PERCEPTION POINT™

# 2024 ANNUAL REPORT

*Cybersecurity Trends & Insights*

PRESENTED BY PERCEPTION POINT

PERCEPTION POINT™

# Table of Contents

# Executive Summary

Over the course of 2023 organizations continued to expand their workspace technologies with additional web-based productivity tools and SaaS applications. In turn, cyber attackers adopted increasingly sophisticated evasion techniques, like employing malicious QR codes and using generative AI to attack organizations from diverse industries across email, enterprise browsers, and collaboration apps. These trends underscore the urgent need for organizations to implement robust cybersecurity measures to protect a more digitally dependent workforce.

This report serves as a comprehensive guide for organizations seeking to understand the overarching cybersecurity landscape of 2023 and beyond. Based on data collected by Perception Point's advanced threat detection platform and the company's Incident Response service's in-depth analysis, the report examines the most pervasive attacks in 2023. By providing insights into emerging threats, evolving attack vectors, and industry-specific targeting, Perception Point aims to equip organizations with the knowledge needed to fortify their cybersecurity posture.

Key takeaways include:

- 1 in every 5 emails was not legitimate.
- Social engineering/BEC attacks have increased by 1,760% since 2022.
- External ATO attacks grew by 350%.
- Phishing remained the most prevalent threat vector accounting for more than 70% of all attacks.
- Two-step phishing attacks grew by 175%.
- Quishing (QR code phishing) accounted for 2% of total threats.
- The total number of attacks users received every month grew by 8%.
- Phishing attacks via the web browser increased in frequency from 60% of all browser-based attacks in 2022 to nearly 80% of all browser-based attacks in 2023.
- Malware distribution accounted for 65% of attacks in Microsoft 365 applications including OneDrive, SharePoint and Teams.
- Evasive threats and malware accounted for more than 50% of attacks targeting CRMs like Zendesk and Salesforce.

# Top Attack Trends of 2023

Throughout the year, Perception Point's cybersecurity analysts observed a spectrum of novel attacks, a notable escalation in the severity of these attacks, and an expansion of the attack surface. This section delves into pivotal trends that significantly influenced the cybersecurity landscape of 2023: the emergence of GenAI-enhanced cyber threats; the rise of quishing attacks; two-step phishing attacks; account takeover attacks.

## GenAI Powered BEC Attacks

This past year has been defined by the advances and widespread usability of generative AI (GenAI). The advent of accessible AI has in turn given rise to more intricate and deceptive malicious campaigns. Cybercriminals have harnessed the power of GenAI to enhance and scale their attacks, much to the detriment of defenders and targets alike. This emerging trend presents substantial obstacles for organizations when it comes to identifying and countering threats.

Business Email Compromise (BEC) attacks have seen perhaps the most success through the addition of GenAI. BEC attacks involve cybercriminals posing as authentic business stakeholders through fraudulent emails, seeking funds or confidential information from employees and business associates. These impersonation-driven attacks, using social engineering, pose an escalating challenge in detection, exploiting the susceptibility of busy employees who can be easily deceived. Unlike preventing malicious files and URLs, traditional security systems such as secure email gateways fall short in addressing BEC attempts because these threats rely on text-based social engineering tactics.

***BEC attacks increased at a rate of 1760%, from 1% of all attacks in 2022 to 18.6% of all attacks in 2023.***

Perception Point has implemented an LLM-based detection engine to catch BEC attacks originating from LLMs. This method enables organizations to fortify their security measures, swiftly identifying these advanced attacks and minimizing the potential financial setbacks and damage to reputation associated with BEC incidents.

*According to Osterman Research, cybercriminals have shown rapid adoption of AI tools to their favor with 91.1% of organizations reporting that they have already encountered email attacks that have been enhanced by Artificial Intelligence (AI), and 84.3% expecting that AI will continue to be utilized to circumvent existing security systems ("The Role of AI in Email Security," 2023).*

As the landscape of generative AI-driven cyber threats continues to expand, organizations must stay vigilant and proactive in their cybersecurity strategies. By harnessing state-of-the-art technologies and methodologies such as Perception Point's LLM-based detection, organizations can enhance their resilience and safeguard their crucial assets against these evolving threats.

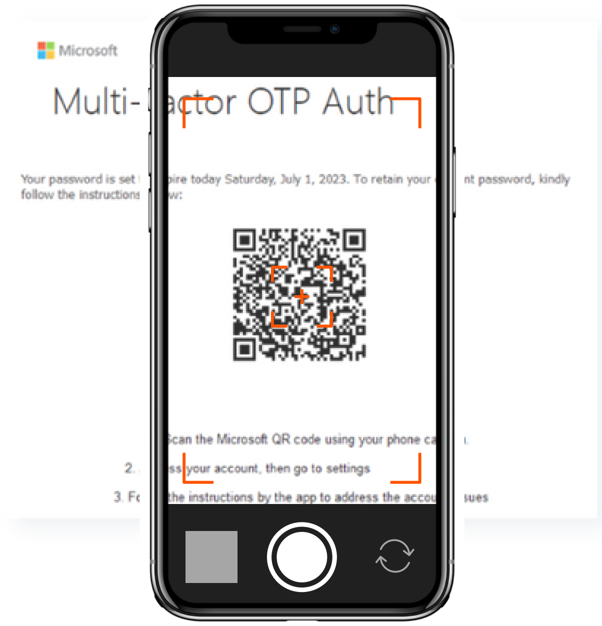
Click here to read "An AI for an AI: LLM-Based Detection of GPT-Generated BEC Attacks."

# Quishing

In 2023, there was a rapid increase in the number of quishing attacks targeting organizations of all sizes, worldwide. Quishing, or QR code phishing, is a somewhat recent derivative of phishing attacks, leveraging the prevalence and inherent trust of QR codes in modern life. The extensive use of QR codes across various domains has made them an attractive vector for cybercriminals.

Through quishing, attackers managed to at first bypass many security vendors, compounding the new tactic with deceptive social engineering when defensive strategies and awareness training were instituted. What makes the use of QR codes in emails difficult to detect is that the content and intent of QR codes are not immediately apparent. When coupled with convincing language, impersonation of trusted entities, and a sense of urgency to manipulate users, quishing can be even more difficult to detect and nearly impossible for users to avoid.

The tactic involves redirecting individuals to a malicious web page, like a spoofed login page, upon scanning a QR code, which ultimately shifts the threat landscape to mobile devices. Scanning a QR code on a personal device, removed from the protection of a workspace environment, exposes users to heightened risks.



Microsoft

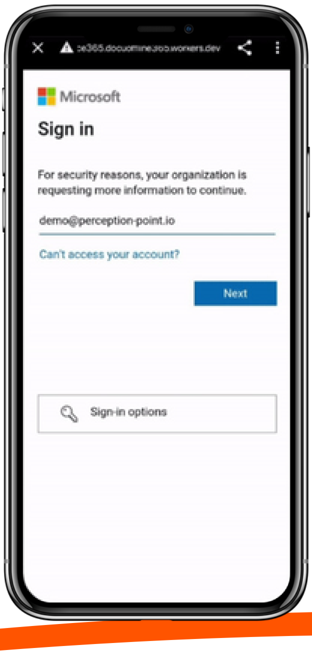
Multi- actor OTP Auth

Your password is set pire today Saturday, July 1, 2023. To retain your nt password, kindly follow the instructions w:

Scan the Microsoft QR code using your phone ca .

2. ss your account, then go to settings

3. Fo the instructions by the app to address the accou sues



oe365.docuomine.joo.workers.dev

Microsoft

Sign in

For security reasons, your organization is requesting more information to continue.

demo@perception-point.io

Can't access your account?

***In 2023, 1 out of 18 (6%) QR codes sent via email were malicious. On a grander scale, 2.7% of all phishing incidents involved malicious QR codes, meaning that quishing accounted for 2% of all threats in 2023.***

To combat this escalating threat across not only email, but also web browsers and collaboration apps, Perception Point has adopted a simple and secure approach, focusing on actual prevention of quishing rather than mitigation or education. By scanning all QR codes and following the URLs within them, Perception Point uses image recognition and AI to detect and block quishing attacks at their source before they even reach the end user.

Click here to read "Navigating the Next Wave of Quishing Attacks."

## Two-Step Phishing

***The prevalence of two-step phishing attacks increased by 175% in 2023,*** highlighting the escalating threat posed by this sophisticated tactic. Unlike traditional phishing methods that rely on generic emails, messages, and social engineering tactics, two-step phishing involves a more deceptive approach. The additional step in the attack chain helps avoid detection.

In these attacks, threat actors exploit compromised legitimate email accounts or legitimate services and hosting sites. For example, a user receives an email or message in a collaboration app, notifying them of an expired password, which prompts them to click a link to reset the new password. This link redirects them to a usually legitimate hosting service, often utilized for website building, web hosting, or file sharing. The exploitation of the reputation of these well-known domains helps evade detection, particularly as these platforms are commonly used for legitimate business collaboration.

What distinguishes two-step phishing attacks is their wide-ranging scope, exploiting over 400 commonly used services. These include services like Salesforce, SharePoint, Adobe, and even public Jira tickets.

The second step of the attack occurs when users are presented with another clickable element on the seemingly legitimate webpage or file. This link redirects them to a spoofed page designed to illicitly harvest sensitive information, such as login credentials or credit card details.

Despite the apparent authenticity of these emails, messages, files, and websites, they pose a significant threat. Many security solutions struggle to detect two-step phishing attacks due to the high sender reputation of the compromised accounts and the utilization of familiar services.

The severity of the issue is underscored by the alarming rise in two-step phishing attacks throughout 2023, with incidents increasing by threefold compared to previous years.

Read the 2024 State of Phishing report here.

## Account Takeover

Account Takeover (ATO) usually starts with a phishing attack in order to gain unauthorized access to a user's email account. Subsequently, the attacker can leverage this compromised account to conduct two-step phishing, malware and thread hijacking attacks.

Targeted emails can then be sent to individuals known to the victim, which can be within the same organization or customers. These communications are crafted to appear as though they originate from a trusted source, often containing prompts for recipients to click on embedded links or text within the message body or requests to change payment terms.

For example, in email, because the account was compromised, the attacker can see the ongoing emails between the victim and their contacts. The attacker will search for payment-related emails that contain information about bank accounts, invoices, and deposits and wait for the opportune time to hijack the thread and continue the conversation from a newly registered domain that resembles the original domain.

By capitalizing on recipients' familiarity and past communication patterns with the apparent senders, attackers increase the likelihood of successful phishing, BEC and VEC attempts.

***In 2023, external account takeover attacks increased 350%.***

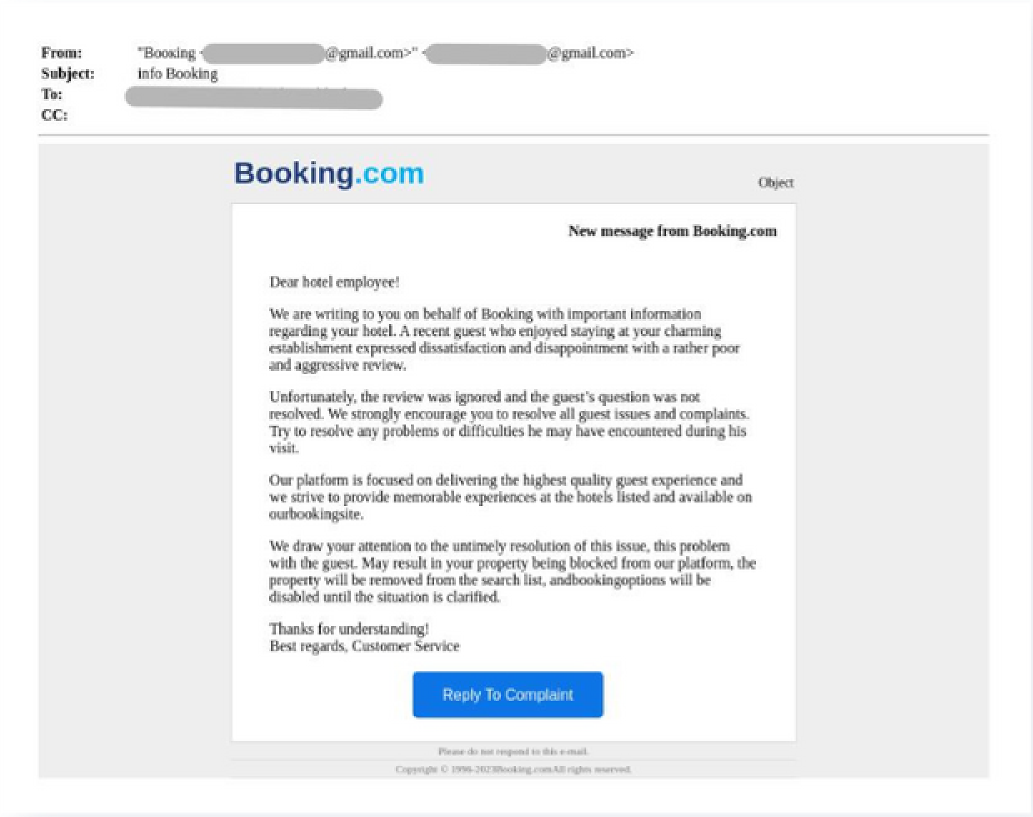
Read about ATO, email thread hijacking and more here.

# Industry Spotlight: Hospitality

The hospitality sector is grappling with an upswing in threats fueled by various social engineering techniques employed by threat actors seeking to defraud hotels, guests, and popular travel sites. From utilizing InfoStealer malware to exploiting platforms like Booking(.)com, attackers have intensified their efforts against hotels, putting both establishments and their guests at risk.

Threat actors have employed evasive tactics and technologies, specifically tailored to exploit industry practices and business relationships in the realm of targeted phishing and malware attacks. To conduct these campaigns, attackers leverage advanced tools such as GenAI and sophisticated phishing kits, emphasizing the substantial gravity of these modern threats.

Examining a recent series of phishing attacks intercepted by our advanced threat prevention platform and analyzed by security experts, these attempts share a common payload: the theft of Booking(.)com credentials from hotels. The primary objective of these attacks is to gain access to Booking(.)com hotel profiles, a stepping stone towards the larger goal of acquiring guest information, including emails, phone numbers, and financial details. Armed with this data, attackers can execute large-scale phishing campaigns against hotel guests.



**From:** "Booking <[redacted]@gmail.com>" <[redacted]@gmail.com>
**Subject:** info Booking
**To:** [redacted]
**CC:**

Booking.com

Object

**New message from Booking.com**

Dear hotel employee!

We are writing to you on behalf of Booking with important information regarding your hotel. A recent guest who enjoyed staying at your charming establishment expressed dissatisfaction and disappointment with a rather poor and aggressive review.

Unfortunately, the review was ignored and the guest's question was not resolved. We strongly encourage you to resolve all guest issues and complaints. Try to resolve any problems or difficulties he may have encountered during his visit.

Our platform is focused on delivering the highest quality guest experience and we strive to provide memorable experiences at the hotels listed and available on ourbookingsite.

We draw your attention to the untimely resolution of this issue, this problem with the guest. May result in your property being blocked from our platform, the property will be removed from the search list, andbookingoptions will be disabled until the situation is clarified.

Thanks for understanding!
Best regards, Customer Service

Please do not respond to this e-mail.

Copyright © 1996-2023Booking.comAll rights reserved.

# Attack Types by Channel

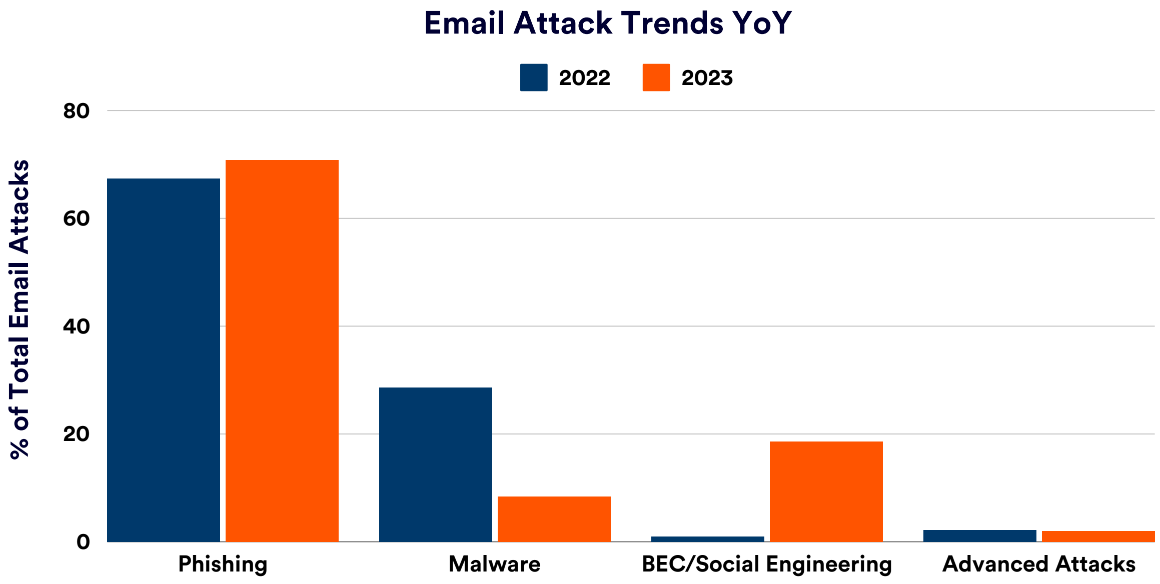
This section explores the spectrum of cyber threats encountered in 2023, providing nuanced insights into their distinctive features and implications. Our analysis delves into the prevalence and gravity of a range of attack vectors, including phishing, social engineering (BEC and account takeover), malware, and advanced attacks. The data is broken down into multiple channels, including email, web browsers, and collaboration applications.

## Email - The #1 Attack Vector

When analyzing email as an attack vector, the first thing to consider is spam - a major deterrence to workspace productivity. Spam accounted for 19% of all email traffic in 2023. On average, each user was sent a staggering 74.5 instances of spam per month, revealing the relentless onslaught of unwanted and potentially harmful content. However, the true cause for concern emerges in the realm of targeted malicious attacks, which surged to 2.9 per user per month, marking an 8% increase compared to the previous year.

***Phishing is still the top cyber threat, accounting for more than 70% of all attacks, with little change from the previous year.***

Phishing is the fraudulent practice of attempting to trick users into disclosing sensitive information. Perception Point thwarts these attacks through the use of advanced engines, like the recursive unpacker and image-recognition engine. It verifies URLs using data from top reputation engines and integrates threat intelligence from leading sources. This multi-layered approach ensures proactive protection against evolving phishing threats.



Looking at the progression of email attacks from 2022 to 2023, social engineering attacks stand out. ***These attacks, comprised largely of BEC incidents, increased at a rate of 1760%, from 1% of all attacks in 2022 to 18.6% of all attacks in 2023.***

Perception Point employs an AI-powered solution specifically designed to combat BEC and impersonation attacks, which are among the fastest growing and costliest social engineering threats. These attacks often rely on text-only emails, appearing to be from a known entity and lacking any malicious attachments. Instead, threat actors exploit spoofed domains and compromised accounts to appear legitimate, aiming to deceive recipients into transferring funds or sharing confidential data.

To counter these threats, Perception Point's anti-BEC strategy integrates advanced techniques such as Supply-Chain Recognition to identify trusted domains, the GenAI Decoder™ to spot AI-generated text patterns, and Content & Anomaly Analysis to extract sensitive information and detect fraud indicators. Additionally, Advanced Anti-Spoofing measures strengthen defenses against spoofing attacks and domain impersonation. This multi-layered approach effectively safeguards organizations against BEC threats, minimizing the risk of financial loss and data breaches.

***In 2022, malware accounted for 28.6% of all cyber threats, but by 2023, it notably declined to 8.4%, potentially influenced by the prevalence of social engineering attacks. Advanced attacks remained steady at 2.2% of all threats in 2023, underscoring their persistent threat to organizations.***

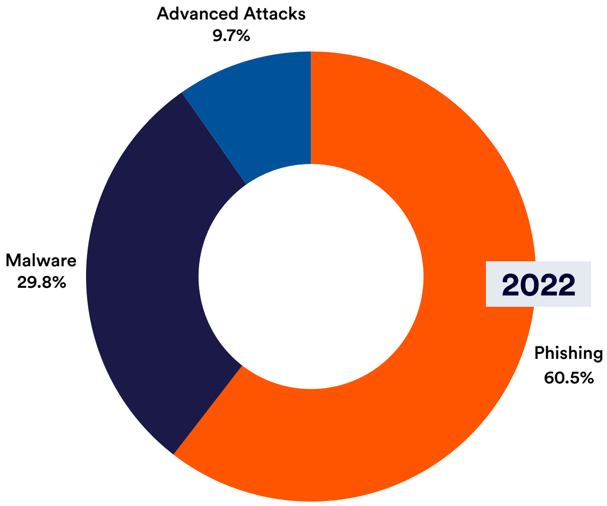
Advanced attacks, characterized by their complexity and precision, often entail multi-step processes including reconnaissance and malware delivery, bolstered by sophisticated evasion techniques.

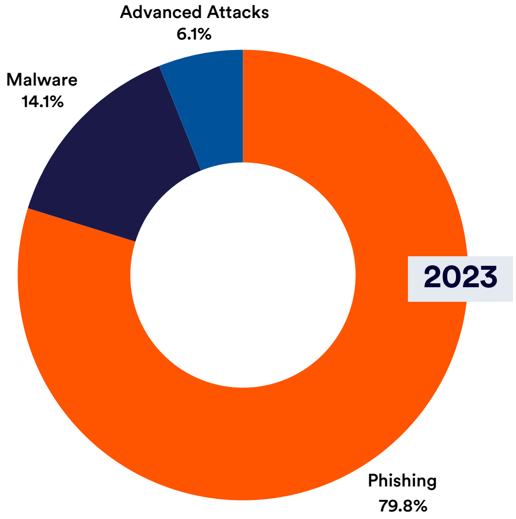
To counter such threats, Perception Point employs cutting-edge static and dynamic engines like the Recursive Unpacker and the HAP™. The Recursive Unpacker meticulously dissects content to reveal deeply embedded links and files, while the HAP™ intercepts exploitation attempts, neutralizing unknown threats at the exploit stage. This proactive defense is particularly crucial in combating zero-day attacks, where traditional detection methods may fall short.

The revelation that advanced attacks constitute a small fraction of threats in 2023, juxtaposed with the rise in social engineering attacks, highlights the evolving cybersecurity landscape, emphasizing the necessity for resilient and adaptable defense strategies.

# Web Browser

Web-based threats are notably more perilous in nature than their email counterparts, despite appearing at a lower frequency. Browser-based attacks are primarily made up of phishing, malware (e.g., auto-downloads of files and archived files), and advanced attacks.





***Phishing attacks increased in frequency for the browser from 60% of all attacks in 2022 to nearly 80% of all attacks in 2023. Malware followed, decreasing by almost half from 30% of all browser attacks in 2022 to 14% in 2023. Advanced attacks also decreased from 10% of all attacks in 2022 to 6% in 2023, likely due to the increase of phishing attacks.***

The Gartner Hype Cycle for Endpoint Security report notes that “enterprise browsers represent a new way of delivering security services and receiving real time intelligence from existing security agents layered into the OS. Today, many of these products are able to deliver some important features and benefits of other web security products; however, trade-offs still remain. This gap is expected to close over time as the category becomes more mature and more partners enter the ecosystem.”

To address these threats, Perception Point has developed a browser extension, part of the Advanced Browser Security offering. Perception Point’s browser extension excels in dynamic scanning within the browser environment, swiftly detecting and pinpointing malicious behaviors like phishing pages and web vulnerabilities. This solution plays a pivotal role in account takeover investigations, offering insights into services used and login activities, aiding in identifying compromised accounts, addressing password reuse, and enhancing overall security awareness.

With browser-specific policies, the extension reinforces organizational security by mitigating potential risks and internal threats. Integrated seamlessly with standard web browsers, such as Chrome, Edge, Safari, Firefox, and more, this enterprise-grade security solution combines advanced threat detection with browser-level governance and DLP controls to empower organizations.

# Cloud Collaboration Apps

Email and web continue to be the main threat vectors for attackers, yet the evolution of the modern workspace has made cloud-based applications appealing targets. As attackers continually innovate to breach organizations, the need to monitor and safeguard these applications has never been more critical. ***In 2023, 75% of organizations scanning over 500 files a month were attacked.*** This section explores the 2023 attacks launched against Microsoft 365 applications (SharePoint, OneDrive, Teams), Salesforce, and Zendesk.

According to an Osterman Research paper, “Many newly adopted cloud collaboration apps and services have only been around for a few years. Worryingly, the rate of malicious incidents against these new apps and services is already 60% of what organizations experience against their email services. Threat actors have responded quickly to the emergence of new channels for employee productivity and collaboration.”

*Click here to download the full Osterman Research report, “The Rise of Cyber Threats Against Email, Browsers and Emerging Cloud-Based Channels.”*

## Microsoft 365 Collaboration Apps

The increasing adoption of Microsoft cloud products has amplified the appeal of these collaboration channels. This includes platforms such as SharePoint, OneDrive, and Teams, which have become significant targets for cyber threats. Attackers exploit vulnerabilities in file-sharing features or inject malicious links into collaboration channels to infect users' devices and compromise organizational networks.

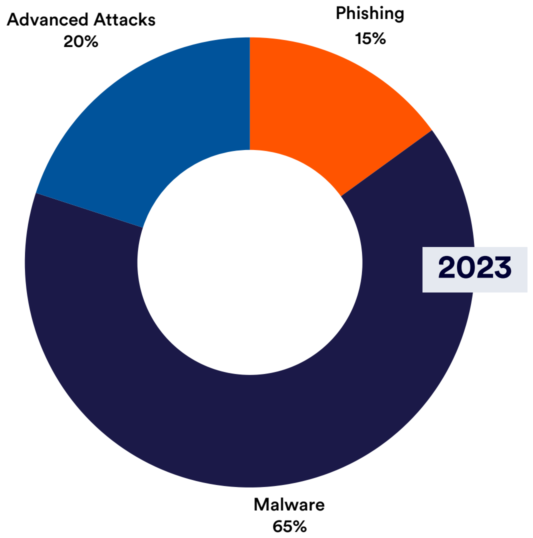
***In 2023, Microsoft 365 channels faced notable challenges, with malware emerging as the most prevalent attack, constituting 65% of all incidents.***

***Advanced attacks followed at 20%, and phishing at 15%, underscoring the severity of these threats and the heightened danger they pose.***

As organizations embrace cloud-based applications for remote access by employees, customers, and suppliers, conventional security measures offer minimal protection. Microsoft's native, built-in security features in its cloud products are a valuable starting point. However, they exhibit inherent limitations, leaving entry points vulnerable to evolving cyber threats.

The integration and interconnectedness of M365 apps provide attackers with avenues to conduct lateral movement within organizations' environments, facilitating data exfiltration, espionage, or disruption of critical operations. As a result, organizations must prioritize direct cybersecurity measures for these apps to mitigate the risks posed by these evolving cyber threats targeting M365 apps.

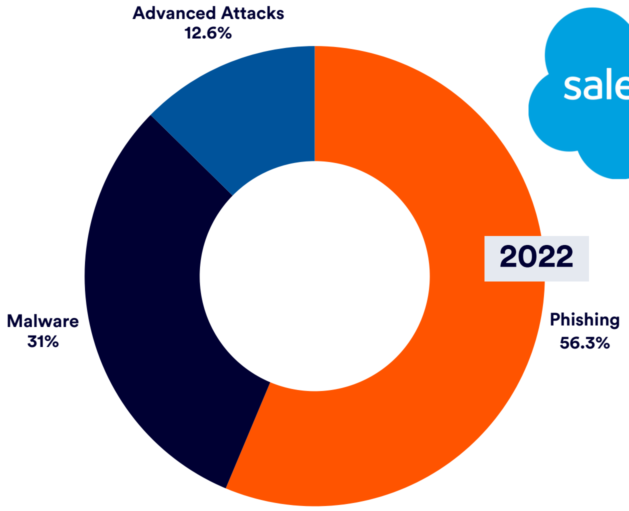
Perception Point's Advanced Security for Microsoft 365 is crafted to identify and thwart elusive and emerging attacks that circumvent Microsoft's native defenses. This solution enhances or replaces the threat prevention capabilities of EOP and Defender to their maximum potential by incorporating next-gen engines and employing unlimited dynamic scanning.

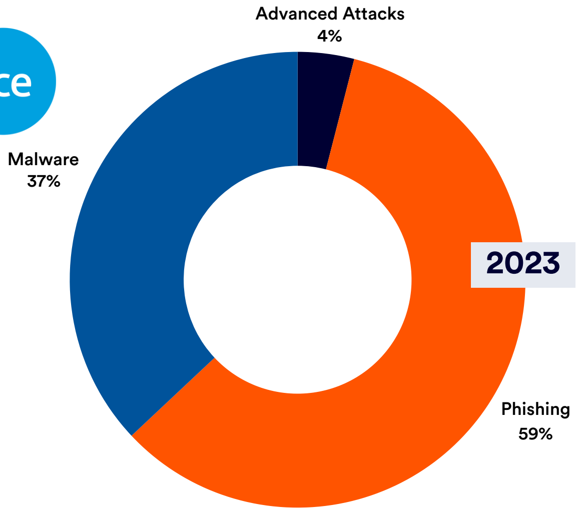


## Salesforce

Salesforce is a crucial tool for managing relationships with external users like customers and partners. However, this introduces a vulnerability as users upload diverse content into the organization's Salesforce environment, heightening the risk of cyber attacks. In 2023, attacks targeting Salesforce remained consistent with the previous year.

***Phishing, via embedded links in files and forms, continued to lead at 59% of all attacks (compared to 56.3% in 2022), with malware following closely at 37%, marking an increase from 31% in 2022. Advanced attacks decreased from 12.6% in 2022 to 4% in 2023, potentially influenced by the rise in malware attacks.***





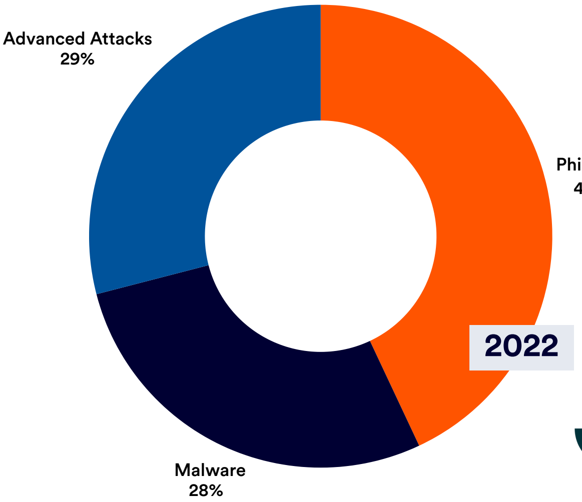
To counter these threats, Perception Point's Salesforce Advanced Threat Protection solution swiftly and accurately identifies and prevents all forms of malicious content from breaching organizations through Salesforce, ensuring optimal security.

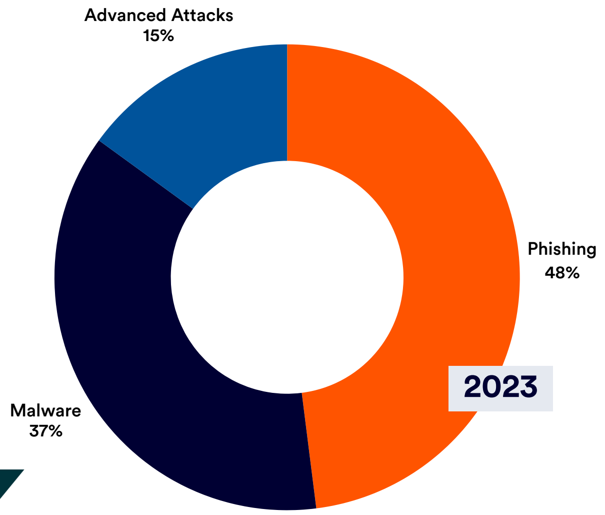
Salesforce environments such as Experience Cloud, Sales Cloud, and Service Cloud facilitate external interactions with employees through activities like chatting, opening cases, completing web forms, and more. Perception Point stands apart from standard Anti-Virus solutions by conducting real-time, in-depth scans on all content uploaded to Salesforce. This multi-layered patented platform intercepts any threat type before it reaches the end user.

## Zendesk

Organizations heavily rely on Zendesk as a versatile platform for customer engagement and support. With Zendesk's multi-channel capability, customers can communicate through various channels such as email, live chat, messaging, social media, and web forms. While excelling in customer communication and support ticket management, Zendesk's native defenses against cyber threats are constrained. It primarily relies on static file scanning and lacks the capability to scan URLs embedded in messages and attachments, leaving a significant security gap. This vulnerability is noteworthy, considering that threat actors often leverage URLs to distribute phishing links, exposing organizations to potential cyber attacks.

***In 2023, Zendesk continued to face attacks similar to those in the previous year, with malware comprising a substantial portion at 37%, compared to 28% in 2022. Phishing witnessed a slight uptick from 43% in 2022 to 48% in 2023. Advanced attacks, however, decreased proportionally to malware and phishing attacks, constituting 15% of all Zendesk attacks in 2023, down from 29% the previous year.***





# Brand Impersonation

In 2023, attackers employed a diverse array of methods to exploit unsuspecting victims and their data, with one prevalent tactic being the impersonation of popular brands. This technique focuses on impersonating the most widely recognized and utilized brands, capitalizing on the potential to deceive victims into trusting the legitimacy of emails or URLs.

Brand impersonation, a form of cybercrime, involves the creation of counterfeit emails or websites that mimic legitimate companies or organizations. These deceptive campaigns are crafted to trick recipients into divulging personal information, including passwords, account numbers, or other confidential data, posing a significant security threat with potential repercussions such as identity theft and fraud.

To achieve their malicious goals, threat actors may employ logos, fonts, and other design elements to replicate the appearance of legitimate emails or websites. Creating a sense of urgency by falsely claiming immediate action is required, or resorting to generic greetings instead of addressing the user by name, are common tactics.

Notably, throughout 2023, Microsoft emerged as the most impersonated brand in malicious email messages, with SharePoint also being a frequent target. Attackers regularly impersonated other well-known brands, including Netflix, FedEx, LinkedIn, PayPal, and American Express, further underscoring the pervasive nature of this malicious activity.

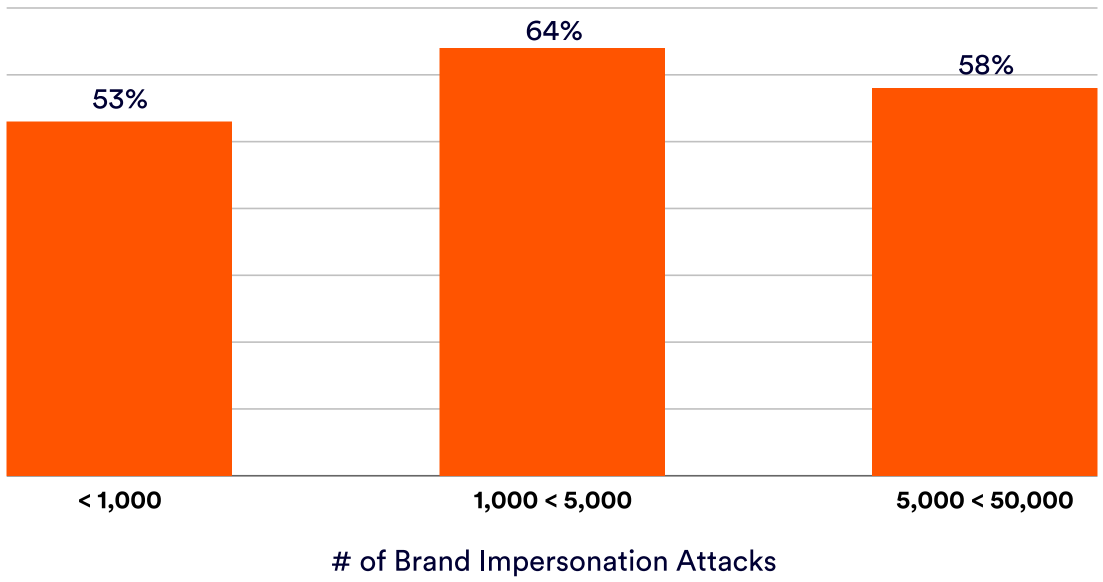
In addition to impersonating well-known brands, cyber attackers also impersonate the brands of the targets themselves. For example, a Google employee might receive an email from an attacker purporting to be from Google.

***An average of 55% of all brand impersonation attacks consisted of organizations' own brands in 2023.***

This alarming statistic highlights the pervasive nature of cyber threats, underscoring the attackers' willingness to exploit the trust associated with a target's own identity.

***Breaking down attack volumes, organizations with fewer than 1,000 brand impersonation attacks in 2023 saw their own brand targeted in 53% of cases on average. For those with 1,001 to 5,000 attacks, the average rose to 64%, while organizations facing 5,000 to 50,000 attacks experienced an average of 58% targeting their own brand in 2023.***

Average Brand Impersonation Attacks
Targeting Organizations' Own Brand 2023



# Final Words

Organizations must stay adaptive and vigilant in order to ensure their security. The report emphasizes that attackers are continually embracing more sophisticated techniques, diversifying their targets to include new channels such as Microsoft 365 collaboration apps, Salesforce, and Zendesk. In response to this evolving threat landscape, organizations must proactively safeguard their most valuable assets by adopting a comprehensive approach to cybersecurity. This approach should extend across the entirety of the modern workspace, mitigating risks and fortifying defenses against the multifaceted challenges posed by cyber adversaries.

## About Perception Point

Perception Point is a Prevention-as-a-Service company for the fastest and most accurate next-generation detection and response to all attacks across email, cloud collaboration channels, and web browsers. The solution's natively integrated incident response service acts as a force multiplier to the SOC team, reducing management overhead, improving user experience and delivering continuous insights; providing proven best protection for all organizations.

Deployed in minutes, with no change to the enterprise's infrastructure, the patented, cloud-native and easy-to-use service replaces cumbersome legacy systems to prevent phishing, BEC, spam, malware, Zero-days, ATO, and other advanced attacks well before they reach end-users. Fortune 500 enterprises and organizations across the globe are preventing content-borne attacks across their email and cloud collaboration channels with Perception Point.

Visit us: www.perception-point.io
Contact us: info@perception-point.io