Spear Phishing: Top Threats and Trends

Vol. 6 July 2021

Insights into attackers' evolving tactics and who they're targeting

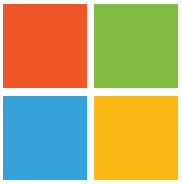
Whether it's taking advantage of the buzz around cryptocurrency, stealing credentials to start a ransomware attack, or tailoring attacks to less suspicious targets in low profile roles, cybercriminals are constantly adapting their tactics and making their attacks more sophisticated. This in-depth report takes a look at the most recent trends in spear-phishing and the new tricks attackers are using to sneak past their victims' defenses.»

Barracuda
Your journey, secured.

Table of Contents

Key findings

1 in 10 social engineering attacks are **business email compromise**



43% of phishing attacks impersonate **Microsoft brands**

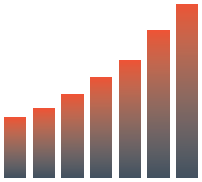
An average organization is targeted by over **700 social engineering attacks in a year**

1 in 5 BEC attacks target employees in **sales roles**

77% of BEC attacks target **employees outside of finance and executive roles**

IT staffers receive an average of **40 targeted phishing attacks in a year**

An average **CEO** will receive **57 targeted phishing attacks in a year**



Cryptocurrency-related impersonation attacks **grew 192% between October 2020 and April 2021**

Increasing complexity of email threats

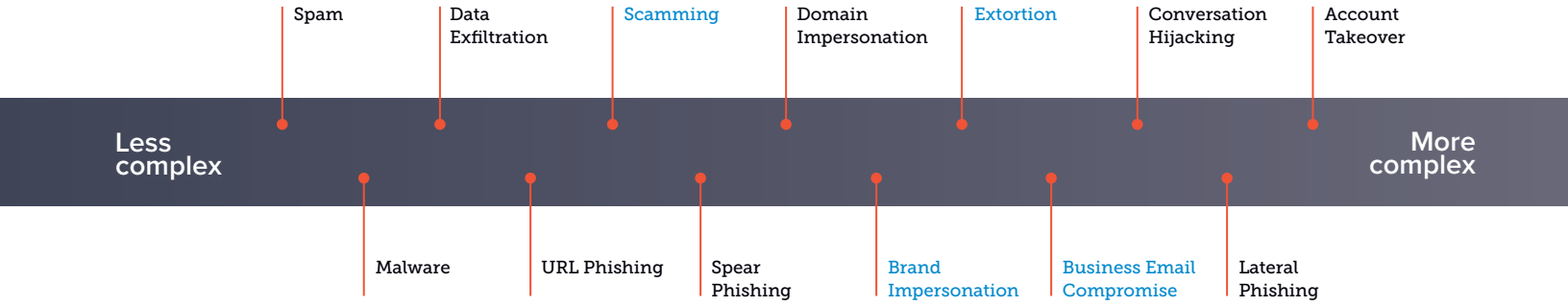
Over the past several decades security vendors have invested in protecting against email attacks, and the defense perimeters they have built for their customers have proven effective at blocking most malicious or unwanted email messages.

Despite organizations having the ability to halt millions of attacks, email threats are still succeeding and becoming increasingly complex. There is a real shift underway, moving from volumetric to targeted attacks, from malware to social engineering, from single hackers to organized criminal enterprises profiting from attacks that begin with a single phishing email.

Old methodologies of email protection that relied on rules, policies, allow or block lists, signatures, and other attributes of traditional email security are no longer effective against the growing threat of socially engineered attacks.

Researchers at Barracuda have identified 13 email threat types faced by organizations today. These range from high-volume attacks, such as spam or malware to more targeted threats that use social engineering such as business email compromise and impersonations.

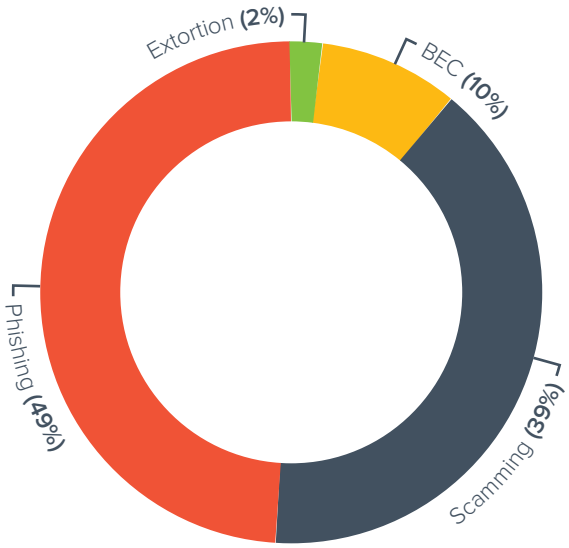
13 email threat types: Email threat types included in this research.



Hackers use a combination of tactics to trick their users into taking an action, such as giving up their credentials so that the attackers can get access to the company's environment or launch a ransomware attack, sharing sensitive information that could be sold or used for further attacks, or simply sending a payment, gift cards, or money transfers.

Between May 2020 and June 2021, Barracuda researchers analyzed more than 12 million email attacks impacting more than 3 million mailboxes at roughly 17,000 organizations. In that analysis, we have been tracking four distinct categories of social engineering attacks:

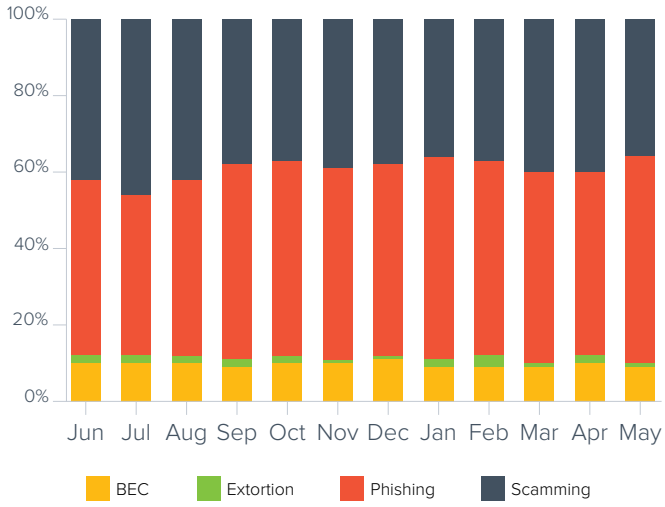
Social engineering attacks (June 2020 – May 2021)



Business email compromise, or simply BEC, attacks usually involve impersonating an individual either inside or outside of an organization. In the past year, these attacks made up 10% of all the socially engineered attacks we've seen, but they are grabbing a bigger share of headlines. Education, healthcare, commercial, travel—organizations from every industry fell victim to one of these attacks, often losing millions of dollars. In a typical BEC attack, a hacker will impersonate an employee, usually an executive, and request wire transfers, gift cards, or that money be sent to bogus charities.

Phishing impersonation attacks will usually pose as emails from a well-known brand or service in order to trick victims into clicking on a phishing link. These attacks make up 49% of all socially engineered threats we've seen in the past year. Almost all of the attacks that fall into this category will include a malicious URL. Although phishing emails are nothing new, hackers have started to deploy ingenious ways to avoid detection and deliver their malicious payloads to users' inboxes. They shorten URLs, use numerous redirects, and host malicious links on document sharing sites, all to avoid being blocked by email scanning technologies. Phishing impersonation attacks have also been trending upwards. These attacks made up 46% of all social engineering attacks we detected in June 2020 and grew to 56% by the end of May 2021.

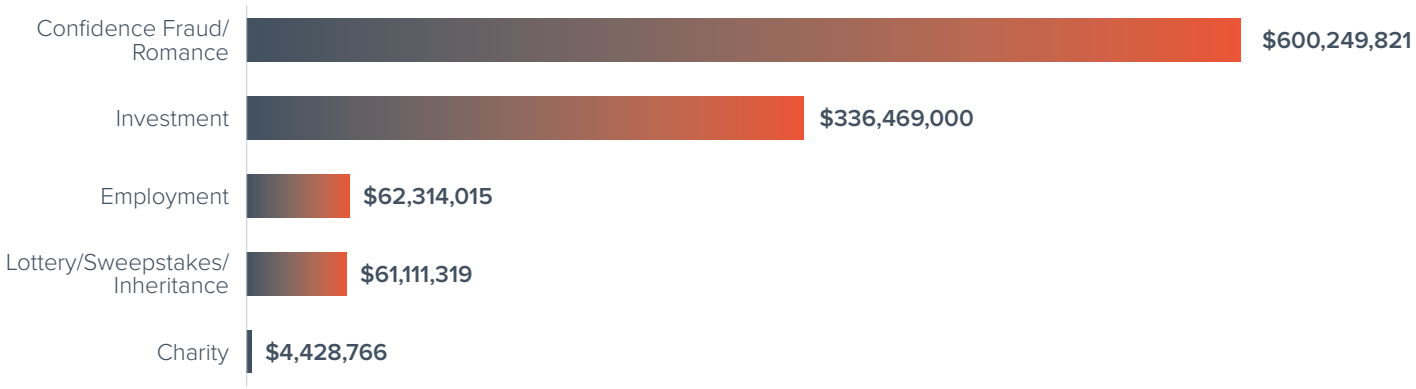
Social engineering attacks over the past year



Extortion attacks make up only 2% of the total number of targeted phishing attacks we have seen in the past year. These attacks were mostly sextortion email threats, where hackers threaten to expose sensitive or embarrassing content to their victim's contacts unless a ransom is paid out. Demands are usually a few hundred or a few thousand dollars and need to be paid in bitcoin, which is potentially difficult to trace. With so many people working remotely, Zoom was mentioned a number of times in these attacks, at times referencing Jeffrey Toobin's well publicized scandal. The number of extortion attacks reported to the FBI in 2020 increased by 78% from the previous year, and estimated losses were over $70 million. These scams can also have very tragic consequences that go beyond monetary losses. Victims of these scams have killed themselves because they were concerned about their private details going public.

Scamming attacks can take many shapes and forms, ranging from claims of lottery wins and unclaimed funds or packages, to business proposals, fake hiring, donations, and other schemes. They tend to be a little less targeted than other types of attacks described above, but scamming attacks represent 39% of all social engineering attacks we've detected in the past year and are no less successful. Because hackers cast a wide net with the different types of scams they develop, these threats cost victims hundreds of millions of dollars. For example, this past year hackers used COVID-19 in their investment related scams, looking for investment in fraudulent coronavirus treatments or vaccines.

Cost of scamming attacks



Source: FBI Internet Crime Complaint Center Internet Crime Report 2020

...Scamming attacks represent 39% of all social engineering attacks we've detected in the past year...»

Phishing impersonation of top brands

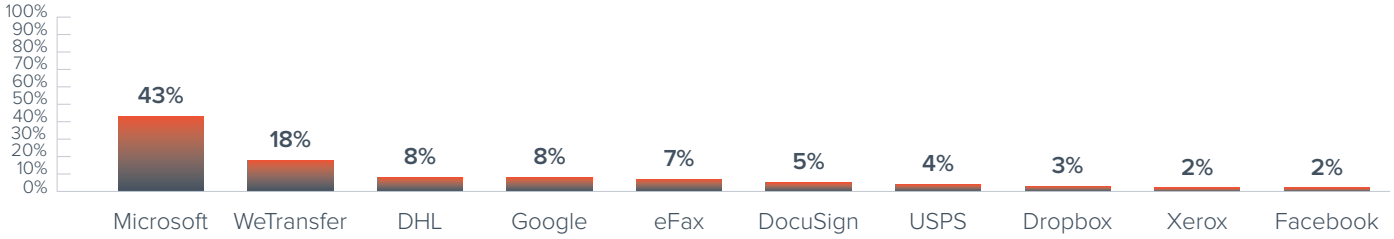
Taking on the identity of a well-known and trusted brand is an old trick that many hackers use. People tend to expect to see communication that comes from our favorite brands, and that makes them more likely to trust it. The top three brands used in phishing impersonation attacks — Microsoft, WeTransfer, and DHL — have stayed consistent since 2019.

With 79% of organizations using Office 365 and many more looking at migrating in the immediate future, it's not surprising that Microsoft brands remain a top target for cybercriminals.

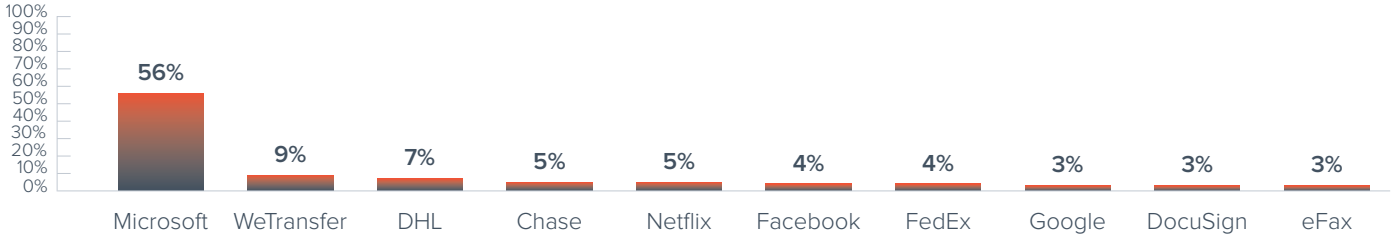
Looking at the top 10 impersonated brands, Microsoft was used in 43% of phishing attacks in the past 12 months. Hackers are taking advantage of the increasing popularity of Microsoft's cloud-based services and the shift to remote working over the past year. Cybercriminals will send fake security alerts or account update information to get their victims to click on a phishing link. The goal of these attacks is simple—to steal login credentials to gain access to corporate networks. From there, hackers can launch other types of attacks, including ransomware.

A compromised account can cause real havoc within organizations. Earlier this year Colonial Oil Pipeline fell victim to a ransomware attack that was reportedly enabled by compromised passwords. While a ransom payment of $4.5 million was made to restore operations, the real cost of the fallout is almost impossible to measure.

Top 10 brands impersonated (2021)

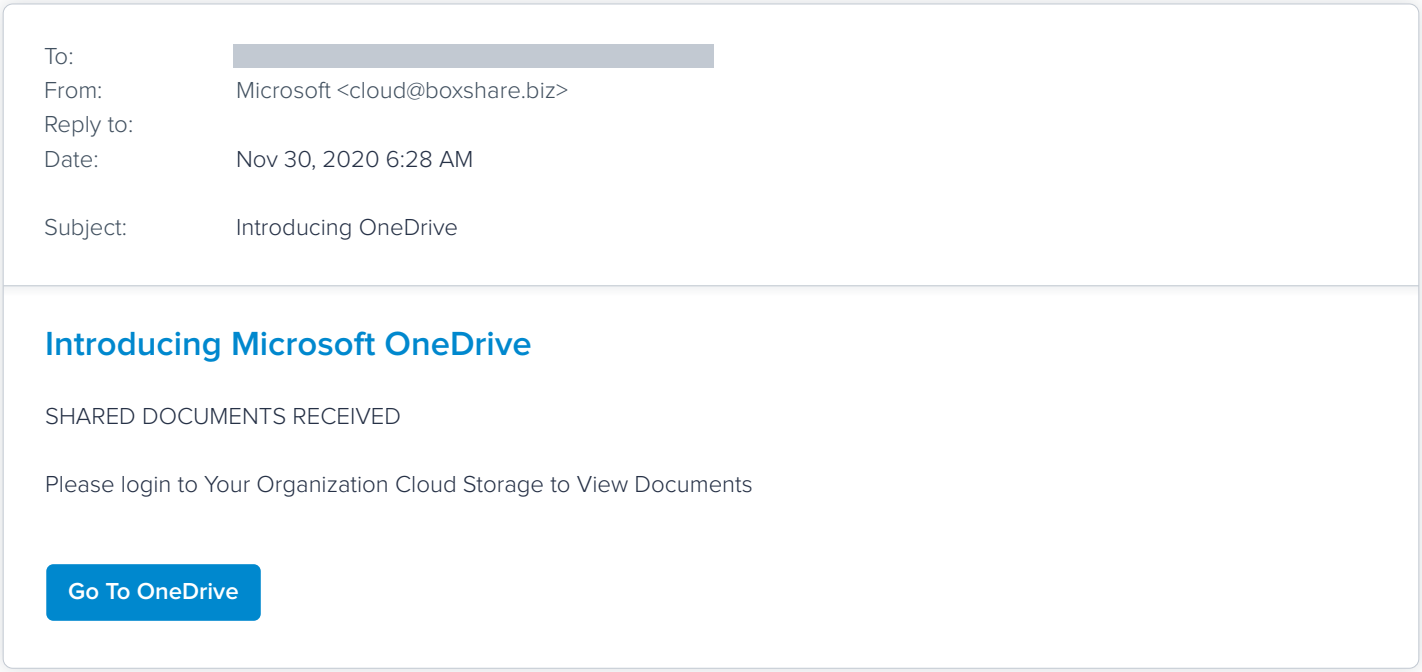


Top 10 brands impersonated (2019)



WeTransfer online file transfer services allows users to share files of large sizes that they may not be able to send directly through email. This brand was impersonated in 18% of phishing attacks. Hackers will send phishing emails asking to login and confirm account information, download potentially malicious files, provide payment details, or offer tech support. Use of WeTransfer in phishing attacks became more common in recent years, increasing from 9% in 2019 to 18% by mid-2021. This increase can be attributed to the rising popularity of the service and additional ways hackers can use document-sharing sites in their attacks.

Some attacks use WeTransfer as an intermediary website in a phishing attack. The original email will include a legitimate link to a file on WeTransfer and therefore pass through email scans. However, once it's opened, the file will include a link to a phishing site that often looks exactly like the Office 365 sign-in page and asks for login information to access the file. These types of redirect attacks that use file transfer sites are gaining in popularity.


To:
From: Microsoft <cloud@boxshare.biz>
Reply to:
Date: Nov 30, 2020 6:28 AM

Subject: Introducing OneDrive

Introducing Microsoft OneDrive

SHARED DOCUMENTS RECEIVED

Please login to Your Organization Cloud Storage to View Documents

Go To OneDrive

Logistics and delivery companies also regularly make the list of top impersonated brands. Around 12% of attacks used either DHL or USPS branding to provide fake updates on shipments and deliveries. Hackers have been capitalizing on the fact that so many people have been stuck at home over the past year and getting more deliveries.

Other brands that made it into the top 10 in 2021 included Google, DocuSign, and Facebook. Compromising any of these accounts will provide hackers with a wealth of personal information that they can exploit in further attacks.

To: [redacted]
From: EXPRESSDHL <trackingdhl-2021-@skynet.be>
Reply to:
Date: Mar 03, 2021 4:02 PM

Subject: EXPRESS SHIPMENT TRACKING NUMBER ... 978526330211

Hello,

Your DHL Express shipment with waybill number 978526330211
is waiting for delivery. Please confirm the payment details in the following link below.

The current Status of the shipment is: On Hold.

to complete your delivery options **Here**

DELIVERY INFORMATION

Waybill No.	978526330211
Available for delivery	We will message you when ready
Opening hours	Monday - Sunday 00:00-23:59 Holiday 00:00-23:59
Delivery Time	By End of Day

Thank you for using On Demand Delivery.
DHL Express – Excellence. Simply delivered?

DHL Express | Contact DHL | Privacy Policy | Unsubscribe

Target identity

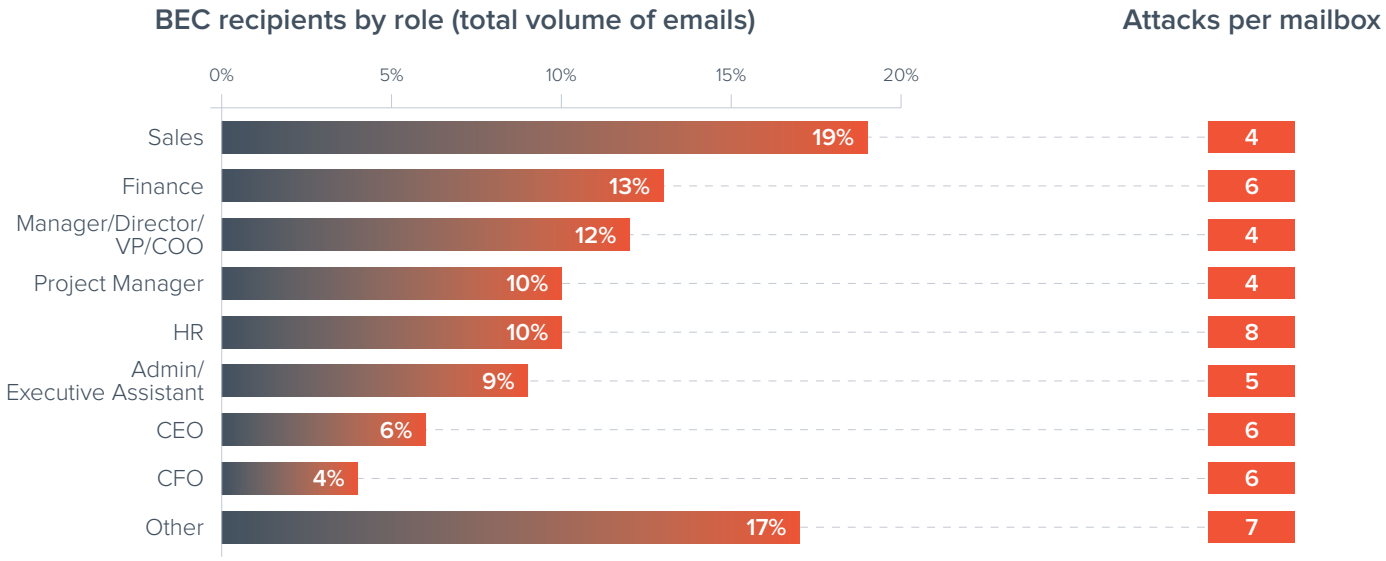
Spear-phishing attacks are defined by their targeted nature. Attackers will spend time researching their victims and their organizations, designing attacks targeting specific individuals with a customized message. There are many publicly available sources and social media sites that will help attackers create a relatively accurate picture of the individuals within an organization and the nature of their roles.

Based on our analysis, an average organization is targeted by over 700 social engineering attacks in a year. Our researchers analyzed the 100 most-targeted business titles and the type of attacks they receive. We have all heard of CEO and CFO fraud, but is the CFO really the most targeted employee within the organization? Are there any other prime targets that hackers like to focus their efforts on?

BEC attacks

BEC attacks target a variety of roles within each organization. A classic BEC attack will seek to impersonate an executive, focusing on employees in the finance department, including the CFO or others with access to funds so they can be tricked into making a fraudulent payment. Interestingly, CFOs received around 4% of all BEC attacks in the past year, while the rest of the finance department were targeted by 13% of these attacks. This can partially be explained by the size of the finance department, which will usually include multiple employees, while CFO is an individual role. Members of finance departments on average received six targeted BEC attacks, the same number as a CFO.

Roles related to sales received the largest number of BEC attacks, but this was mostly due to the number of sales reps that organizations have. The average number of attacks per mailbox was four, which is below average.



Due to the nature of their role, sales reps are used to getting external messages from senders they haven't communicated with before. At the same time, they are all connected with payments and with other departments including finance. For hackers, these individuals could be a perfect entry point to get into an organization and launch other attacks.

Administrative or executive assistants were also a popular target. These individuals will usually have access to executive calendars or accounts. They are often targeted by gift card scams or credential theft.

Many organizations focus their training and protection on who they perceive to be the most targeted individuals within the organization—usually executive and finance teams. However, 77% of BEC attacks targeted employees in other departments. Attackers look for an entry point and a weak link within your organization, and then they work their way to more valuable accounts. This highlights the need to secure and educate every employee to the same level.

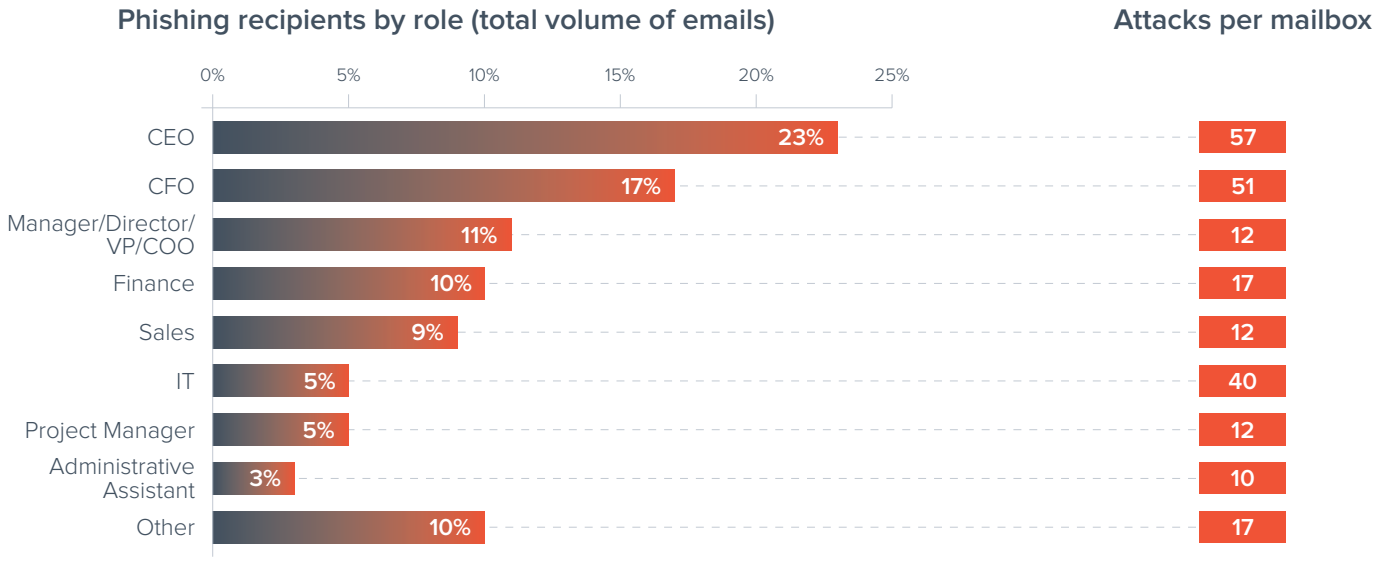
Phishing attacks

Phishing attacks that impersonate a service or business application usually include a phishing URL with a goal of stealing account credentials or other valuable information. Hackers target these attacks at a different set of roles.

Executive teams and individuals at a management level received the greatest number of phishing attacks. These accounts are very valuable to hackers as they often contain important correspondence that can be used in further attacks.

When we look at the number of phishing emails targeting IT teams, although they received only 5% of the total number of attacks, each employee was targeted by 40 email attacks, which is well above average. IT staff has access to business-critical applications, so compromising their accounts can be extremely valuable to hackers as it will give them access to organizations' security and IT infrastructure. Cybercriminals tailor their attacks to their victims, so there were barely any BEC attacks, which usually look for quick monetary return, targeting IT teams. However, when it comes to attacks that include phishing URLs designed to compromise accounts, IT was one of the top targets.

Organizations need to pay attention to which employees are targeted by what types of threats. This intelligence can be used to design more relevant and effective security awareness training.



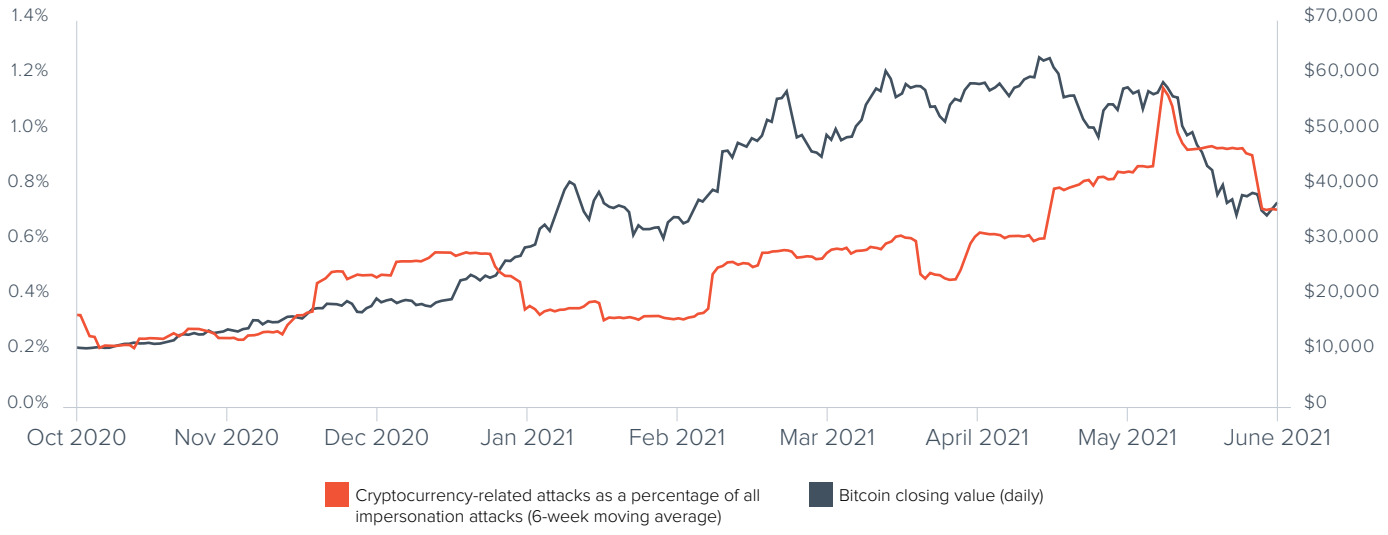
Cryptocurrency & spear phishing

Cryptocurrency is a type of currency that is available only in a digital format. Because of the decentralized nature of cryptocurrency and lack of regulation, it has become the currency of choice for cybercriminals.

Traditionally used in extortion and ransomware attacks, hackers have now started to incorporate cryptocurrency into spear phishing, impersonation, and business email compromise attacks.

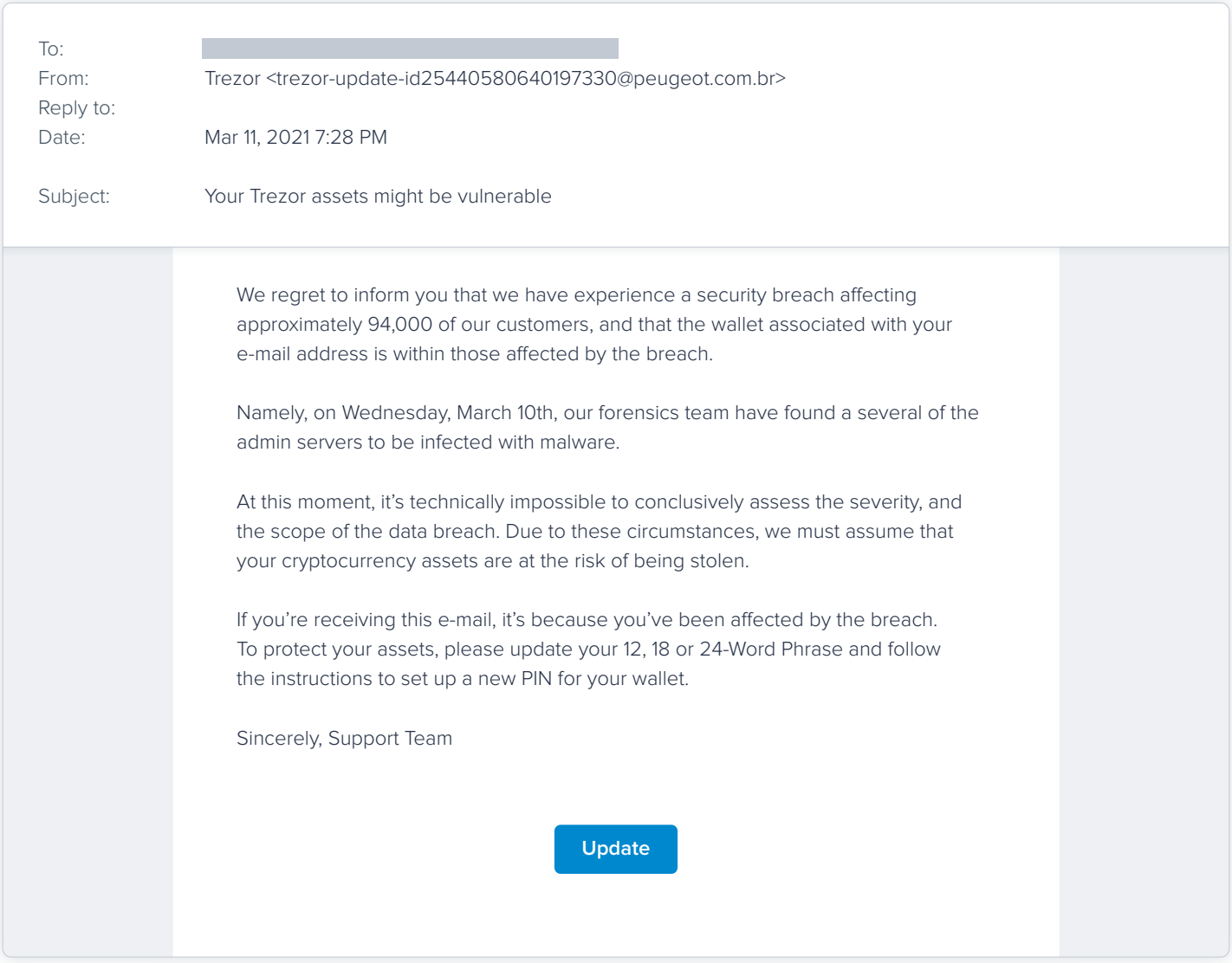
Until very recently you couldn't use cryptocurrency in the real world to pay for day-to-day goods. However, as some companies started to announce that they will accept payments in bitcoin, it generated more interest in cryptocurrency and started to drive its value up. Fueled by the news frenzy surrounding bitcoin, its price increased by almost 400% between October 2020 and April 2021. Cyberattacks quickly followed with impersonation attacks growing 192% in the same period of time.

Value of cryptocurrency and volume of related impersonation attacks



Hackers use bitcoin to get paid in extortion attacks, where hackers claim to have a compromising video or information that will be released to the public if the victim does not pay to keep it quiet. While this scheme has been around for some time, as the price of bitcoin climbed, cybercriminals started to come up with more sophisticated schemes to cash in on bitcoin-mania.

Over the past eight months we have seen the number of phishing impersonations and business email compromise attacks related to cryptocurrency closely follow the increasing price of bitcoin. Hackers impersonated digital wallets and other cryptocurrency-related apps with fraudulent security alerts to steal log-in credentials. In the past, attackers impersonated financial institutions targeting your banking credentials. Today they are using the same tactics to steal valuable bitcoins.



To:
From: Trezor <trezor-update-id25440580640197330@peugeot.com.br>
Reply to:
Date: Mar 11, 2021 7:28 PM

Subject: Your Trezor assets might be vulnerable

We regret to inform you that we have experience a security breach affecting approximately 94,000 of our customers, and that the wallet associated with your e-mail address is within those affected by the breach.

Namely, on Wednesday, March 10th, our forensics team have found a several of the admin servers to be infected with malware.

At this moment, it's technically impossible to conclusively assess the severity, and the scope of the data breach. Due to these circumstances, we must assume that your cryptocurrency assets are at the risk of being stolen.

If you're receiving this e-mail, it's because you've been affected by the breach. To protect your assets, please update your 12, 18 or 24-Word Phrase and follow the instructions to set up a new PIN for your wallet.

Sincerely, Support Team

Update

To: [redacted]
From: [redacted]
Reply to:
Date: May 29, 2021 12:50 PM

Subject: Subject: I invested 1 bitcoin and after 5 minutes I received 2 bitcoins from Elon Musk

Name: [redacted]
Phone: [redacted]
Email: [redacted]
Message: You have received 10 BTC, urgently pick it up today >>>>>>>>>>>>>>> http://www.tesla.com.donaldtrumpcoin.store/bitcoin?8743<<<<<<<<<<<<<<<

Cybercriminals have also included bitcoin as part of their business email compromise attacks impersonating employees within an organization. They target and personalize these emails to get their victims to purchase bitcoin, donate them to fake charities, or even pay a fake vendor invoice using cryptocurrency.

To: [redacted]
From: [redacted] <smsinfo@verizonsmswireles.com>
Reply to:
Date: Jan 15, 2021 1:40 PM

Subject: Gift Reward

Hi [redacted] a quick message before it skips my mind again. I have been updated and concluded that we can use bitcoin to pay compensation and bonuses as rewards for some staffs because the Pandemic has changed many things as I have switched to using bitcoin too.

I need you to help purchase some bitcoin to kickstart the process from any Bitcoin ATM which can be found nowadays in many stores.

Kindly try to locate any BTC ATM closest to you and let me know how soon you can get it done.

[redacted]
COO

Sent from my iPhone

To: [redacted]
From: [redacted] <xonlyfamily@gmail.com>
Reply to:
Date: April 07, 2021 9:00 AM

Subject: RESPONSE NEEDED

[EXTERNAL] [redacted]

Hello [redacted]

Are you available at the moment? If you are, I have a task for you to carry out urgently today, I need you to head to the nearest Bitcoin Machine to make a charity donation on my behalf before the day runs out.
Email me once you get this.

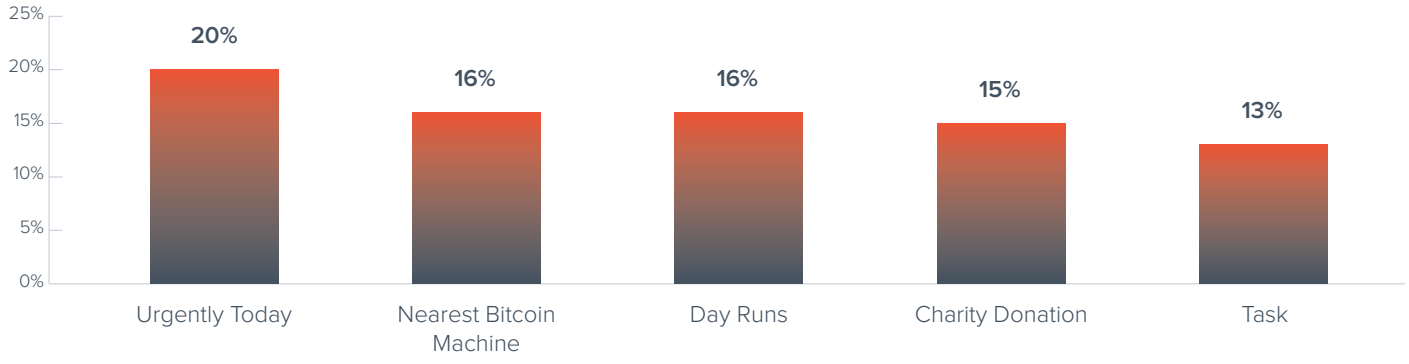
Regards,
[redacted]
Executive Vice President

Sent from my iPhone

We also used Barracuda's AI natural language processing capabilities to analyze the language used in cryptocurrency-related BEC attacks and determine key phrases and calls to action that hackers used to incite their victims. Similar to typical BEC attacks, cybercriminals will create a sense of urgency by using phrases like "urgent today" or "before the day runs out."

Their call to action is typically for their victim to go to the "nearest bitcoin machine." They also play on their victims' sentiments to request that a payment be made as a "charity donation," making their victims believe they are doing a good thing.

Top 5 key phrases and call to actions in BEC attacks



Best practices to protect against spear-phishing attacks

Organizations today face increasing threats from targeted phishing attacks. To protect your business and users, you need to invest in technology to block attacks and training to help people act as a last line of defense.

Technology

- **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, impersonation, and extortion attacks. 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.

- **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.

People

- **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.

- **Review internal policies.** 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.

- **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.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-enabled, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level.

Get more information at barracuda.com.

Barracuda
Your journey, secured.