Spear Phishing: Top Threats and Trends

Vol. 5 December 2020

Best practices to defend against evolving attacks

As their speedy exploitation of fears around the COVID-19 pandemic show, cybercriminals adapt quickly to current events and new tactics. This in-depth report takes a look at the evolving trends in spear-phishing and the new ways attackers are tricking their victims.»

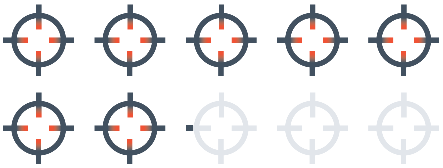
Barracuda.
Your journey, secured.

Table of Contents

Key findings

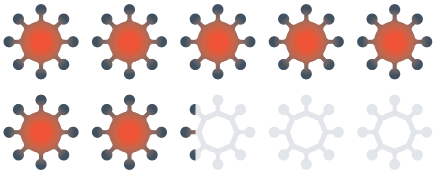
12% of spear-phishing attacks are BEC attacks

Business email compromise (BEC) makes up 12% of the spear-phishing attacks analyzed, an increase from just 7% in 2019.



71% of spear-phishing attacks include malicious URLs

Hackers use multiple tactics to disguise malicious links and avoid detection by URL protection solutions.

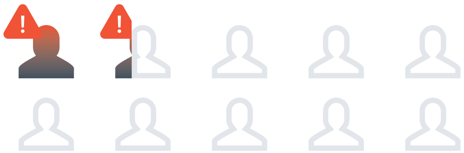


72% of COVID-19-related attacks are scamming

In comparison, 36% of overall attacks are scamming. Attackers prefer to use COVID-19 in their less targeted scamming attacks that focus on fake cures and donations.

Only 30% of BEC attacks included a link

Hackers using BEC want to establish trust with their victim and expect a reply to their email, and the lack of a URL makes it harder to detect the attack.



13% of all spear-phishing attacks come from internally compromised accounts

Organizations need to invest in protecting their internal email traffic as much as they do in protecting from external senders.

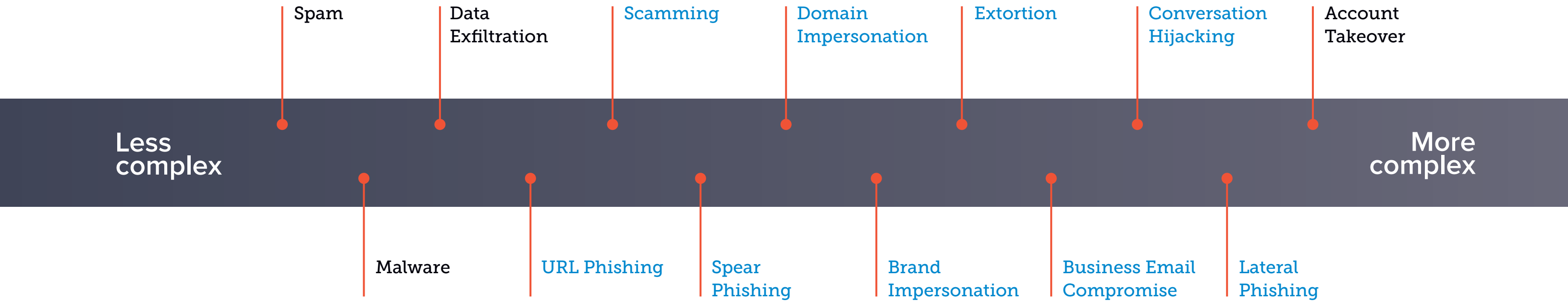
Overview of spear-phishing attacks

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.

Some of these attacks are used in conjunction with others; hackers often combine various techniques. For example, many brand impersonation attacks include phishing URLs, and it's not uncommon to see conversation hijacking as part of business email compromise. Understanding the nature and characteristics of these attacks helps you build the best protection for your business, data, and people.

This research will focus on nine of the more complex and targeted attacks, including:

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



Traditionally, hackers focused on malware attacks, but in recent years they have shifted their efforts to ransomware and targeted phishing attacks with the goal of capturing user credentials.

Targeted spear-phishing attacks are growing in volume, complexity, and the impact they have on businesses. These carefully designed and targeted attacks have a much higher success rate getting through email security, landing in users' inboxes, and tricking them into taking an action. This research focuses on trends associated with these social engineering attacks, the latest tactics and techniques used by cybercriminals, how these threats have evolved over time, and what organizations can do to prevent and block these attacks.

Barracuda researchers evaluated more than 2.3 million spear-phishing attacks between August and October 2020 that targeted more than 80,000 organizations around the world.

All these email attacks have been classified into five major categories:

Phishing

This category of attacks uses various impersonation tactics that are designed to trick individuals into believing they're getting an email from a brand or service they've used before. This includes:

- **Brand impersonation** — Attacks impersonate well-known brands or organizations
- **Form-based attacks** — Hackers leverage file, content sharing, and productivity sites, like sway.office.com
- **Phishing attacks with attachments**
- **URL phishing** — Cybercriminals use email to direct their victims to enter sensitive information on a fake website that looks like a legitimate website
- **Spear phishing** — A highly personalized email phishing attack typically crafted to steal sensitive information, such as login credentials or financial details

Business Email Compromise (BEC)

BEC, also known as whaling, CEO fraud, or wire-transfer fraud, is a fast-growing threat for organizations today. Hackers impersonate an employee, vendor, or other trusted individual for a financial gain. Some common tactics Barracuda researchers have recently seen include:

- **Wire transfer fraud** — Requests for a fraudulent money transfer to an illegal account.
- **Payroll scams** — Fraudulent requests to change account details for paycheck deposits.
- **Gift card scams** — Fraudulent requests to purchase and send gift cards.
- **Conversation hijacking** — Also known as vendor impersonation scams. Cybercriminals hijack or insert themselves into existing business conversations, usually between a vendor and a business, requesting a payment or providing a last-minute change to payment details, diverting money to illegitimate accounts.
- **Domain impersonation** — Attackers attempt to impersonate a domain by using techniques such as typosquatting.

Extortion

In this type of attack, the criminal contacts potential victims by email and claims to have compromising videos or information that will be released to the public if the victim doesn't pay to keep it quiet. As "proof" that the criminal has access to this material, the email includes sensitive information that only the victim should know, such as passwords. According to the FBI, the cost of extortion attacks was more than $107 million in 2019.

Lateral phishing

Lateral phishing attacks typically come from compromised accounts and target users internally within the organizations. These attacks are especially difficult to detect because they come from internal, legitimate email accounts and appear to be from a trusted colleague. In this research, these internal attacks are examined separately from external attacks, such as scamming, extortion, phishing and BEC.

Scamming

Email scamming is a type of spear-phishing attack designed to steal the identity of the victim or trick them into disclosing personal information. Many of these scams include fake invoices, phony charities, and other schemes meant to lure the victim into sending money to the attacker. Here are some examples of scamming attacks that Barracuda researchers regularly see:

- **Tech support scams** — A fraudulent company informs you that you have a virus and asks you to hire them to fix it.

- **Foreign money exchange scams** — You're offered a large payment to help with a foreign transfer of money, but first you must pay fees or taxes.

- **Charity scams** — A national or personal tragedy occurs, and scammers send emails asking for donations to help the victims. The donations go to the criminal, not the victims or any legitimate charity.

- **Political donation scams** — During election seasons, scammers send emails asking for donations to support a candidate or political organization, but the donations go to the criminal instead.

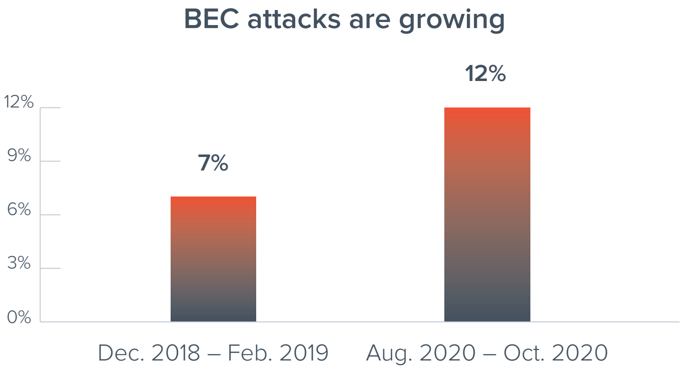
The 2019 FBI Internet Crime Report recorded $791 million in reported losses to email scams.

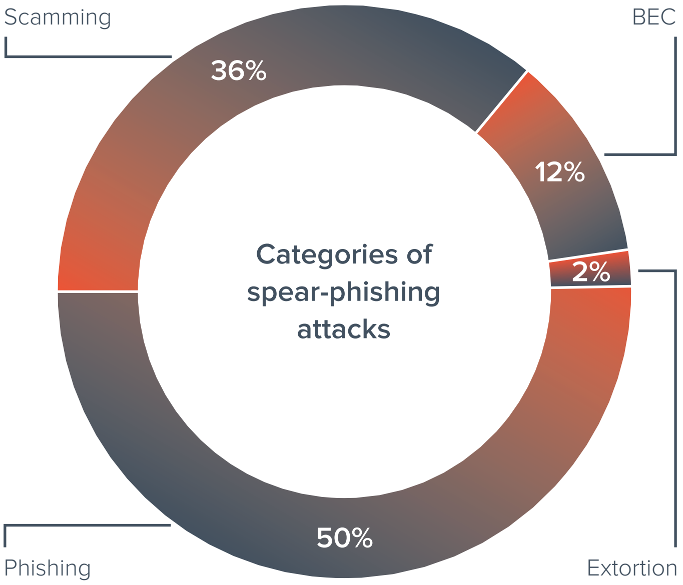
Spear-phishing attack trends

Phishing attacks make up half (50%) of all spear-phishing attacks Barracuda researchers analyzed over this three-month period, by far the largest category. These attacks target individuals with the intent to steal confidential information, such as login credentials.

Business email compromise is a growing threat to organizations. In March 2019, Barracuda researchers reported that 7% of all spear-phishing attacks could be classified as BEC, but today that number has increased to 12%. This fast-growing trend reflects how successful this type of attack can be. According to the FBI, BEC attacks led to over $3.5 billion in losses in 2019. Over the past two years, there have been a number of high-profile BEC attacks, such as Japan's Toyota Boshoku Corporation – supplier of auto parts – lost $37 million to a BEC attack in 2019 and the Government of Puerto Rico lost $2.6 million in early 2020.

According to the FBI, these attacks cost business over $26 billion between 2016 and 2019.





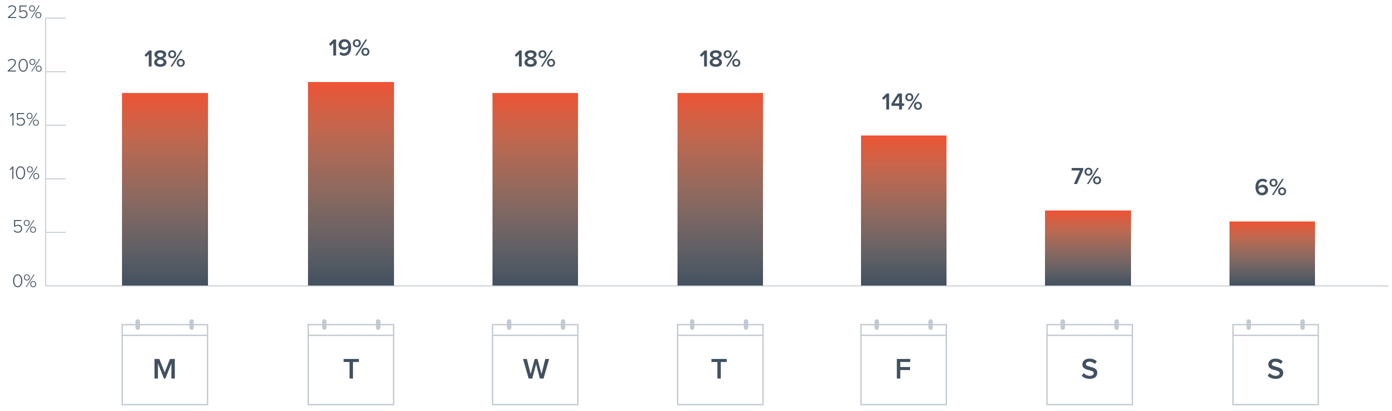
Scamming and extortion made up the rest of the attacks analyzed in this research – 36% and 2%, respectively. These attacks are less targeted in nature, but still represent a significant portion of the overall scams Barracuda researchers have seen. Today, extortion attacks make up a smaller portion of spear-phishing attacks than researchers saw in 2019 — 2% compared to 11% back in 2019. This is due not to a decline in the number of extortion attacks, but rather very fast growth of other types of spear-phishing attacks.

Hackers 'work' when their targets work

A full 87% of all spear-phishing attacks in this analysis were sent during the work week — days when most businesses operate. However, it's not unusual for hackers to exploit the weekends in their targeted attacks. 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"

Spear-phishing attacks during the week



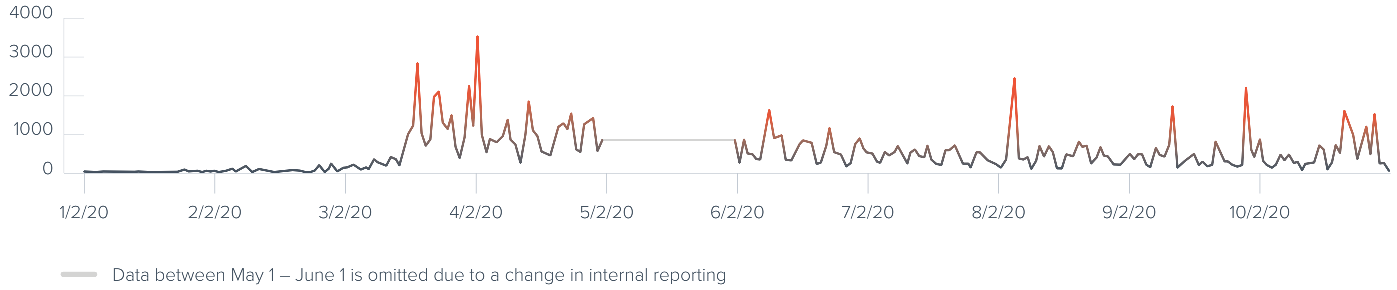
Barracuda researchers saw similar dips during the holidays, like Fourth of July, when the number of spear-phishing attacks were 62% below average. Other times, however, cybercriminals use holidays or seasonal events to try to exploit security weaknesses and other vulnerabilities. Barracuda's earlier research on spear-phishing attacks targeting the education sector found that the number of attacks targeting schools and colleges increased significantly in September when students returned.

COVID-19-related spear-phishing attacks

Earlier this year, as the world started to face the new reality of the COVID-19 pandemic, Barracuda researchers noted a steady increase in the number of coronavirus COVID-19-related spear-phishing attacks starting in January, with a significant spike of 667% in early weeks of March 2020.

Barracuda researchers continued to monitor this trend throughout 2020. Hackers still use COVID-19 as a lure in their attacks, however the overall volume of these attacks has not grown significantly since March. COVID-19-related spear-phishing attacks represented around 2% of all spear-phishing attacks detected by Barracuda. While hackers' interest in this type of spear-phishing cooled off, it did not disappear completely.

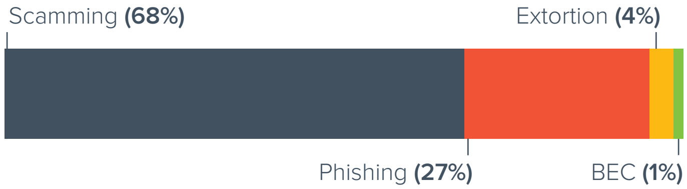
COVID-19-related spear-phishing attacks in 2020



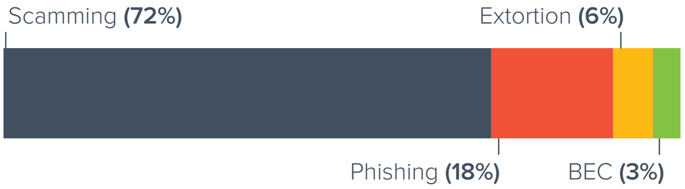
The vast majority of these attacks are scamming, mostly messages looking for donations, investments, or inheritance scams. There was a minor increase in the number of BEC attacks that used COVID-19 as a way to grab their victims' attention—from 1% to 3%—but these numbers remain low compared to the overall average of BEC attacks of 12%.

In the early days of COVID-19, hackers were able to take advantage of the uncertainty of the situation with great success. As everyone learned to live with their new COVID reality, cybercriminals diverted their interest to other areas. It shows how quickly attackers can adapt to current events.

COVID-19 related spear-phishing Jan. – Apr. 2020



COVID-19 related spear-phishing June – Oct. 2020



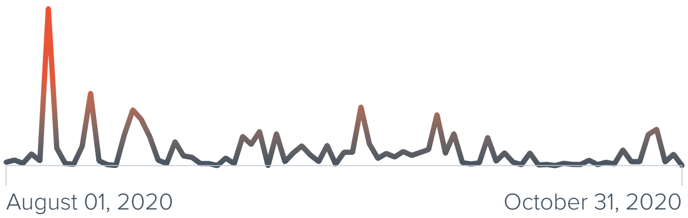
Lateral phishing attacks

So far, this report has focused on email messages that were delivered to users' inboxes from external sources. However, Barracuda researchers also saw a number of lateral phishing attacks; these are spear-phishing attacks that are sent internally, usually from potentially compromised accounts.

Hackers compromise a business email account and use it to launch attacks. These compromised accounts are highly valuable for attackers because they provide a perfect launchpad for further email attacks due to the high degree of trust associated with emails sent from these legitimate accounts.

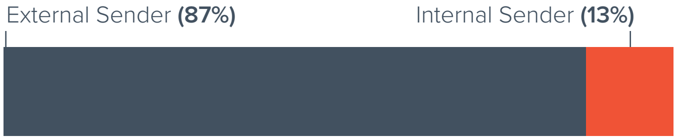
In this analysis, Barracuda researchers saw some large-scale lateral phishing attacks because attackers want to send as many emails out as possible before their malicious activity is detected and they're locked out of an account. Spikes in the trend graph show large numbers of malicious messages (often in the thousands) being sent from these compromised accounts.

Lateral phishing trends



When looking at the total number of malicious messages (both from internal and external sources), around 13% of messages can be classified as lateral phishing sent from potentially-compromised, internal email accounts. Some industries are more impacted by account takeovers and outbound fraud than others. Earlier this year, Barracuda researchers looked at the education sector, which is hugely impacted by this problem. In fact, in that analysis, Barracuda researchers detected more attacks that were sent out of email accounts owned by educational institutions than those coming in.

Spear-phishing emails: internal vs external sender



Not all these outbound messages were targeting the same organization as the compromised account. In fact, the vast majority of these messages (85%) targeted recipients with a different email domain. It should be noted that organizations can have different email domains in use for different employees, however it's safe to assume that most of these messages targeted external users.

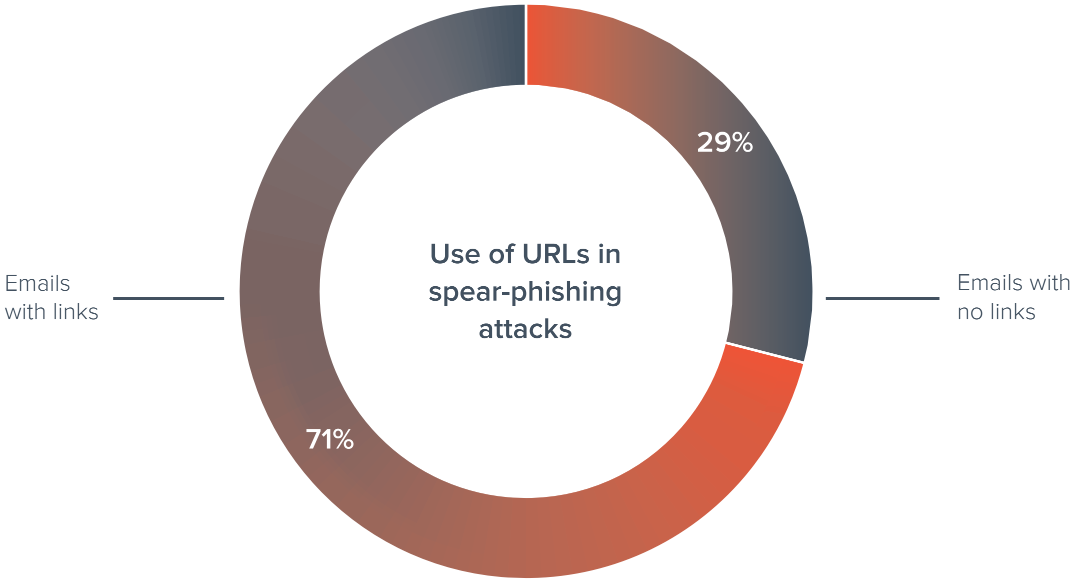
These internal messages do not pass through email gateways, leaving organizations exposed to threats they may deliver. Messages that originate from these compromised accounts, especially if they are coming from a colleague, can potentially have a higher success rate compared to other attacks because people trust messages sent from someone they know.

Organizations need to invest in protection against account takeover, by scanning messages sent internally within the organization and training users to recognize signs of a compromised account and email messages that come from compromised accounts.

Malicious URLs in spear-phishing emails

Most phishing emails will have a URL included, and more targeted spear-phishing attacks are no exception. Hackers use carefully-designed social engineering tactics to trick users into clicking on malicious URLs included in email messages. Around 71% of all spear-phishing attacks that Barracuda researchers examined in this analysis included at least one URL in the body of the email. These URLs usually lead to a phishing site that is used by hackers to steal login credentials or distribute malware.

Although a lot of organizations today have some form of link protection, many of these URLs will go unnoticed by traditional gateway filters. Cybercriminals use hacked websites or newly registered sites to create a nearly perfect replica of an official login page. These messages bypass scanners that look for malicious content to land in users' inboxes.

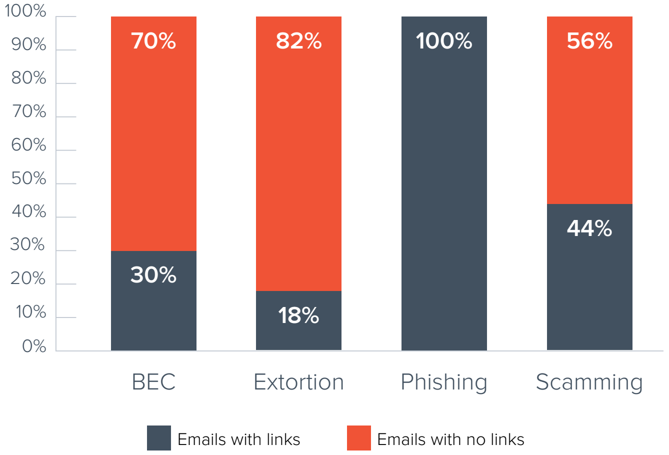


Attackers almost always include a link inside phishing attack emails because they help “phish” for sensitive information. However, link use varies in other attack types. Only 30% of BEC attacks included a link. Usually, the goal of these employee impersonation attacks is to establish trust and get a response from the victim.

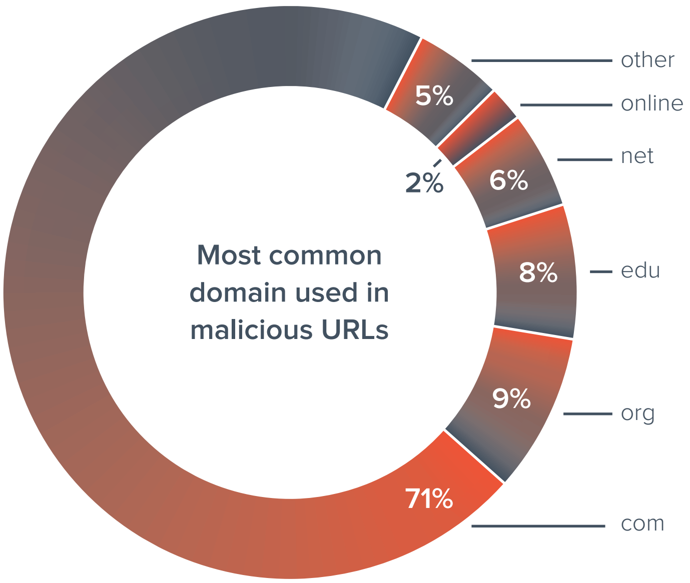
Extortion attacks, on the other hand, don’t look for a response and login credentials.

The scammers claim to have compromising information, allegedly recorded on the victim’s computer, and threaten to share it with all their contacts unless they pay up. Bitcoin is the form of payment typically demanded, with wallet details included in the message.

Use of URLs across different types of email attacks



The domains used in malicious URLs reflect those commonly used in everyday life. Most common domains used are .com, which is something people are very used to seeing in their email messages. Cybercriminals also adapt their attacks to their victims, using techniques to make these URLs appear more legitimate. For example, domains like .edu are commonly used to attack users within the education sector when hackers are looking to impersonate a familiar website or service.

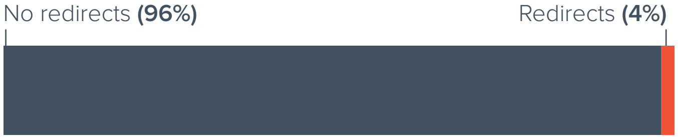


URL redirects in spear-phishing attacks

Cybercriminals use URL redirects in their attacks to add legitimacy to their phishing emails. These attacks redirect traffic to a malicious site using URLs embedded in a phishing email. These links may appear legitimate to end users but take them to a phishing site through multiple redirects. Attackers use Google and Adobe open redirects as they are often included in the allow lists of many security solutions.

Around 4% of all messages with links in the content took advantage of URL redirects. While setting up URL redirects requires additional work from attackers, these redirects are used to avoid detection of known phishing links.

Use of URL redirects in spear-phishing attacks

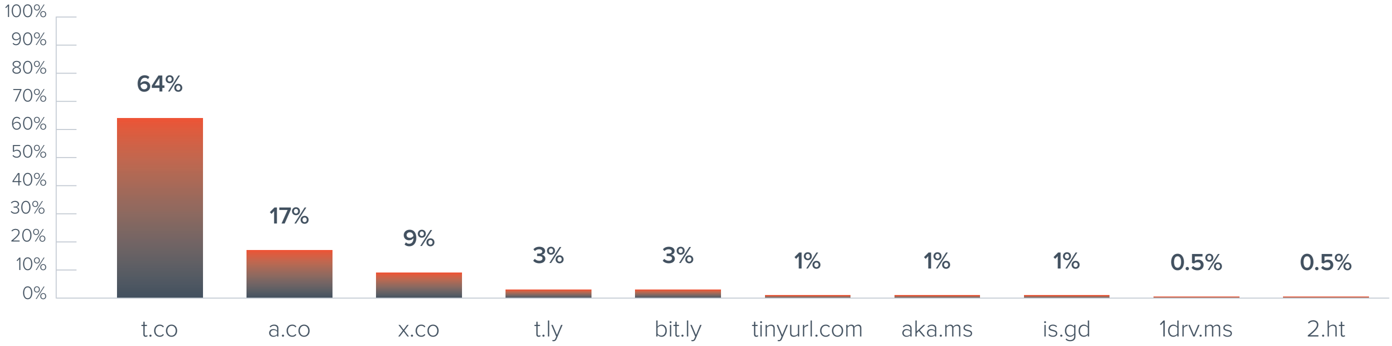


Use of URL shorteners in spear-phishing attacks

Cybercriminals increasingly use popular URL shortening services such as t.co, bit.ly, tinyurl.com, and others to embed malicious links in phishing emails. URL shorteners condense the link, so the actual link of the site becomes obscured with random letters or numbers. Using this tactic can disguise the true destination of the link, making it easier for hackers to trick their victims.

Just like other phishing messages, emails that contain shortened links appear to come from familiar entities with links directing victims to legitimate-looking sites that require login credentials to access information. There are several different services used by attackers with a preference for t.co—Twitter's service to shorten the links—which is used in about 64% of all attacks that included a shortened URL.

Top 10 shortening services used in spear-phishing attacks



Best practices to protect against spear phishing

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.

Your journey, secured.