Spear Phishing: Top Threats and Trends

Vol. 7 March 2022

Key findings on the latest social engineering tactics and the growing complexity of attacks

Cybercriminals are constantly refining their tactics and making their attacks more complicated and difficult to detect. In this in-depth report, Barracuda researchers share their insights on the most recent trends in social engineering and the new methods attackers are using to trick their victims.»

Barracuda
Your journey, secured.

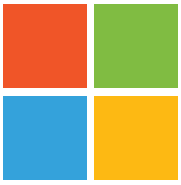
Table of Contents

Key findings

51% of social engineering attacks are phishing

Conversation hijacking grew almost **270%** in 2021

An average employee of a small business with less than 100 employees will receive **350%** more social engineering attacks than an employee of a larger enterprise



Microsoft is the most impersonated brand, used in **57%** of phishing attacks

1 in 5 organizations had an account compromised in 2021

Cybercriminals compromised approximately **500,000** Microsoft 365 accounts in 2021

1 in 3 malicious logins into compromised accounts came from Nigeria

Cybercriminals sent out **3 million** messages from 12,000 compromised accounts

The 13 email threat types continue to grow more complex

For years, security vendors have focused on protecting against email attacks, and the defense perimeters they built for customers have been effective at blocking most malicious or unwanted email messages. But that approach is no longer enough on its own.

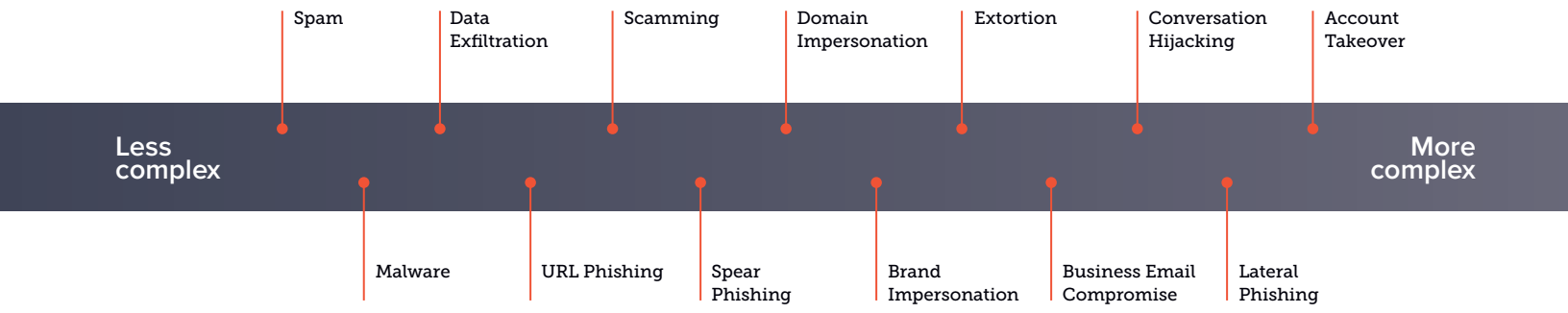
Even though organizations can stop millions of attacks, email threats are still succeeding because they are becoming increasingly complex and sophisticated. A significant shift is underway as cybercriminals move from volumetric to targeted attacks, from malware to social engineering, from operating as single hackers to forming organized criminal enterprises profiting from attacks that begin with a single phishing email.

Email protection that relies on rules, policies, allow or block lists, signatures, and other types of traditional email security are no longer effective against the constantly evolving threat of socially engineered attacks.

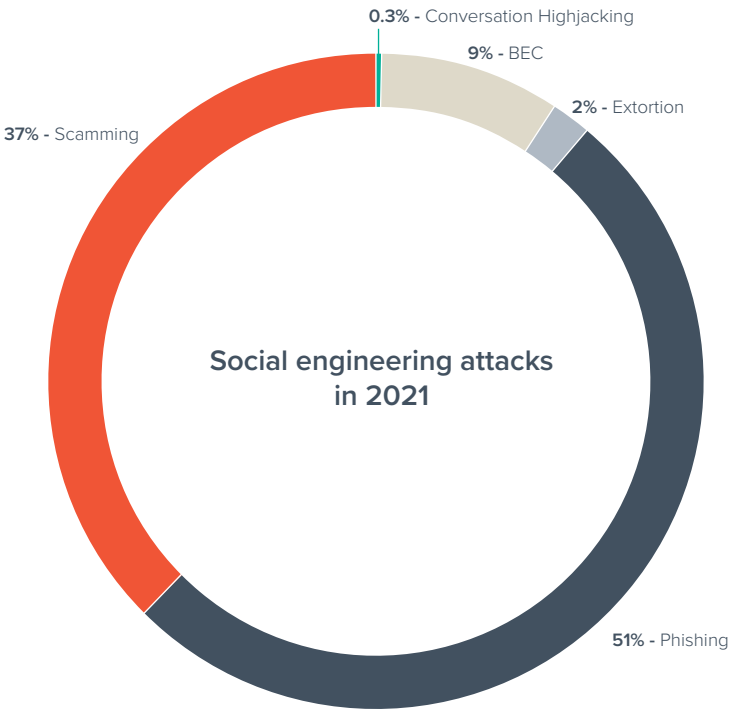
Hackers use a combination of tactics to trick their users into taking an action, such as giving up their credentials so that the attackers can get access to the company's environment, sharing sensitive information that could be sold or used for further attacks, or simply sending a payment, gift cards,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

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



We have been tracking five distinct categories of social engineering attacks:



Business email compromise, or simply BEC, attacks usually involve impersonating an individual either inside or outside of an organization. In 2021, these attacks made up 9% of all the socially engineered attacks we've seen, roughly the same as the year before. 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.

These attacks don't target just high-profile users. Our previous report showed that, for example, an organization's CFO is just as likely to be a target as anyone else in their department.

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 51% of all socially engineered threats we've seen in the past year. Almost all 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 by link protection technologies and delivering 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.

Hackers are starting to increasingly use phishing as part of their ransomware attacks. They impersonate well-known brands to lead victims to phishing sites and steal their login credentials. Once they have access to a company's accounts, they can spread ransomware from within, reducing the chances of it being detected.

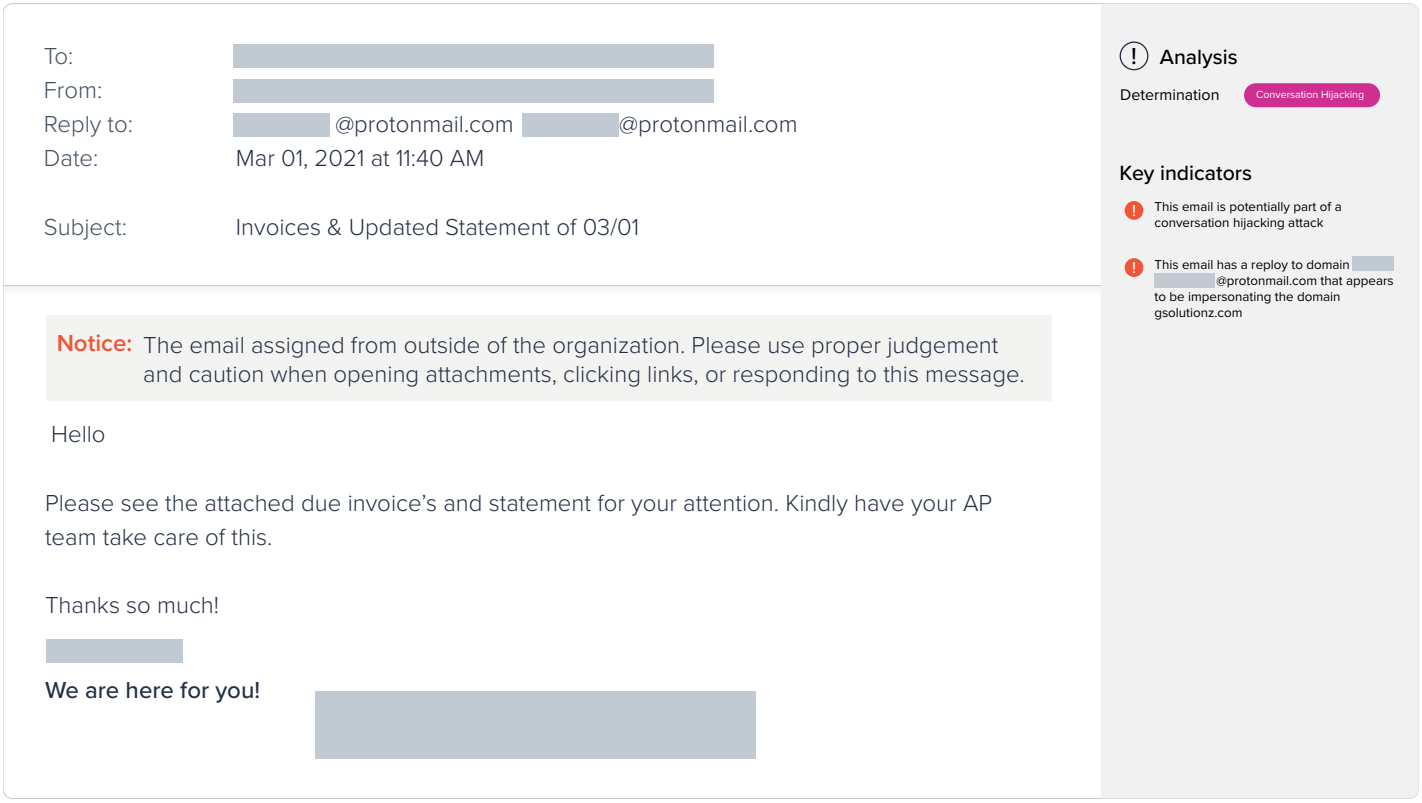
Extortion attacks make up only 2% of the total number of targeted phishing attacks we have seen in the past year. These attacks were mostly sextortion email threats, where hackers threaten to expose sensitive or embarrassing content to their victim's contacts unless a ransom is paid. Demands are usually a few hundred or a few thousand dollars and need to be paid in bitcoin, which is difficult to trace. In the UK, the number of sextortion cases reported to National Crime Agency increased by 88% between 2018 and 2020, and the number is expected to continue to increase.

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. Scamming attacks tend to be a little less targeted than the other types of attacks described above, but they represent 37% of all social engineering attacks we've detected in the past year and are still successful. Because hackers cast a wide net with the different types of scams they develop, these threats cost victims hundreds of millions of dollars overall.

For example, over the past couple of years hackers have used COVID-19 in their scams. In early 2021 we saw an uptick in vaccine-related scams with fake offers for early access to vaccinations, while by the end of 2021 cybercriminals switched tactics by focusing on selling COVID-19 tests to their victims.

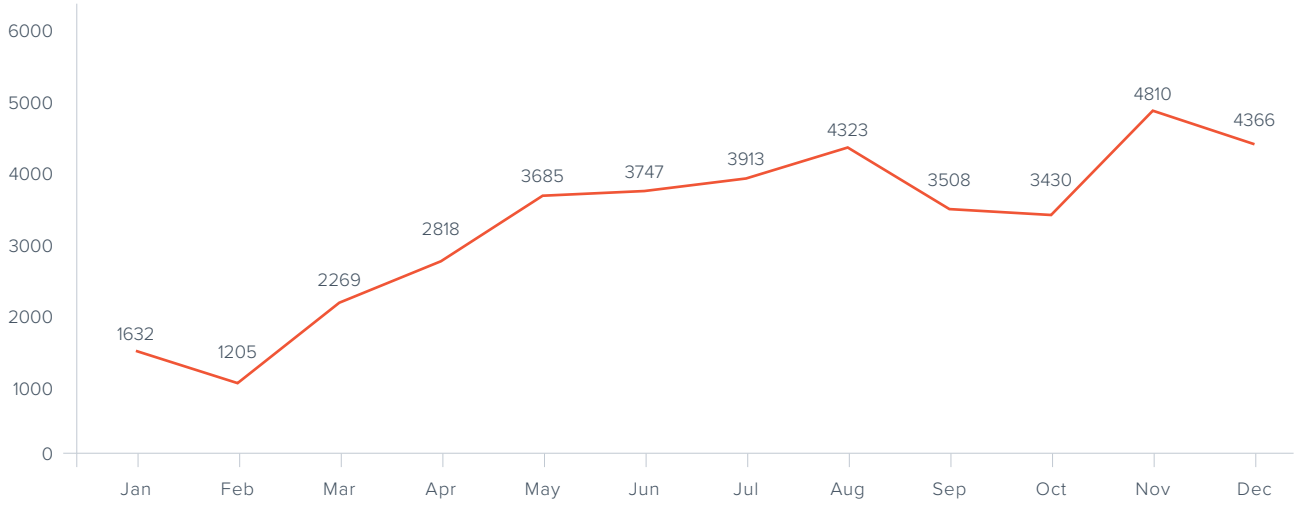
Conversation hijacking, also known as vendor impersonation, is a type of targeted email attack in which cybercriminals insert themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts or other sources.

Conversation hijacking is typically, but not always, part of an account-takeover attack. Attackers use phishing attacks to steal login credentials and compromise business accounts. They then spend time reading through emails and monitoring the compromised account to understand business operations and to learn about deals in progress, payment procedures, and other details. Criminals leverage this information including internal and external conversations between employees, partners, and customers, to craft authentic-looking and convincing messages, send them from impersonated domains, and trick victims into wiring money or updating payment information.



Conversation hijacking makes up only 0.3% of the social engineering attacks we've seen in the past year. However, even in small numbers they can be devastating for organizations. The overall volume of conversation hijacking has been growing over the years, and their popularity among hackers doubled in 2021. This is not surprising because while these attacks require a lot of effort from hackers to set up, the payout can be significant.

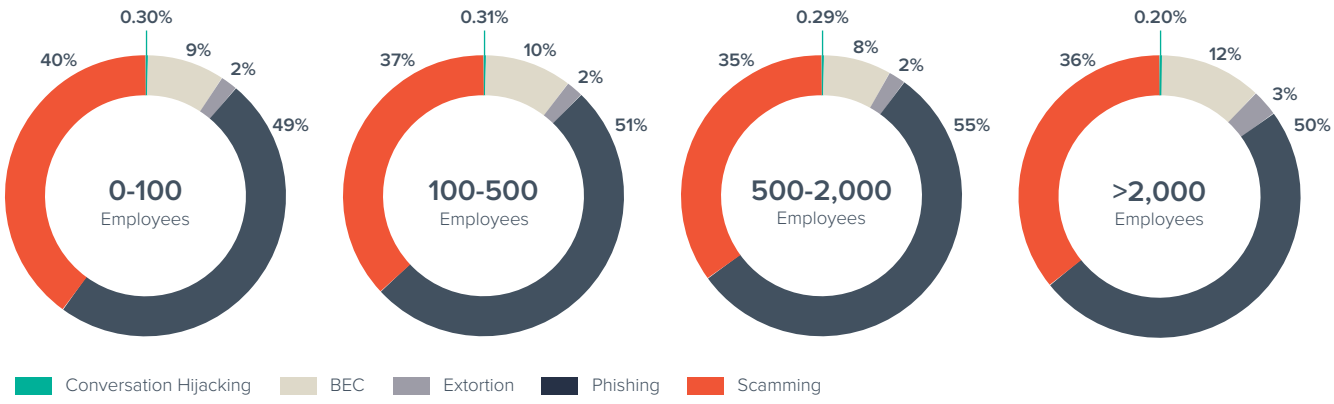
Conversation hijacking attacks in 2021



Targets of social engineering attacks

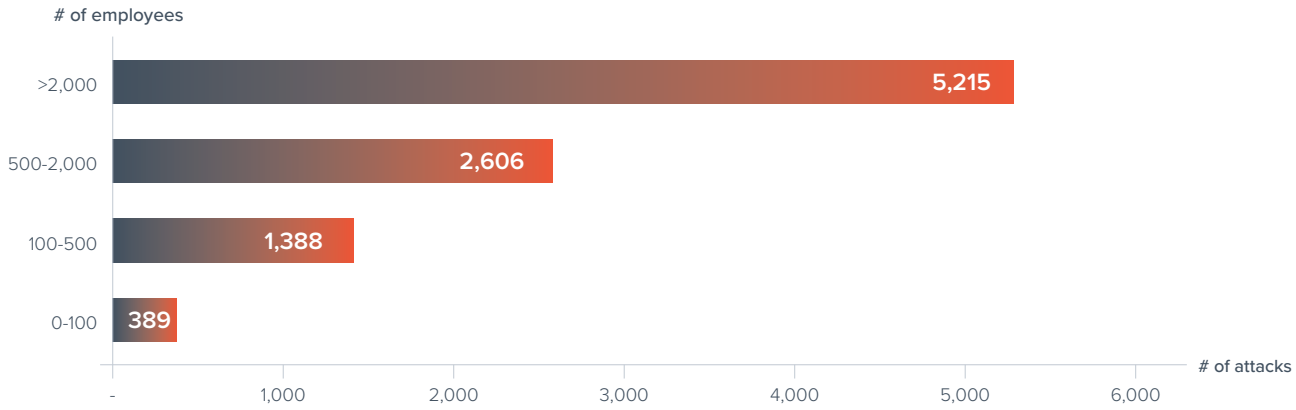
Email attacks do not discriminate based on the size of an organization. Larger enterprises with over 2,000 employees are only getting marginally more targeted business email compromise attacks than a small business with less than 100 employees. Staying vigilant about all attack types is important for every organization regardless of its size.

Types of attacks by organization size



It's also not surprising that larger organizations will face a larger volume of attacks simply due to their size. For example, a business with over 2,000 employees will be targeted with over 5,000 social engineering email attacks every year. That number is a lot smaller for organizations with fewer employees.

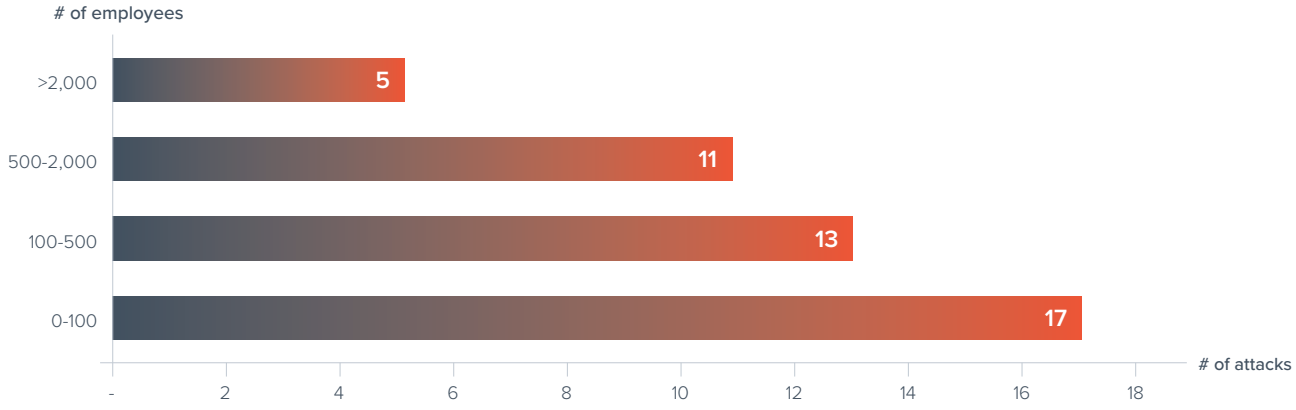
Average number of social engineering attacks per organization



However, the picture is reversed when it comes to the volume of attacks per mailbox. The smaller the organization, the more likely their employees are to be targets for an attack. In fact, an average employee at a small business with less than 100 employees will receive 350% more social engineering attacks than an employee of a larger enterprise. SMBs are an attractive target for cybercriminals because collectively they have a substantial economic value and often lack security resources or expertise.

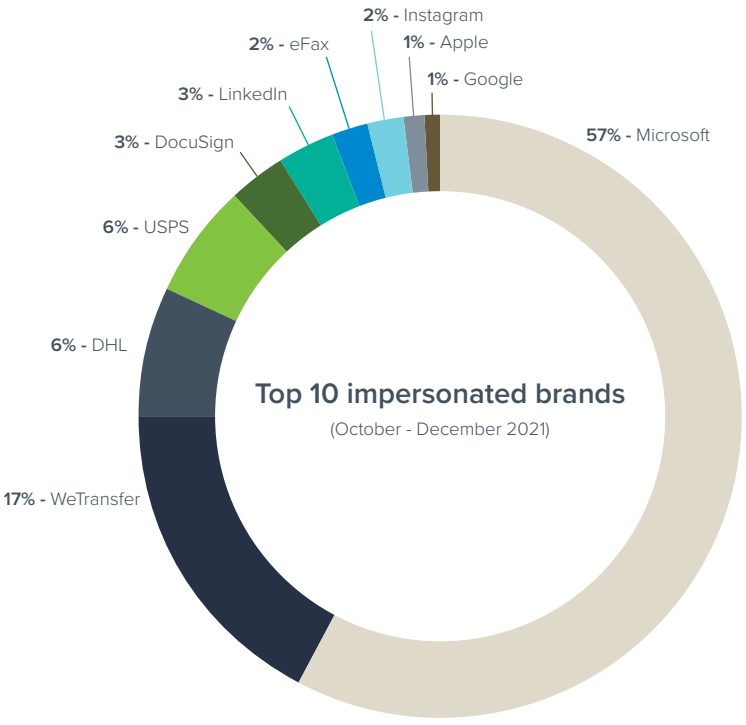
Smaller businesses should not overlook investment in security — both in terms of technology and user education. The cost of a breach can be a lot more devastating to smaller businesses. According to research by Cybersecurity Ventures, 60% of small businesses will close their doors six months after a security breach. With 43% of online attacks targeting small businesses, the cost of doing nothing can be too high.

Average number of social engineering attacks per mailbox



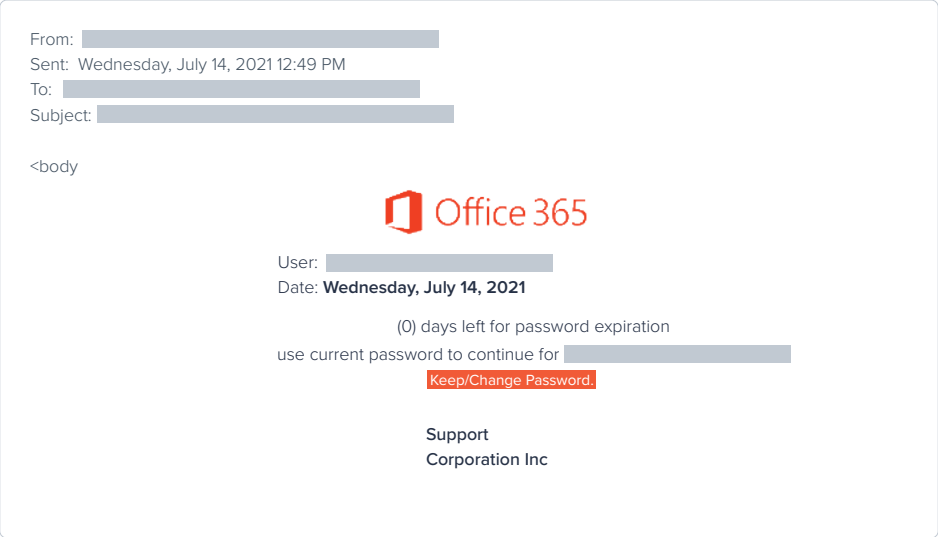
Top brand impersonations

Taking on the identity of a well-known and trusted brand is an old trick that many hackers use. We tend to expect and trust communication that comes from our favorite brands. When it comes to the top 10 brands used in brand impersonation attacks, the three top brands — Microsoft, WeTransfer, DHL — have not changed since 2019.



With 79% of organizations having migrated to Microsoft 365 and many more looking at doing so in the immediate future, it's not surprising that Microsoft brands remain a top target for cybercriminals.

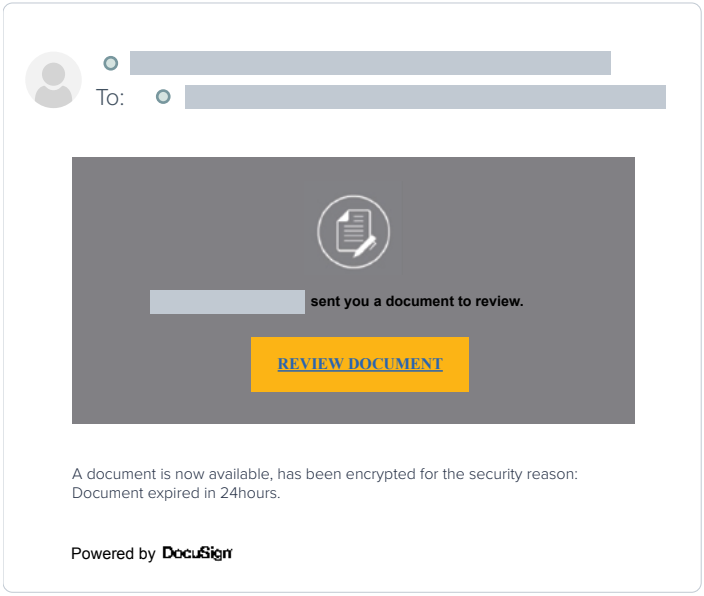
Looking at the top 10 impersonated brands, Microsoft was used in 57% of phishing attacks, up significantly from 43% in July 2021. Hackers are taking advantage of the increasing popularity of Microsoft's cloud-based services and remote working over the past two years. Cybercriminals will send fake security alerts or account update information to get their victims to click on the phishing link. The goal of these attacks is simple — steal login credentials to gain access to corporate networks. From there hackers can launch other phishing attacks including ransomware.



WeTransfer provides online file transfer services, allowing users to share files of large sizes that they may not be able to send directly through email. The brand was used in 17% of phishing attacks. The company is well aware of their brand being used in these types of attacks, and they warn their users to be vigilant. Organizations should include WeTransfer scams as part of their security awareness training.

DocuSign impersonations accounted only for 3% of phishing attacks, but these attacks can be devastating for organizations. With so many business practices moving online and to the cloud, getting a DocuSign for review is nothing out of the ordinary, so many employees won't think twice about clicking. Cybercriminals register fake DocuSign accounts or compromise already existing ones, then create and send files to their victims.

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



Account takeover on the rise

Adoption of Microsoft 365 has accelerated in recent years, fueled by the impact of the pandemic on remote working and cloud migration. Today, Microsoft reports over 200 million monthly active users. This popularity is not surprising as Microsoft 365 improves productivity and communication within organizations. Employees can now connect to their email accounts and access their data from anywhere. But so can hackers. Access to Microsoft 365 accounts is incredibly valuable because they act as a gateway to organizations and their data.

Account takeover is a form of identity theft and fraud where a malicious third party successfully gains access to a user's account credentials. By posing as the real user, cybercriminals can change account details, send out phishing emails, steal financial information or sensitive data, or use any stolen information to access further accounts within the organization.

Account takeover is one of the fastest growing threats. In 2021, roughly 1 in 5 organizations (20%) had at least one of their Microsoft 365 accounts compromised. This means that in 2021 hackers managed to compromise around 500,000 Microsoft 365 accounts around the globe. Without the right level of protection, account takeover can go undetected and cause real damage to the organization, its business partners, and its customers.

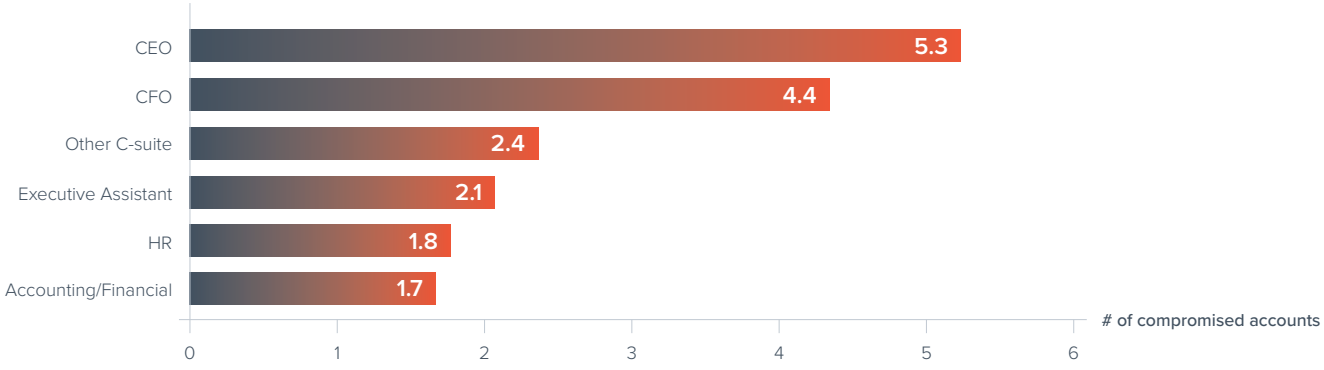
1 in 5 organizations had their Microsoft 365 accounts compromised.

C-level executives are a main target of account takeover

Hackers target high-value accounts for takeover. Accounts of CEOs and CFOs are almost twice as likely to be taken over compared to average employees. Once they have access, cybercriminals use these high-value accounts to gather intelligence or launch attacks within an organization.

Executive assistants are also a popular target as they often have access to executive accounts and calendars and usually can send messages out on behalf of executive teams.

Account takeover across business functions (per 1,000 mailboxes)



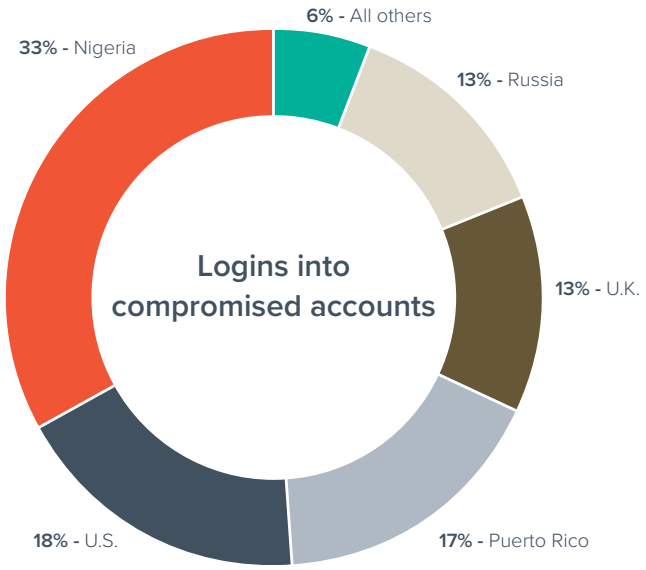
Four stages of account takeover

Infiltration

Microsoft is one of the most impersonated brands. Around 57% of phishing attacks impersonate one of Microsoft's brands such as Microsoft 365, OneDrive, SharePoint, or others. Hackers use social engineering tactics to trick users into visiting a phishing website and sharing their log in credentials, which allows the hackers to infiltrate the system.

Reconnaissance

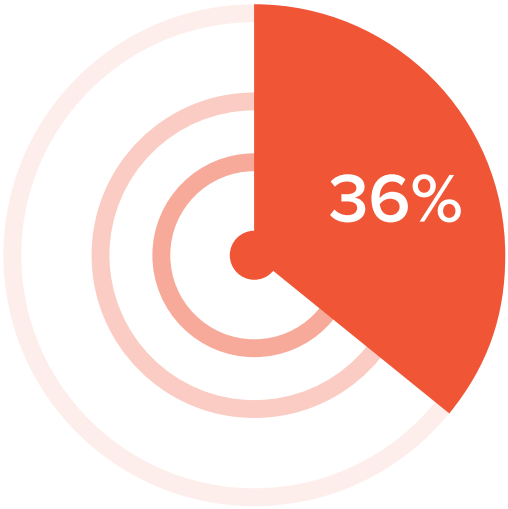
Once they have access to an organization's network, hackers rarely launch their attacks right away. They are using the compromised account to monitor and track activity at your company. Then they use that information to their advantage. Most hackers in the attacks we analyzed log in from just a few countries from around the globe, with Nigeria at the top of the list. One in three fraudulent logins into compromised accounts came from Nigeria.

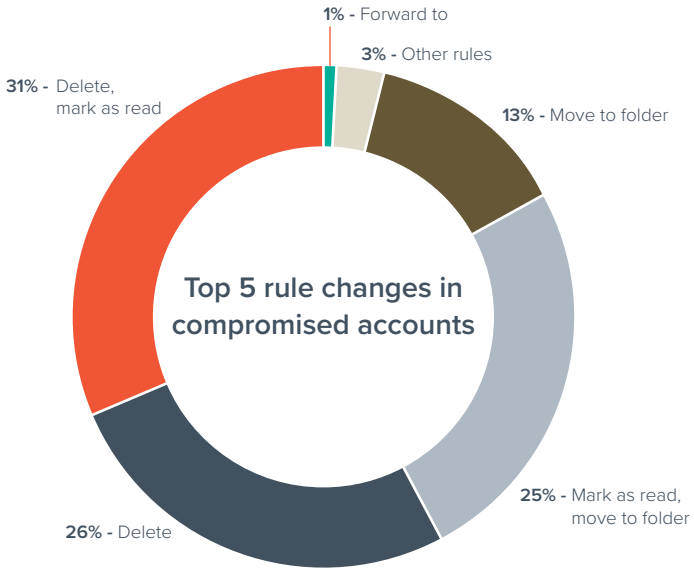


Once they're inside an account, hackers create forwarding rules or scripts to hide and delete any email that they send from the compromised inbox. Suspicious inbox rules are often one of the signs of an account takeover. A full 36% of organizations that had an account compromised had hackers set up malicious inbox rules to hide their activity. In fact, hackers on average created two rules for each compromised account.

In over half of the cases when hackers set up malicious rules, they set rules to delete messages from accounts so that account owners would not notice any suspicious email activity. Another popular action included moving messages to a specific folder and often marking it as read. Hackers will come back to the account later and review messages in the folder.

Compromised accounts with malicious rule changes





Credential harvesting and monetization

Hackers use compromised accounts as a launchpad for their attacks. They target high-value accounts trying to steal their credentials and then move laterally within an organization. Overall, compromised accounts are used in a wide range of attacks from spam to business email compromise. Our research of almost 12,000 compromised accounts showed that they were used to send over 3 million malicious messages and spam in 2021.

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 in 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.

- **Monitor inbox rules and suspicious logins.** Use technology to identify suspicious activity, including logins from unusual locations and IP addresses, a potential sign of a compromised account. Be sure to also monitor email accounts for malicious inbox rules, as they are often used as part of account takeover. Criminals log into the account, create forwarding rules, and hide or delete any email they send from the account, to try to hide their tracks.

- **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.

- **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.

- **Automate incident response.** An automated incident response solution will help you quickly clean up any threats found in users' inboxes, which will make remediation more efficient for all messages going forward.

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-first, 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.