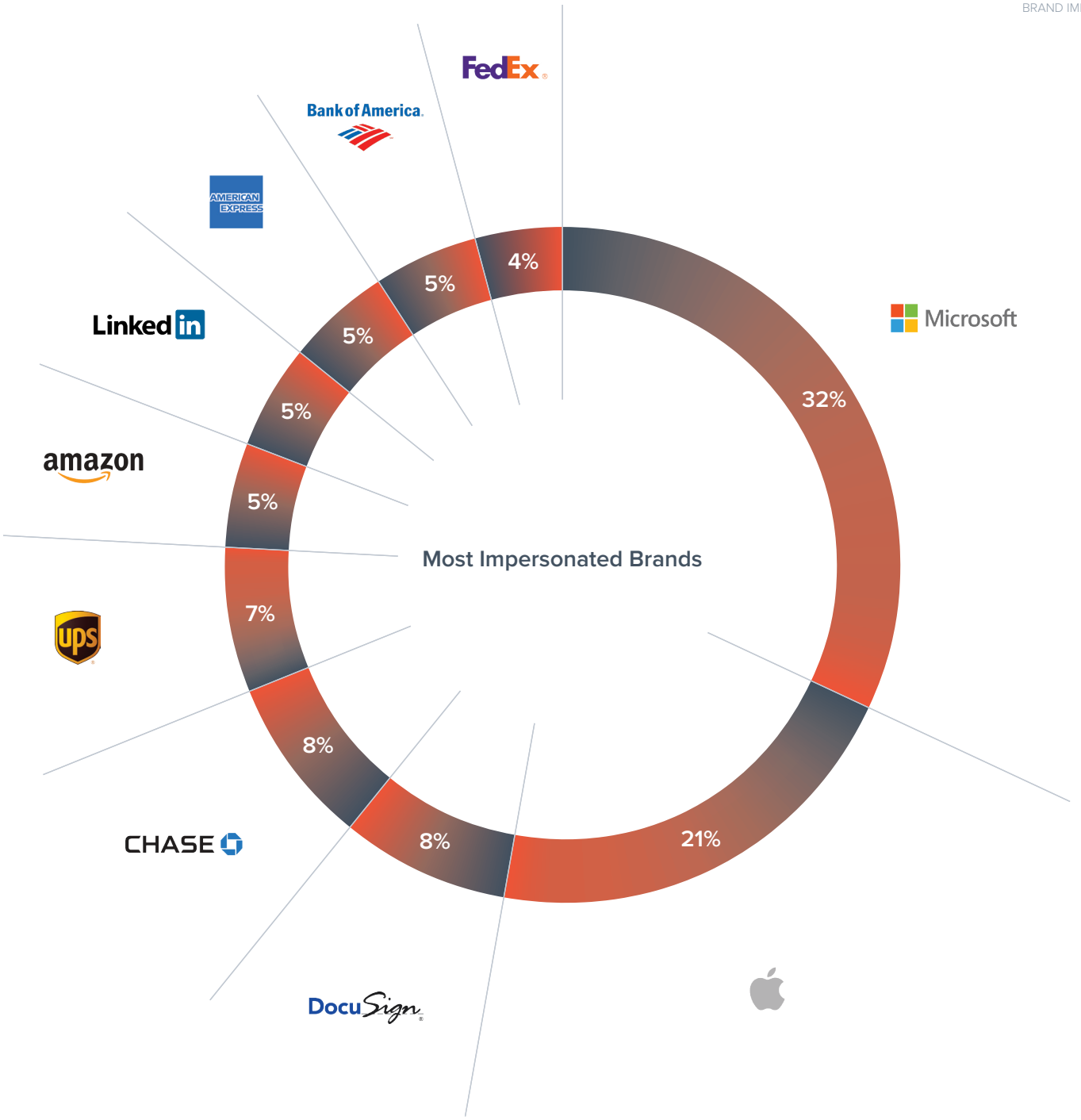
In most brand-impersonation attacks, scammers use email to impersonate a trusted entity, such as a well-known company or a commonly-used business application. Typically, attackers try to get recipients to give up account credentials or click on malicious links. Attackers often use domain-spoofing techniques or lookalike domains to make their impersonation attempts convincing.

Using carefully-designed templates that impersonate top brands, cybercriminals send an email claiming your account has been frozen and giving you a link to reset your password. Sometimes, these emails ask you to review your account or a document. If you click on the link provided, you'll arrive at a phishing website; it looks legitimate, but it's designed to harvest your login credentials. If you enter your username and password on the fake site, the crooks then gain access to your real account, and they can steal confidential data, conduct financial fraud and launch more targeted attacks within your organization.



Why Traditional Email Security Can't Stop Attacks

- Brand-impersonation attacks often bypass traditional email security because they originate from high-reputation senders. Since most traditional email-security techniques rely on block-list and reputation analysis, these attacks get through.
- Brand-impersonation attacks often include "zero-day" links. These URLs are typically hosted on domains that weren't used in previous malicious attacks or that have been inserted into hijacked legitimate websites; they are unlikely to be blocked by URL-protection technologies.
- Attackers use compromised accounts to launch some of these attacks. With the fraudulent email coming from a legitimate account, it's likely to be considered safe by gateways.
- Employees often fall victim to these types of spear-phishing attacks because the email appears to come from a colleague or trusted business application they work with every day. Whether through spoofing or the use of a compromised account, they are difficult to detect as fraud.



The Latest Targets and Techniques

- Impersonating Microsoft is one of the more common techniques used by cybercriminals trying to take over accounts.
- Scams that impersonate Apple vary. In some attacks, cybercriminals send an email about a recent alleged iTunes purchase, asking for credit card details to cancel the order and provide a refund. The stolen information is used to commit financial fraud.
- Financial institutions are impersonated in nearly 1 in 5 attacks. Cybercriminals try to steal bank account login details. Finance department employees are heavily targeted, as they are most likely to deal with banks and other financial institutions.

Extortion

Sextortion scams twice as likely as business email compromise attacks.

Key Findings

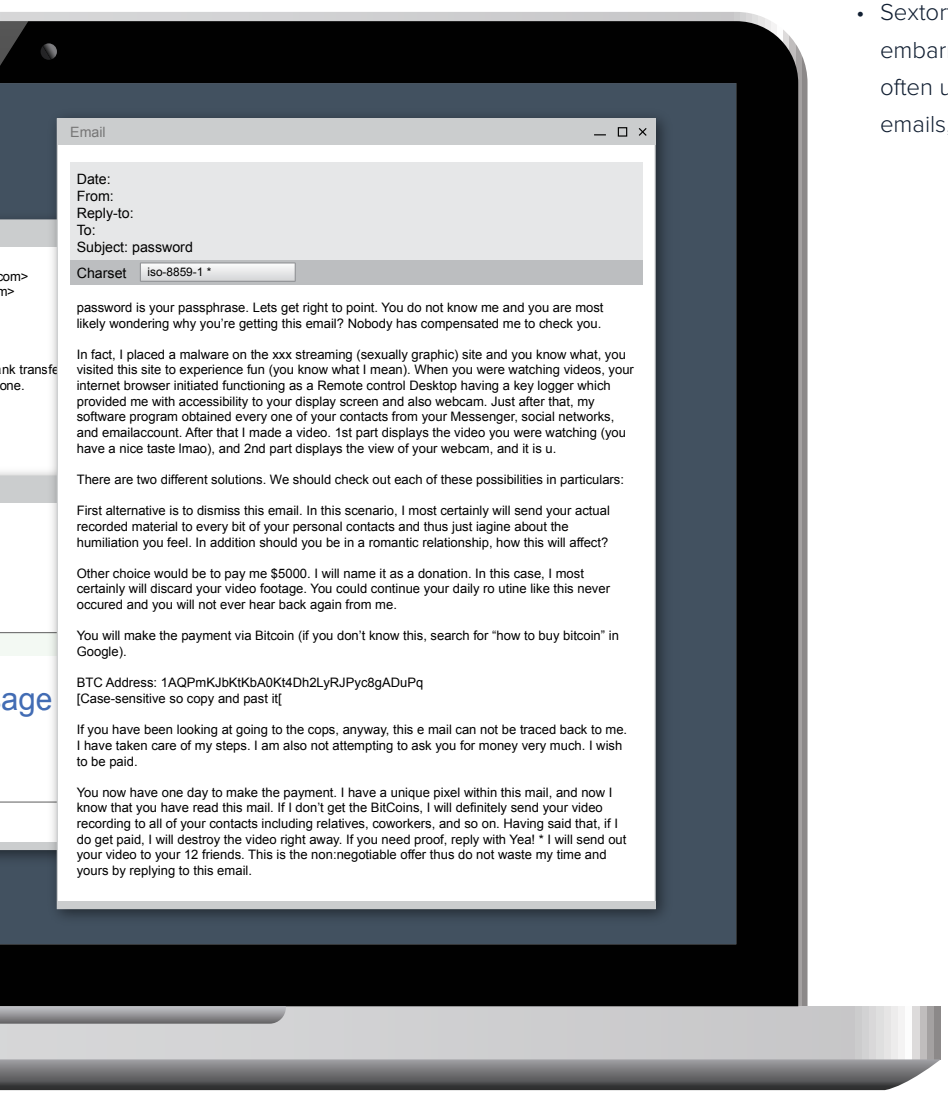
- Sextortion scams, a form of extortion, are increasing in frequency, becoming more sophisticated and bypassing email gateways.
- 1 in 10 spear-phishing emails are sextortion attacks.
- The majority of subject lines on sextortion emails contain some form of security alert.
- Attackers often include the victim's email address or password in the subject line.

1 in 10 spear-phishing emails are sextortion attacks.»

How Sextortion Scams Work

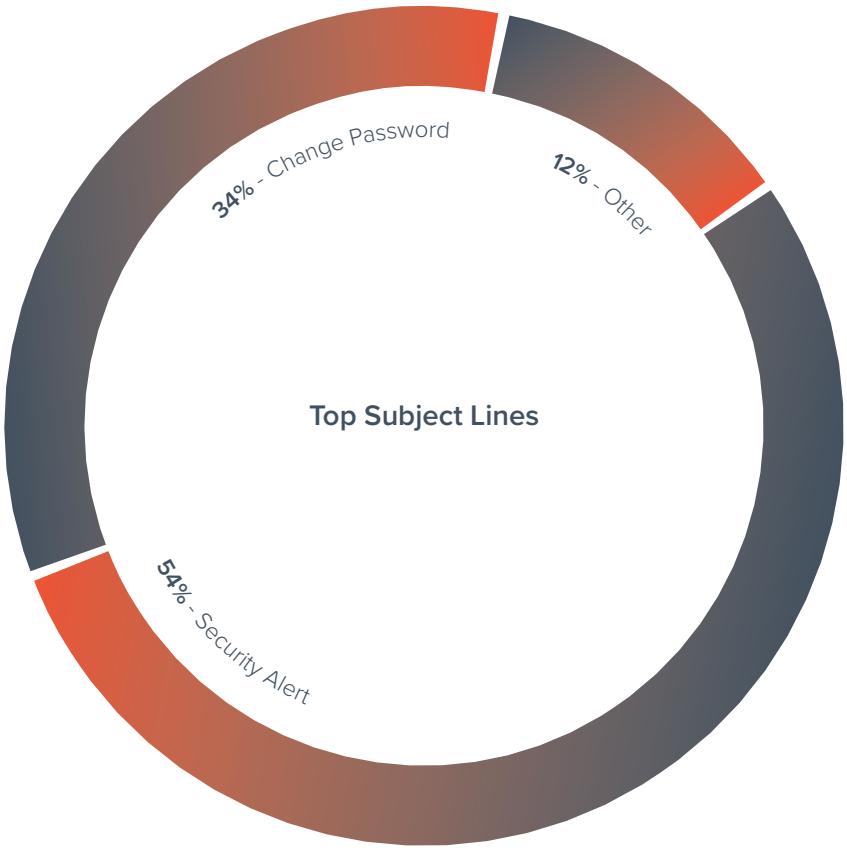
In most sextortion scams, attackers leverage usernames and passwords stolen in data breaches, to send threatening emails and trick victims into giving them money. Often, attackers spoof their victim's email address, pretending to have access to it, to make the attack even more convincing.

The scammers claim to have a compromising video, images or other content allegedly recorded on the victim's computer, and threaten to share it with all their email contacts unless they pay up. Typically, the ransom is a few hundred dollars; cybercriminals prefer Bitcoin payments because they can't be traced.



Why Traditional Email Security Can't Stop Attacks

- Scammers continue to evolve their email-fraud techniques, including using social-engineering tactics in sextortion attacks.
- Sextortion emails don't usually contain malicious links or attachments found by traditional gateways.
- Attackers have started to vary and personalize the content of the emails, making it difficult for spam filters to stop them.
- Sextortion emails that end up in inboxes typically do so because they originate from high-reputation senders and IPs; cybercriminals use already-compromised Office 365 or Gmail accounts.
- Sextortion scams are under reported due to the intentionally-embarrassing and sensitive nature of the threats. IT teams are often unaware of these attacks; employees don't report the emails, regardless of whether they pay the ransom.



More than 60% of the sextortion emails analyzed contained 30 common subject lines.

- Attackers often include the victim's email address or password in the subject line to get them to open and read the email.
- In addition to security alerts and requests to change passwords, other frequently-used subject lines include references to a customer service ticket number or incident report.
- Occasionally, attackers are more straightforward, using threatening subject lines.

Examples of Sextortion Subject Lines

- Name@emailaddress.com was under attack change your access data.
- Your account has been hacked you need to unlock.
- Your account is being used by another person.
- Change your password [password] immediately your account has been hacked.
- Cybercriminals know your password [password] password must be changed now.
- You are my victim.
- Better listen to me.
- This is my last warning name@emailaddress.com.

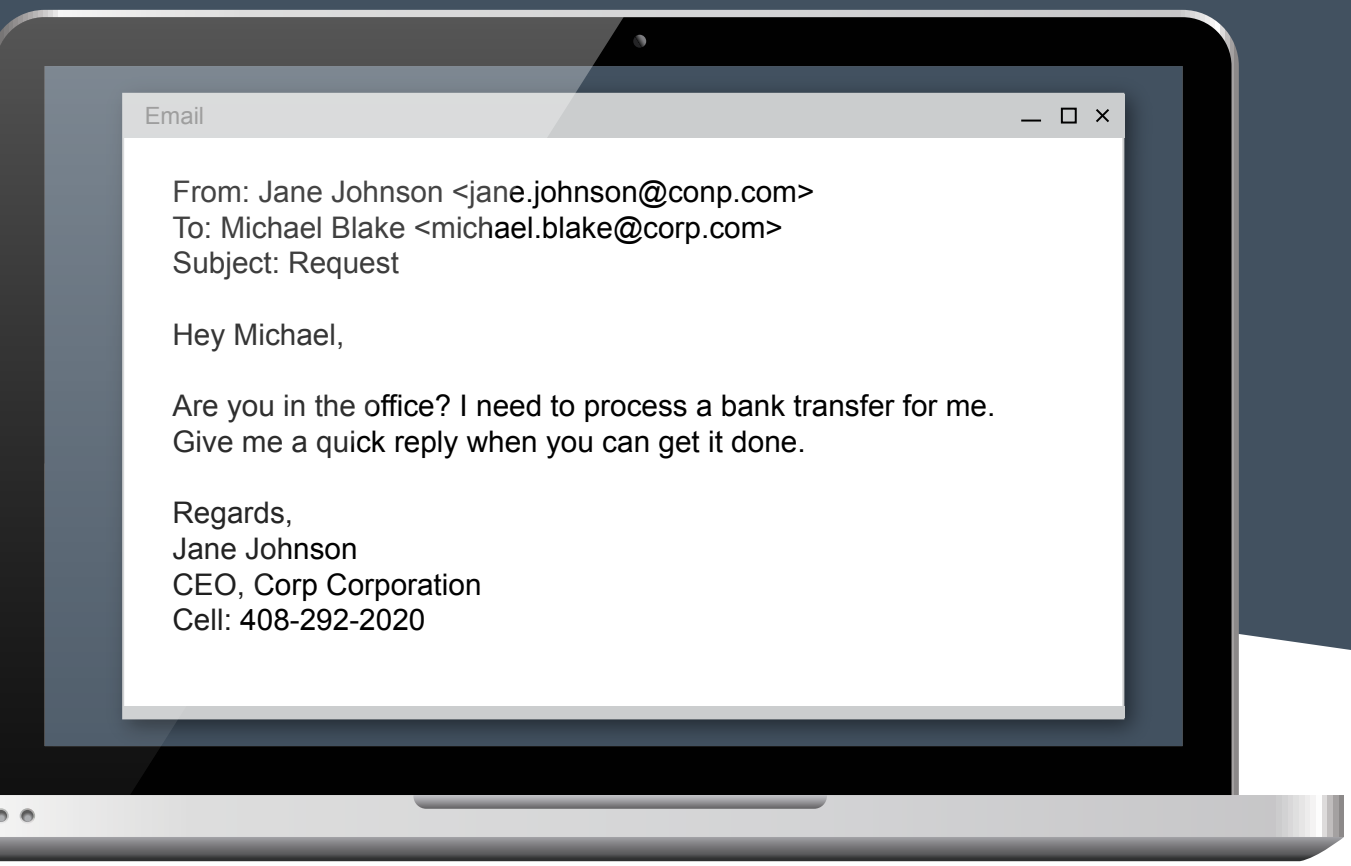
Business Email Compromise

Cybercriminals use urgency and brevity to steal billions every year.

Key Findings

- Business email compromise attacks make up only 6% of spear-phishing attacks but have caused more than $12.5 billion in losses since 2013, according to the FBI.
- Just 10 popular email domains are used to launch 62% of attacks.
- Subject lines on the majority of attack emails try to establish rapport or a sense of urgency; many imply the topic has been previously discussed.
- Cybercriminals adjust their email techniques to more effectively target users in different industries.
- Finance department employees are heavily targeted due to their access to banking and personal information.

...more than $12.5 billion in losses since 2013...»



How Business Email Compromise Attacks Work

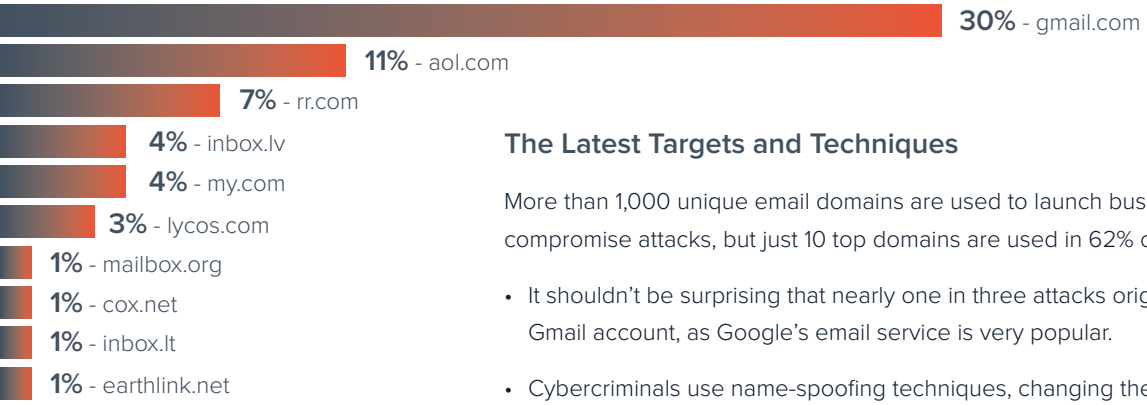
In most business email compromise attacks (also called CEO fraud, whaling and wire-transfer fraud), scammers impersonate an employee within the organization. Attackers use spoofing, social-engineering tactics and compromised accounts to trick employees into disclosing sensitive financial and personal information. Often, these highly-personalized email attacks do not contain malicious links or attachments, making them very difficult to detect with traditional email security.

Cybercriminals spend time researching an organization and its employees before launching an attack. They impersonate an executive or other employee in an email, requesting a wire transfer or personally-identifiable information from finance department employees and others with access to sensitive information. Once the money has been transferred to a fraudulent account, it's usually impossible to get it back.

Why Traditional Email Security Can't Stop Attacks

- Attacks are carefully designed and aren't sent as mass campaigns, so they aren't blocked as spam.
- The email services that are being used to launch attacks are assigned high-reputation scores, which helps cybercriminals get the emails through security gateways.
- Business email compromise attacks do not contain malicious links or attachments, making them very difficult to detect and block with traditional email security.
- Attacks may originate from compromised email accounts, making them even more difficult to detect.
- Domain spoofing and display-name spoofing are used to make the impersonations convincing.
- Cybercriminals also use social-engineering tactics, including brevity, urgency, personalization and pressure, to increase the likelihood of success.

Top domains used to launch BEC attacks

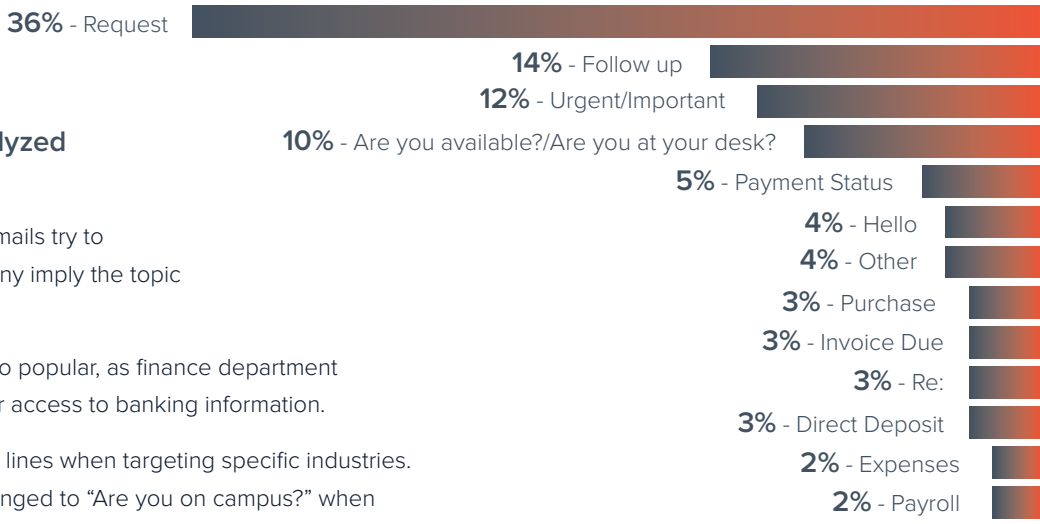


The Latest Targets and Techniques

More than 1,000 unique email domains are used to launch business email compromise attacks, but just 10 top domains are used in 62% of all attacks.

- It shouldn't be surprising that nearly one in three attacks originate from a Gmail account, as Google's email service is very popular.
- Cybercriminals use name-spoofing techniques, changing the display name on Gmail and other email accounts to make the email appear to come from a company employee. This tactic can be especially deceiving to those reading the email on a mobile device.

Top subject lines in BEC attacks



Nearly 60% of the attack emails analyzed contained 50 common subject lines.

- Subject lines on more than 70% of attack emails try to establish rapport or a sense of urgency; many imply the topic has been previously discussed.
- Subject lines about financial matters are also popular, as finance department employees are heavily targeted due to their access to banking information.
- Scammers customize popular email subject lines when targeting specific industries. For example, "Are you at your desk?" is changed to "Are you on campus?" when education-sector users are targeted.

Best Practices

Top email-defense strategies to protect against spear phishing

Preventing spear-phishing attacks requires the right combination of technology and user-security training. Here's a variety of best practices every business should consider to protect against these sophisticated, targeted and costly attacks.»

Take advantage of artificial intelligence

Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against spear-phishing attacks, including business email compromise, brand impersonation and sextortion. Deploy purpose-built technology that doesn't solely rely on looking for malicious links or attachments. Using machine learning to analyze normal communication patterns within your organization allows the solution to spot anomalies that may indicate an attack.

Don't rely solely on traditional security

Protect against attacks that use "zero-day" links. Don't rely on traditional email security that uses block-list for spear-phishing and brand-impersonation detection. A reputation analysis of URLs doesn't provide protection against some attacks because "zero-day" links are often hosted on domains that weren't used in previous malicious attacks or that have been inserted into legitimate websites.

Deploy account-takeover protection

Many spear-phishing attacks originate from compromised accounts; be sure scammers aren't using your organization as a base camp to launch these attacks. Deploy technology that uses artificial intelligence to recognize when accounts have been compromised and that remediates in real time by alerting users and removing malicious emails sent from compromised accounts.

Implement DMARC authentication and reporting

Domain spoofing is one of the most common techniques used in impersonation attacks. DMARC authentication and enforcement can help stop domain spoofing and brand hijacking, while DMARC reporting and analysis helps organizations accurately set enforcement.

Use multi-factor authentication

Multi-factor authentication, also called MFA, two-factor authentication and two-step verification, provides an additional layer of security above and beyond username and password, such as an authentication code, thumb print or retinal scan.

Train staffers to recognize and report attacks

Educate users about spear-phishing attacks by making it a part of security-awareness training. Ensure staffers can recognize these attacks, understand their fraudulent nature and know how to report them. Use phishing simulation for emails, voicemail and SMS to train users to identify cyberattacks, test the effectiveness of your training and evaluate the users most vulnerable to attacks. Help employees avoid making costly mistakes by creating guidelines that put procedures in place to confirm requests that come in by email, including making wire transfers and buying gift cards.

Conduct proactive investigations

Given the highly-personalized nature of spear-phishing emails, employees may not always recognize malicious intent or report it to IT. Conduct regular searches to detect emails with content known to be popular with cybercriminals, including subject lines related to password changes and security alerts. Many spear-phishing emails originate from outside North America or Western Europe. Evaluate where your delivered mail is coming from, review any of suspicious origin, and remediate.

Maximize data-loss prevention

Use the right combination of technologies and business policies to ensure emails with confidential, personally-identifiable and other sensitive information are blocked and never leave the company.

Barracuda®
Your journey, secured.

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.