Spear Phishing: Top Threats and Trends

Vol. 3 November 2019

Defending against business email compromise attacks

Business email compromise makes up only a small percentage of spear-phishing attacks, but has caused more than $26 billion in losses in the last four years, according to the FBI. This in-depth report takes a look at the latest tactics used by scammers and how to protect your business.»

Barracuda
Your journey, secured.

Table of Contents

Key findings 1

Overview of spear-phishing attacks 2

BEC tactic: Carefully-timed attacks 4

BEC tactic: Targeted attacks from trusted sources 5

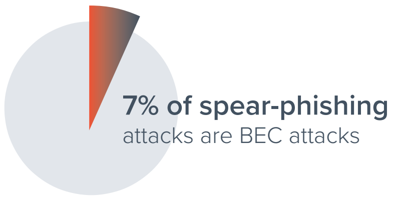
BEC tactic: Short and urgent messages 7

Examples of BEC attacks 9

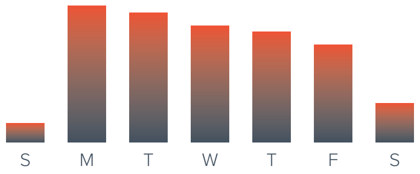
The impact of spear-phishing attacks 12

Protecting against business email compromise attacks 13

Key findings

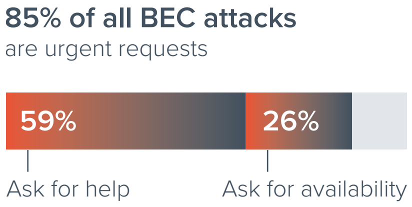


Business email compromise (BEC) makes up only **7% of all spear-phishing attacks**, but has caused more than **$26 billion in losses in the last four years**, according to the FBI.

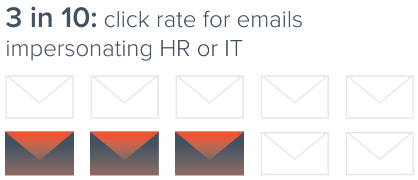


91% of BEC attacks take place on weekdays. Attackers try to mimic business behavior as much as possible, often sending emails during the compromised account's typical working hours to make them appear more convincing and trustworthy.

Business email compromise attacks are low volume and highly targeted. The average attack targets no more than **6 employees**.



85% of all business email compromise attacks are urgent requests that are designed to get a fast response. **59% ask for help, and 26% ask about availability.**



Business email compromise attacks have high click rates. **3 in 10 spear-phishing emails** successfully trick a user into clicking when the email impersonates the organization's HR or IT department.

An average of
$270,000 per org
was lost due to attacks
in the last 12 months

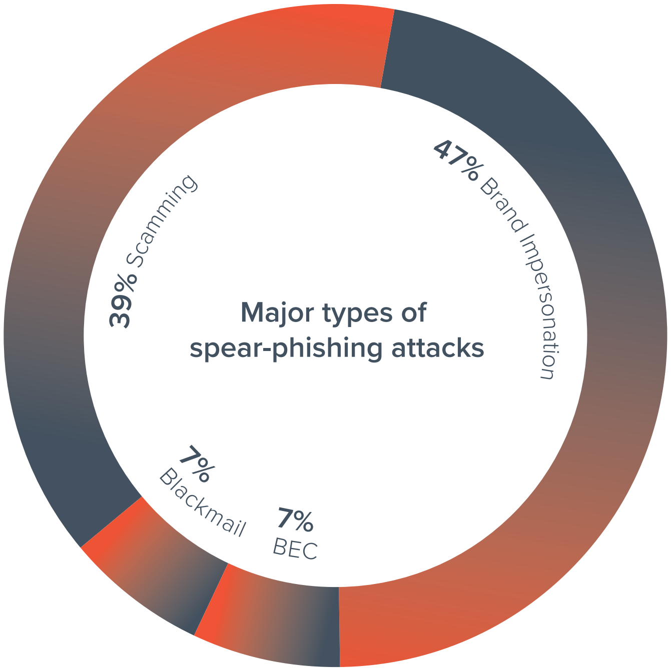
The costs and damages associated with spear-phishing attacks are high. **In the last 12 months, the average amount lost per organization due to spear-phishing attacks was $270,000**. There are a wide range of financial impacts from attacks, including business interruption, reduced productivity, data loss, regulatory fines and brand damage.

Overview of spear-phishing 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 block-list 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 spear-phishing attacks, including urgency, brevity and pressure, to increase the likelihood of success.



Barracuda researchers recently analyzed more than 1.5 million spear-phishing emails and identified four main types of spear-phishing attacks:

Brand Impersonation

This type of spear-phishing, designed to impersonate well-known companies and commonly-used business applications, makes up nearly half of all attacks. They are the most popular type of attack 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. In the business world, attackers like to impersonate popular business applications, such as DocuSign. Microsoft is impersonated in **56% of these types of spear-phishing attacks.**

Scamming

These attacks are designed to capture private, sensitive and personally-identifiable information, such as bank account, credit card and Social Security numbers. Attackers trick victims into disclosing the information and then use it to defraud them, steal their identities or both. Attacks are executed using a variety of hooks, such as lottery winnings, unclaimed packages, donation solicitations and other tactics.

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 **$26 billion in losses in the last four years, according to the FBI**. Scammers impersonate an employee in the organization, a partner, vendor or other trusted person in an email, requesting a wire transfer or personally identifiable information from finance department employees or others with access to sensitive information.

These highly-targeted attacks, which are particularly difficult to detect because they rarely include a URL or malicious attachment, are the focus of this report.

Extortion

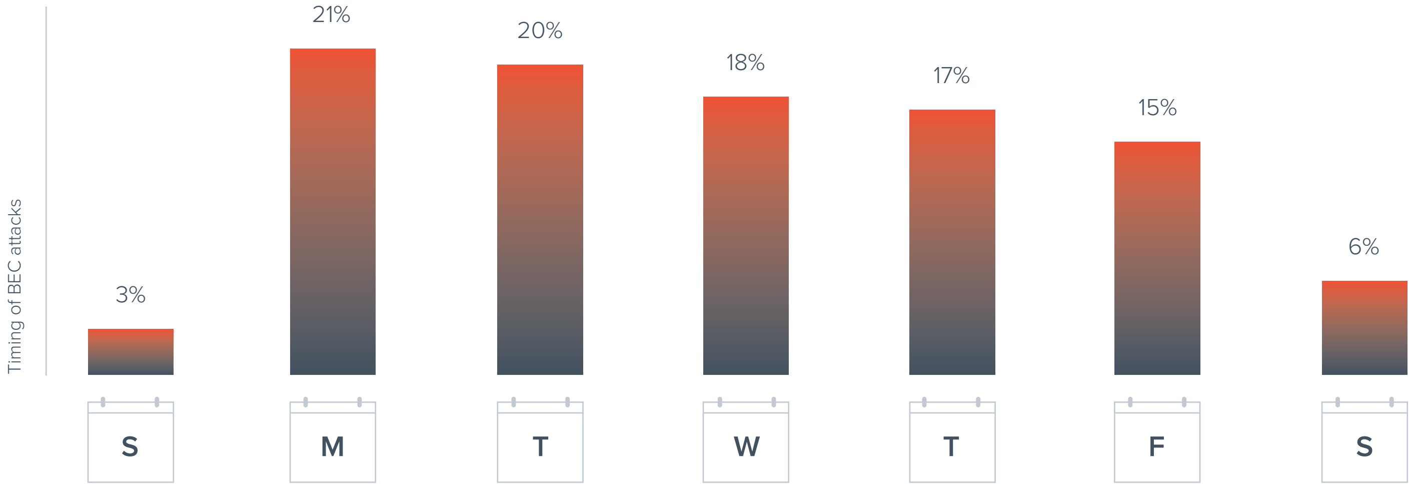
Most extortion scams are sextortion attacks. Cybercriminals claim to have a compromising video, images or other content allegedly recorded on the victim's computer, and threaten to share it with all their email contacts, unless they pay up. Employees are equally likely to be the targets of extortion scams and business email compromise attacks.

BEC tactic: Carefully-timed attacks

Cybercriminals carefully time their BEC attacks. While malicious emails can arrive any day of the week, **91% of BEC attacks take place on weekdays**. Attackers try to mimic business behavior as much as possible, often sending emails during the compromised account's typical working hours to make them appear more convincing and trustworthy. Given the fact that businesses are the typical targets, **it's not surprising that weekends make up less than 10% of attacks**.

Seasonality dramatically impacts the number of spear-phishing attacks. **For example, the number of BEC emails sent on Fourth of July weekend was 94% below average. Similarly, Labor Day weekend saw a drop of 34%**.

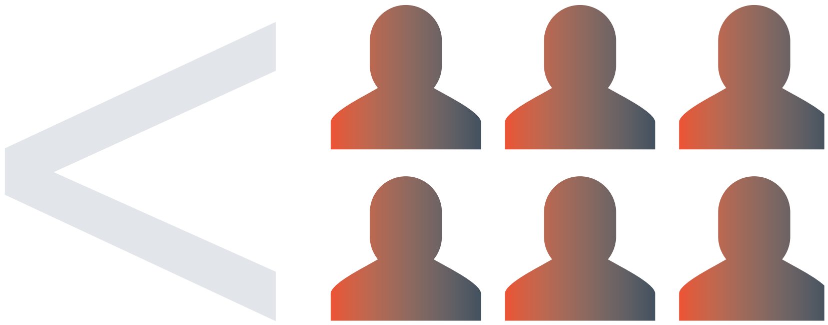
Other times, however, cybercriminals use holidays and seasonal events, such as tax season and back to school, to ramp up their efforts and try to exploit security weaknesses and other potential vulnerabilities. Along those lines, in September, there was a spike in BEC attacks on educational institutions. Back to school is a busy time, with a lot of communication sent out and a lot of new users and staffers that are easy targets for spear-phishing attacks. Cybercriminals try to exploit this weakness in security.



BEC tactic: Targeted attacks from trusted sources

Business email compromise attacks are low volume and highly targeted. **The average attack targets no more than 6 employees**. Attackers use email-domain and display-name spoofing to impersonate an executive or other employee in an email, requesting a wire transfer or personally-identifiable information from finance department employees or others with access to sensitive information.

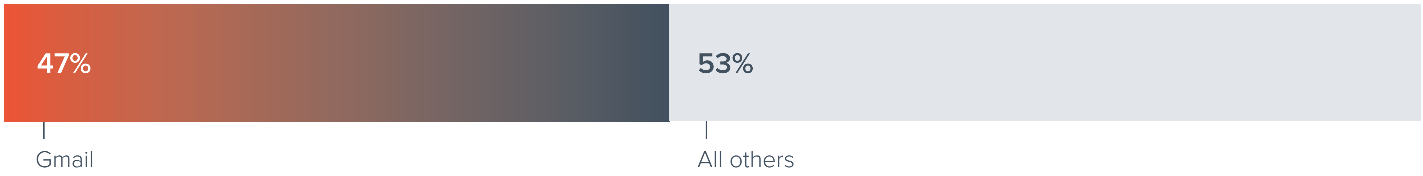
Most BEC attacks are low volume



The average attack targets no more than **6 employees**

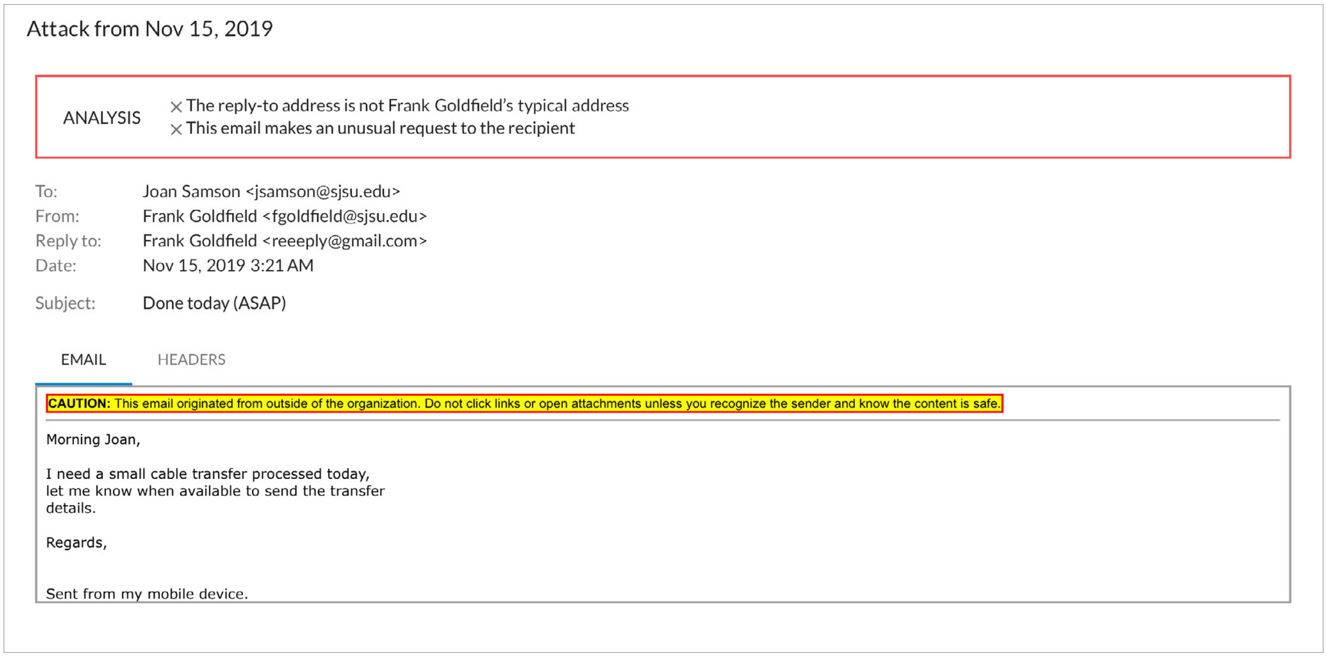
Sending a small number of emails, as opposed to spamming a large number of potential victims, also means that hackers are able to monitor responses from their victims. Hackers want a response from their victim before making a request for a wire transfer or personal information. Along those lines, an overwhelming majority of business email compromise attacks initially include a very simple message, such as “Do you have a minute?” or “I need your help.”

Domains used in BEC attacks



Barracuda researchers analyzed more than 1,000 email domains used to launch spear-phishing attacks. Hackers often use popular, free, web-based email services, such as Gmail and Yahoo to launch attacks. Gmail is by far the most common email domain used in business email compromise attacks. Attacks may also originate from compromised email accounts, making them even more difficult to detect.

An example of email-domain and display-name spoofing



Attack from Nov 15, 2019

ANALYSIS
× The reply-to address is not Frank Goldfield's typical address
× This email makes an unusual request to the recipient

To: Joan Samson <jsamson@sjsu.edu>
From: Frank Goldfield <fgoldfield@sjsu.edu>
Reply to: Frank Goldfield <reeeply@gmail.com>
Date: Nov 15, 2019 3:21 AM

Subject: Done today (ASAP)

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Morning Joan,

I need a small cable transfer processed today,
let me know when available to send the transfer
details.

Regards,

Sent from my mobile device.

With email-domain spoofing, hackers sometimes provide a different reply-to address, so that their victims can engage in the conversation. **In 4% of all business email compromise attacks, the reply-to email was different from the sender's email**.

With display-name spoofing, attackers create a Gmail or other email account and impersonate someone else by changing the display name. This is one of the reasons web-based email services are frequently used in business email compromise attacks. This tactic can be especially deceiving to those reading the email on a mobile device, as it's the display name and not the actual email address that is shown.

BEC tactic: Short and urgent messages

Most emails sent as part of business email compromise attacks are urgent requests that are designed to get a fast response. Often, requests appear to come from a senior executive or trusted colleague.

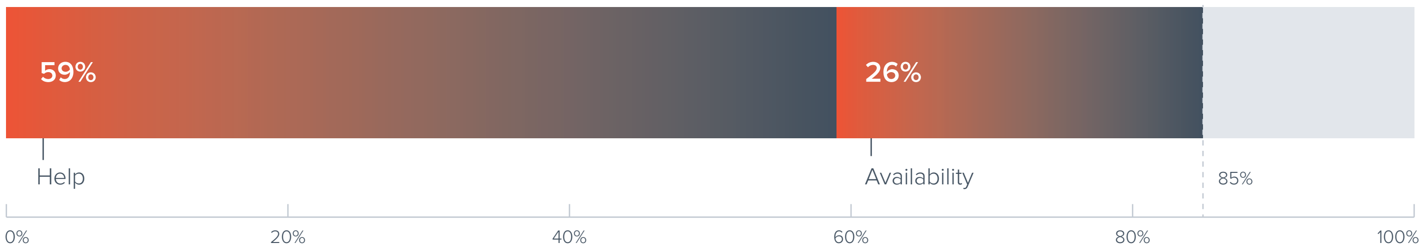
Top subject lines in BEC attacks

Request	30%
Urgent	18%
Follow up	12%
Change direct deposit	8%
Hi/Greetings	5%
Gift cards	4%
Are you available?	4%

Messages are concise, generic and crafted to trigger a sense of urgency with victims; many imply the topic has been previously discussed. Almost half of all BEC emails contained words like “Urgent” or “Request” in the subject line. Their repeated use suggests they are effective.

In some instances, hackers personalize the subject line; 1% of BEC attacks used either the individual’s name or the company’s name in the subject line.

Messages in BEC attacks



Hackers keep the messages short and simple. The two most common approaches are to request help or ask about availability. Once the victim has responded and trust has been established, the actual request will follow, such as making a wire transfer, buying gift cards or reviewing a document.

Only 3% of BEC attacks contain a URL or an attachment. Lack of a malicious payload in BEC attacks makes them hard to detect with traditional filtering technology. Most emails that did include URLs were either asking for payments or to verify information. A lot of the time, attackers impersonate the HR, IT or finance team, instead of an individual.

Examples:

> *"We had a direct deposit issue earlier this week. Can you verify that your information is correct online <URL>.*
> *Please confirm as soon as you can. Thanks, accounting team"*

> *"Your statement is attached. Please remit payment at your earliest convenience <URL>.*
> *Thank you for your business, we appreciate it very much"*

Sometimes, like in this example, hackers include the company's URL in their email signature to make the message appear more legitimate:

> *"Have you got a minute? I need you to complete a task for me discreetly.*
> *p.s. I am in a meeting now and can't talk so just reply."*
>
> *<NAME>*
> *CEO, Acme Corp*
> *<Company URL>*
> *Sent from <NUMBER> wireless"*

Examples of BEC attacks

The three most common business email compromise attacks include urgent requests, payroll scams and gift-card scams. **These types of attacks make up about 97% of all BEC scams**.

Urgent requests

Urgent requests, making up 85% of all business email compromise attacks, are by far the most popular approach used by hackers. **More than half of attacks – 59% – ask for help. More than ¼ of attacks – 26% – ask if the person is available**.

These attacks use subject lines like “Hi,” “Quick request” and “Urgent.” The content of the email is usually very short and designed to get a response.

> *“Are you available?”*
> *“I need your assistance”*

38% of attacks that request urgent help also claim that a sender is currently in a meeting and therefore unable to talk. It’s also a common tactic for hackers to make emails appear to have originated from mobile devices, to help support the claim of the sender being remote and unavailable.

> *“Have you got a minute? I need you to complete a urgent task for me discreetly.*
>
> *P.S. I am in a meeting now and can’t talk, so just reply*
>
> *Thank you*
>
> *sent from <NUMBER> wireless phone”*

Sometimes, hackers request the personal phone numbers of their victims. In these cases, they are very likely to move their attack to the cell phones, sending malicious links, files or requests.

> *“Are you available to work on an urgent request for me today? send me your personal cell phone number”*

Although weekends aren’t the most popular days for BEC attacks, some hackers still try to take advantage of them. An urgent request from an executive over the weekend is designed to get a fast reaction from a distracted employee.

> *“Hello. I hope you’re enjoying the weekend. I need your attention please kindly reply when you get this. Thanks”*

Hackers try to get a response first and then move onto trying to monetize the scam. Hackers rarely ask for a wire transfer or gift cards right away; they want to establish rapport and trust first. They are willing to invest time and effort to trick victims.

The sheer volume of these types of attacks suggest they are very effective.

Payroll and direct-deposit scams

Payroll scams target the HR, finance and payroll departments, with the goal of getting an employee's salary transferred to a different account. Hackers reach out to the payroll department, pretending to be an employee and asking for their paycheck to be deposited into a fraudulent account.

BEC attacks involving the diversion of payroll funds are increasing in frequency, according to the FBI. In the 18-month period between **January 2018 and June 2019, attacks were responsible for an estimated loss of $8.3 million**. **The average dollar loss reported in complaints was $7,904, an increase of more than 815% from the previous 18 months**.

Scam emails are typically sent to payroll and request account changes.»

"I recently switched to a new financial institution and I need your quick assistance to update my paycheck direct deposit details. Thanks"

"I want to make a change to my payroll direct deposit account. Can I send you the new account and routing number or attach a voided check? Regards"

Payroll scams make up around 8% of all BEC attacks.»

Other fraudulent requests ask about the process to make a change.

"I need you to email me a direct deposit form to update my payroll info or would a voided check suffice?"

"I want to change my paycheck direct deposit details and I want my next paycheck to be paid into the new bank account let me know the information needed to make this change active for the next paycheck. Thanks"

Usually, the fraudulent account details are for a pre-paid card, making it difficult to trace the owners. Hackers keep these emails brief and include little information beyond the request.

Gift-card scams

Attackers use social-engineering tactics to trick office managers, executive assistants and others to purchase and send gift cards to the attacker. Most of the time, these attacks impersonate the CEO and ask for gift cards to be bought for employees or clients. This is a popular scam during the holiday season, as it is not an unusual request.

Gift-card scams are less frequent than others, making up about 4% of all BEC attacks.»

> *"Hello. Are you there? I need you to get something done as soon as possible. I need you to get some gift cards. We have some clients we need to send gifts. Let me know if it is possible for you to do handle this.*
> *Thanks, CEO"*

> *"Are you available for a quick task? I need some gift cards to send out today. Let me know if you can get it now from Walmart, CVS or Target and I can advise the quantity and denomination. I will reimburse you later. Thank you"*

Another common tactic is using secrecy, such as asking to purchase gifts or gift cards as a surprise for staffers. This plays on the victims' emotions and their desire to do something good for the team. It also makes them feel like they are in on the surprise, and, as a result of the excitement, they may not pay as much attention to who is really sending the request. In addition, gift cards are commonly used to reward employees, so the request may not cause any suspicion. Messages are also casual and personal.

> *"I hope you are well. I would appreciate your assistance and your confidentiality. I am in the process of surprising some of the staff today including you with a gift and however I need to get a purchase done for me. Email me once you get this. Regards"*

> *"Hi. A quick message before it skips my mind again. I need you to purchase some gift cards from the store today. We intend to reward some staffs with it. Reply and let me know how soon you can get this done. Also, please keep this confidential pending the time we announce it. Sent from my Verizon wireless <NUMBER> smartphone"*

The impact of spear-phishing attacks

Business email compromise attacks have high click rates. **One in 10 spear-phishing emails successfully tricks a user into clicking**. That number triples when the individual or department being impersonated is within the recipient's organization. These attacks are effective because it's not unusual for employees to receive regular updates and requests from the HR and IT departments.

Emails that appear to be from HR notifying employees of a change in benefits or parking rules are particularly effective at baiting users and initiating a successful interaction.

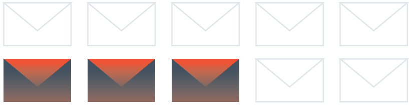
Similarly, emails that look like they come from the internal IT team, warning users of a potential internet outage or announcing a new corporate application that's available for download, also appear to be effective based on their popularity.

Here's an example:

> *"<URL> Email suspension notification. Our server detected some irregular activities in your email today. For your account security we need you to verify your email identity immediately. Please download the attached <URL> account verification form to secure your account."*

Click rates in spear-phishing emails

3 in 10: click rate for emails that appear to come from HR or IT



The cost of attacks

With such high click rates, it's not surprising that the costs and damages associated with spear-phishing attacks are also high. A recent Barracuda survey shows that professionals believe the cost of spear-phishing attacks is increasing. That's bad news, considering **66% of those surveyed claim that attacks have had a direct monetary cost for their organization in the last year**. There are a wide range of financial impacts from attacks, including business interruption, reduced productivity, data loss, regulatory fines and brand damage.

In the last 12 months, the average amount lost per organization due to spear-phishing attacks was $270,000. **One recent business email compromise scam cost a media conglomerate $29 million**! In that case, it appears the email account of a trusted third-party vendor was compromised and then used to perpetrate the attack by asking for payment to be sent to a fraudulent bank account.

Protecting against business email compromise attacks

Consider these best practices to help defeat spear phishing

Educate users

Show employees how to recognize employee impersonation. Be sure to point out that phishing attacks don't always need to have a URL or an attachment and remind them to double-check email addresses and to pay attention to unusual requests.

Set up internal policies

Put policies and protocols in place that require additional safeguards for wire transfers and other financial transactions. Prohibit email requests for purchases and other monetary transactions. Ensure multiple people are required to be involved in the approval process.

Enforce DMARC authentication

Set up DMARC authentication to protect against attackers spoofing your email domain in their impersonation attacks. DMARC reports provide visibility and analysis into who's using your email domain and how. Use this information to establish DMARC enforcement policies.

Use machine learning

Don't rely solely on traditional email security technologies, as most business email compromise attacks are designed to bypass gateways. Machine learning technologies are able to analyze internal emails and create a model of each individual's typical communications. Use this data to predict and detect attacks.

Be ready to respond fast

Train your employees how to recognize and report an attack. It's not a matter of whether an attack will sneak through, it's a matter of how often. Be sure to also use intelligence tools to do your own threat hunting. Deploy automated incident response solution that identifies the scope of attacks and quickly removes malicious messages from inboxes before any damage is done.

Barracuda®
Your journey, secured.