2025 EMAIL THREATS REPORT

Key findings about the evolution of email-based threats

Email remains the most common attack vector for cyber threats because it provides an easy entry point into corporate networks. One in four email messages today are either malicious or unwanted spam.»

Barracuda

Table of Contents

Key findings

1 in 4 email messages are malicious or unwanted spam.

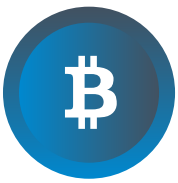
83% of malicious Microsoft 365 documents contain QR codes that lead to phishing websites.

20% of companies experience at least one account takeover (ATO) incident each month.

Nearly half of all companies have not configured a DMARC policy, putting them at risk of email spoofing, phishing attacks, and business email compromise.

Nearly **one-quarter** of all HTML attachments are malicious.

More than **three-quarters** of companies are not actively preventing spoofed emails.



Bitcoin sextortion scams, an emerging trend, account for **12%** of malicious PDF attachments.

The evolution and impact of email-based threats

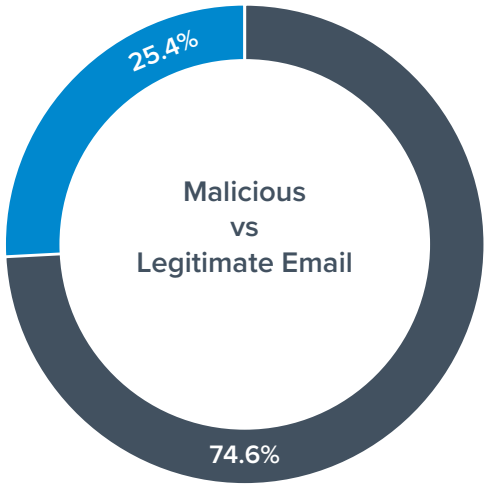
The email threat landscape is constantly evolving, as cybercriminals develop more sophisticated tactics to exploit individuals and organizations. Email remains the most common attack vector for cyber threats because it provides an easy entry point into corporate networks. **One in four email messages today are either malicious or unwanted spam.** Threat actors use a combination of social engineering, automation and advanced malware to bypass security defenses and trick recipients into taking action, such as clicking on a malicious link, opening an infected attachment or transferring funds to fraudulent accounts.

Methodology

This report contains proprietary Barracuda research gathered during February 2025. During that time period, nearly 670 million emails that were malicious, spam or unwanted were analyzed. The report presents the key findings about that threat data.

The impact of email-based attacks can be severe, ranging from financial losses and data breaches to regulatory penalties and reputational damage. One successful attack can disrupt business operations, expose sensitive customer and employee information and lead to long-term financial and legal ramifications.

With attackers continuously refining their tactics to evade traditional security measures, organizations must mitigate the risks by adopting a multi-layered approach to email security, leveraging AI-driven threat detection, real-time monitoring and user awareness training.



Impact on small and medium-size enterprises

Small businesses are particularly vulnerable to email threats, due to limited cybersecurity resources, smaller IT teams and less mature security infrastructures. They frequently have to rely on basic email security solutions that may not be able to handle sophisticated attacks, such as business email compromise (BEC), phishing and ransomware. One successful attack can have devastating consequences, leading to financial loss, reputational damage and even business closure. With regulatory requirements becoming stricter, even a minor data breach could result in fines and legal repercussions.

Here's a look at some of the most common attacks detected by Barracuda systems that will be covered in this report.

24%

Bulk email can clutter inboxes, making it more challenging for users to identify important messages and potentially causing them to overlook critical emails.

21%

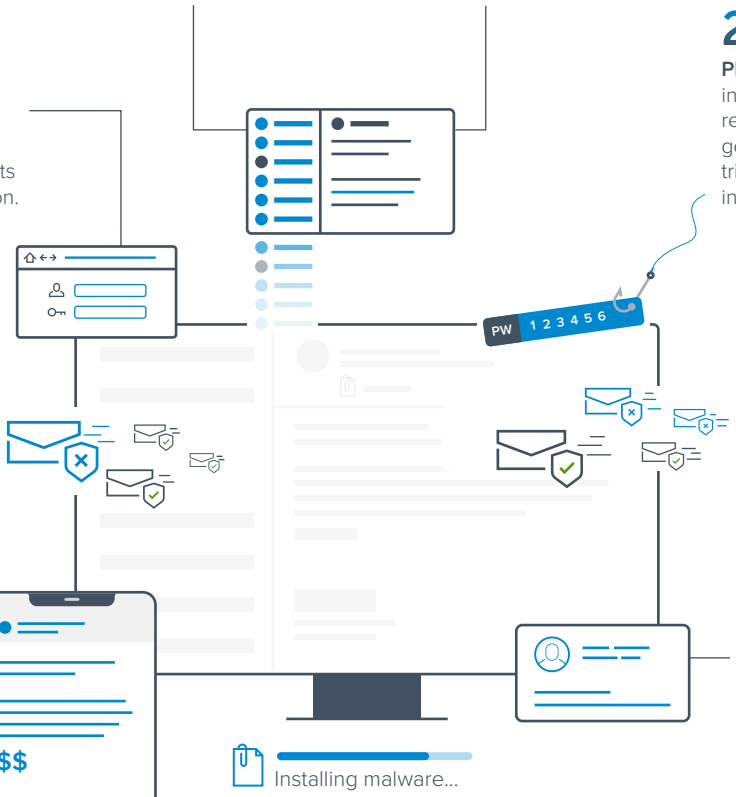
Spam can overwhelm email systems, leading to decreased productivity and increased operational costs for businesses.

2%

Spoofing and impersonation attacks involve attackers forging the sender's email address or domain to appear as a trusted source, often to deceive recipients into divulging sensitive information.

23%

Phishing is a large-scale, indiscriminate attack that targets many recipients simultaneously, relying on generic lures. Attacks are designed to trick recipients into revealing sensitive information, such as login credentials



7%

Unauthenticated mail refers to emails that lack proper verification through authentication protocols like SPF, DKIM or DMARC. These emails may be more susceptible to spoofing, phishing and other fraudulent activities.

0.02%

Conversation hijacking entails attackers infiltrating email threads by compromising email accounts and inserting themselves into ongoing communications.

0.2%

Extortion emails threaten recipients with negative consequences, such as releasing sensitive information or launching cyberattacks, unless a ransom is paid.

0.25%

Spear phishing is a highly targeted attack, customized for specific individuals or organizations, that uses social engineering, impersonation and personalized content to increase credibility and bypass traditional security defenses.

0.03%

Business email compromise (BEC) involves impersonation of trusted individuals, such as executives or business partners, to deceive employees into transferring funds or disclosing sensitive information.

0.5%

Malicious attachments contain harmful code that can install ransomware, spyware and other types of malware, leading to data breaches or system compromises.

22%

The **Other** category includes blocked and quarantined mail, such as messages with invalid recipients or those flagged due to custom policies.

Malicious attachments used to distribute malware and exploit vulnerabilities

Email attachments are often used to distribute malware, launch phishing campaigns and exploit vulnerabilities. The data highlights the prevalence of malicious attachments across different file types.

HTML files are weaponized most often

Despite a relatively low total volume, **HTML attachments stand out as the most weaponized file making up more than three-quarters of the malicious files detected. With 23% marked as malicious**, they are one of the riskiest file types. Attackers often use HTML files for phishing, embedding malicious scripts that redirect users to fake login pages designed to steal credentials. Security teams must implement strict policies around HTML attachments, such as scanning for embedded scripts and blocking suspicious files outright.

Microsoft 365 documents have a relatively low malicious rate but remain a threat

Microsoft 365 documents are commonly used in both legitimate business communications and cyberattacks. With a comparatively low malicious rate (0.17%), attackers still exploit Microsoft 365 documents to deliver malware, often using macros or embedded links.

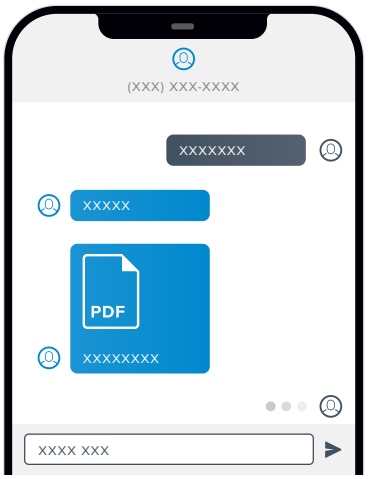
PDFs are less likely to be malicious

PDFs are by far the most frequently shared file type in email attachments. They have a low risk level, which only 0.13% of PDFs being malicious. However, PDFs are starting to be used more in phishing campaigns, often containing embedded scripts or deceptive links to direct recipients to credential harvesting sites.

Bitcoin sextortion scams, an emerging trend, account for 12% of malicious PDF attachments. In these attacks, cybercriminals send emails containing PDFs that claim to have compromising information about their victim, often alleging hacked webcam footage or stolen browsing history. The PDFs include threatening messages demanding Bitcoin payments to prevent the release of this supposed evidence. These scams rely on fear and urgency to manipulate victims into paying, even when no real compromise has occurred.

12%

of malicious PDF attachments are used in sextortion



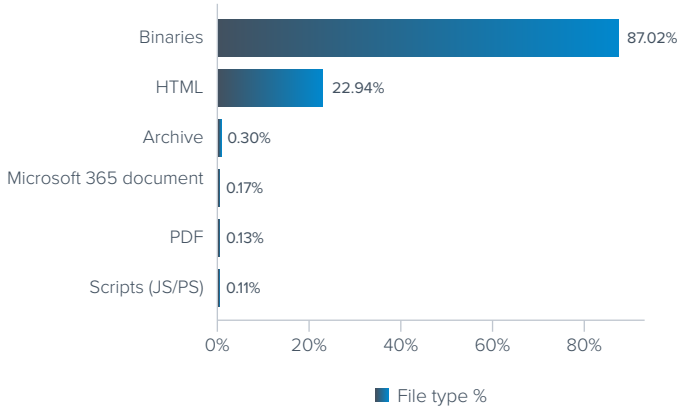
Binaries pose an extreme risk

An alarming 87% of binaries detected were malicious. This highlights the need for strict policies against executable files being sent via email. Since executables can directly install malware, security teams should consider blocking binaries (unless they are absolutely necessary) and ensure all downloads are scanned before execution.

Archive files and scripts have low detection rates but still pose risks

Archive files, such as ZIP and RAR, have a relatively low malicious rate of 0.3%. However, attackers use them to bundle malware and evade detection. Similarly, scripts (including JavaScript and PowerShell) are rare and only 0.11% were marked as malicious. But this does not eliminate the risk because scripts can execute dangerous payloads, especially when embedded in other file types.

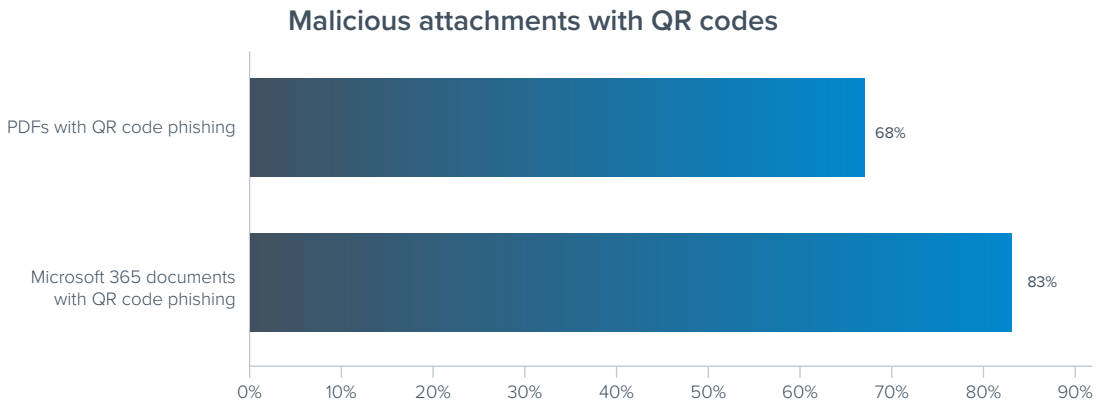
Percentage of different attachment types that are malicious



QR codes in attachments

Cybercriminals are increasingly embedding malicious QR codes in email attachments to deceive users and bypass traditional security.

Malicious QR codes are embedded in commonly used file formats. **68% of malicious PDFs and 83% of malicious Microsoft 365 documents contain QR codes** that lead to phishing or other harmful websites. These file types are widely trusted in business environments, making them effective in social engineering attacks. Once the QR code is scanned, victims are redirected to phishing pages impersonating Microsoft 365 login portals, where attackers steal credentials to compromise business accounts. This growing trend highlights the need for advanced security measures that can analyze QR codes in attachments.



Attackers increasingly favor the use of QR codes for several reasons:

Evasion of traditional security filters

Traditional email security systems often focus on detecting malicious URLs and attachments. QR codes, being images, can slip past these filters, making it easier for attackers to deliver their payloads undetected.

User trust and engagement

QR codes have become common in daily life, used for everything from viewing a restaurant menu to making a contactless payment. This familiarity can lead users to scan codes without suspicion, increasing the likelihood of successful attacks.

Mobile device targeting

Scanning QR codes typically involves mobile devices, which may lack the robust security controls found on corporate desktop computers. This shift allows attackers to take the attack outside of your company's firewall.

Identifying malicious QR codes in email attachments is challenging because encoded content is invisible until scanned, preventing users from assessing its legitimacy beforehand. Many security scanners prioritize text-based threats, often overlooking QR codes embedded in images and PDFs.

Malicious links pose a persistent and widespread threat

Malicious links remain one of the most common and effective tools for cybercriminals. With data showing that **1 in every 100 links** is malicious, organizations face a persistent and widespread threat. These links are embedded in phishing emails, impersonation attacks and malware campaigns. Some could bypass traditional security filters by appearing legitimate at first glance.

Where malicious links lead and their impact

Phishing pages and credential harvesting

Attackers create fake login pages that mimic legitimate services, such as Microsoft 365. When victims enter their credentials, the information is sent directly to attackers. Once compromised, these accounts are used for further attacks, including internal phishing and business email compromise (BEC).

Malware and ransomware downloads

Malicious links lead to websites that host malware-infected downloads, often disguised as invoices, software updates, or security alerts.

Fake payment portals and wire fraud

Cybercriminals impersonate company executives or vendors, sending invoices with links to fraudulent payment sites that are designed to steal sensitive data or initiate unauthorized transactions.

With 1% of all links being malicious, businesses must assume that employees will inevitably encounter malicious URLs. By combining proactive security measures with user education, organizations can significantly reduce the risks posed by these deceptive threats.

Account takeover enables data theft and lateral phishing

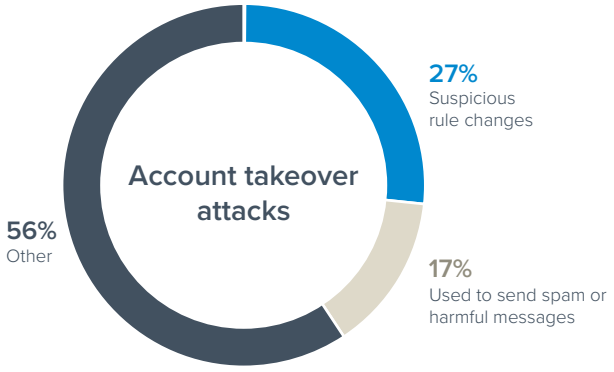
Account takeover (ATO) is a common cyber threat, with 20% of companies experiencing at least one ATO incident per month. Attackers typically gain access through phishing, credential stuffing or by exploiting weak or reused passwords. Once inside an account, they can steal sensitive data, move laterally inside the organization and send phishing emails that appear to be from a trusted source.

20%

of companies experience at least one account takeover (ATO) incident per month

Common signs of ATO include suspicious logins from unfamiliar locations or devices, unauthorized email forwarding rules, sudden password reset requests and an increase in outbound phishing emails from compromised accounts.

ATO attacks create long-term security risks by allowing attackers to conduct reconnaissance activities and spread further attacks. **27% of ATO incidents involved suspicious rule changes**, such as setting up email forwarding to an external address or auto-deleting incoming security alerts. These tactics help attackers maintain persistence and avoid detection. Additionally, **17% of compromised accounts were used to send spam or harmful messages**, often leading to further phishing attacks, malware distribution or BEC scams.



To mitigate risks associated with ATO, SMBs should prioritize multi-factor authentication (MFA), employee security awareness training and automated monitoring for suspicious account activity.

Protecting businesses from email spoofing

Domain-based Message Authentication, Reporting and Conformance (DMARC), an email authentication protocol, protects email domains from unauthorized use, including spoofing and impersonation attacks. By leveraging Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), DMARC ensures that only authorized senders can send emails from your domain.

When configured effectively, DMARC provides organizations with:

- Protection against domain spoofing to safeguard their reputation
- Actionable reporting insights to monitor email authentication and unauthorized use of their domain
- Improved email deliverability by building trust with email service providers

However, almost half of the domains don't have a DMARC policy configured, and only 23% have DMARC enforcement set up.

The fact that **77% of companies** (47% with no record and 30% with a "monitoring only" policy) **are not actively preventing spoofed emails** is a significant security gap. Without enforcement, attackers can impersonate legitimate businesses with business email compromise (BEC), phishing attacks and other threats. This lack of protection not only puts the organization at risk but also damages the brand reputation when customers or partners receive fraudulent emails appearing to come from a trusted domain.

For businesses, failing to implement DMARC enforcement means:

- Increased risk of impersonation attacks leading to financial and data losses
- Higher email fraud rates, as cybercriminals take advantage of unprotected domains
- Decreased email deliverability, as email providers increasingly favor authenticated domains

Why organizations should move to DMARC enforcement

To fully protect against domain spoofing, companies should gradually move from having a DMARC policy set to "p=none," which is monitoring only mode, to a policy set to "p=reject," which will completely reject unauthenticated emails. This ensures that unauthorized emails are blocked, reducing the risk of phishing and improving trust in business email communications. Organizations should also regularly review DMARC reports to gain insights into unauthorized email activity and refine their policies accordingly.

DMARC is a critical yet underutilized security control that helps organizations defend against phishing and email fraud. With nearly half of businesses lacking any DMARC protection and only 11% enforcing DMARC policies, attackers continue to exploit email as a primary attack vector. Businesses must prioritize DMARC enforcement to strengthen their email security posture and protect their brand, employees and customers from email threats.

Best practices to protect against email-based attacks

As cybercriminals continue to adapt their tactics, IT and security professionals need to stay focused on the evolution of email attacks.

Here are five cybersecurity best practices that all organizations should put in place to reduce risk and increase cyber resilience.

1. **Deploy multilayered email security.** Most organizations today will have robust spam and malware filters in place, but they are not always properly configured to block malicious messages effectively. IT teams need to regularly perform a health check on their email gateway settings to ensure optimal performance.

   As threats evolve, so should your organization's protection. Scammers are adapting their tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against targeted phishing attacks. Supplement your gateways with AI-powered cloud email security technology that doesn't solely rely on looking for malicious links or attachments.

2. **Protect users' access.** Protecting access and users' accounts should be an integral part of your organization's cybersecurity strategy. Start using multifactor authentication (MFA), which provides an additional layer of security above and beyond username and password. Today, organizations should consider a more advanced Zero Trust strategy, to continuously verify and allow only the right users to access the right resources. Deploying Zero Trust Access technology protects access and reduces your exposure to lateral attacks.

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

4. **Improve cybersecurity awareness.** Educate users about the latest email threats by making it a part of security awareness training. Ensure employees can recognize these attacks, understand their fraudulent nature and know how to report them. Use phishing simulation for emails and voicemail to train users to identify cyberattacks, test the effectiveness of your training and evaluate the users most vulnerable to attacks.

5. **Secure and back up all data.** To avoid data loss as the result of an email-based attack, such as ransomware, your data needs to be properly secured, isolated and backed up. You also need to make sure that your backup solution allows you to restore data in a reasonable time frame. Make sure you run drills and test your data back up regularly to ensure you are fully prepared.

About Barracuda

Barracuda is a leading cybersecurity company providing complete protection against complex threats. Our platform protects email, data, applications and networks with innovative solutions, and a managed XDR service, to strengthen cyber resilience. Hundreds of thousands of IT professionals and managed service providers worldwide trust us to protect and support them with solutions that are easy to buy, deploy and use. For more information, visit barracuda.com.

John Thome, President
440-498-2310
jthome@chicorporation.com
ChiCorporation.com