

Special Report: 2019 **Email** Security Trends

Global IT security professionals
face evolving challenges. >>

What's inside

About the report.....	1
Key findings	2
Current conditions.....	3
Security spending.....	6
Costs of breaches.....	7
Incident response.....	8
Phishing.....	10
Insider threats.....	11
Office 365.....	12
Looking ahead.....	13
Related resources.....	14
About Barracuda.....	15

About the report

Barracuda surveyed global IT stakeholders to capture their experiences and attitudes about the current state of email security.»

The survey includes responses from 660 executives, individual contributors and team managers serving in IT-security roles in the Americas, EMEA and APAC. Companies surveyed include small, mid-sized and enterprise businesses in technology, financial services, education, healthcare, manufacturing, government, telecommunication, retail and other industries.

A wide range of questions captured hard data about phishing, insider threats and Office 365, as well as the related business impacts, security spending and costs of breaches.

Key findings

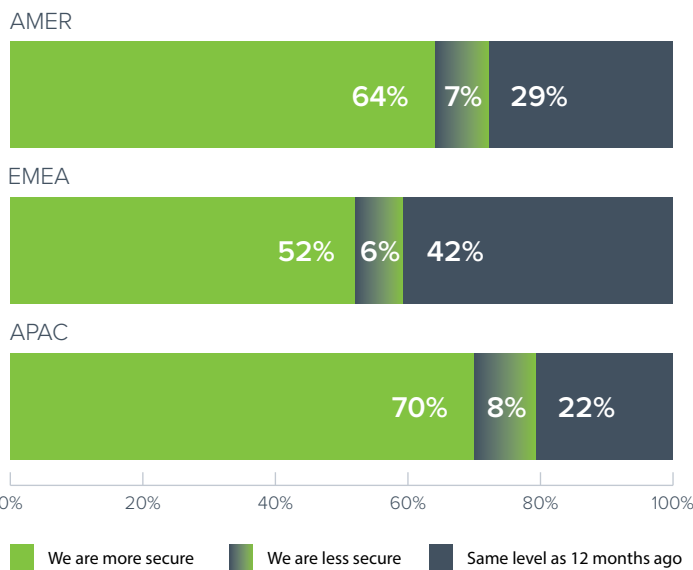
What was the impact of these email security attacks on your company? N=660



- IT professionals are more confident about their email security systems than they were a year ago.
- The vast majority say email attacks are having a major impact on their businesses.
- Phishing and ransomware are top concerns.
- Breach costs and monetary losses are on the rise.
- Employees remain a major weak link in an organization's security defenses.
- There are growing concerns about insider threats and Office 365.

Current conditions

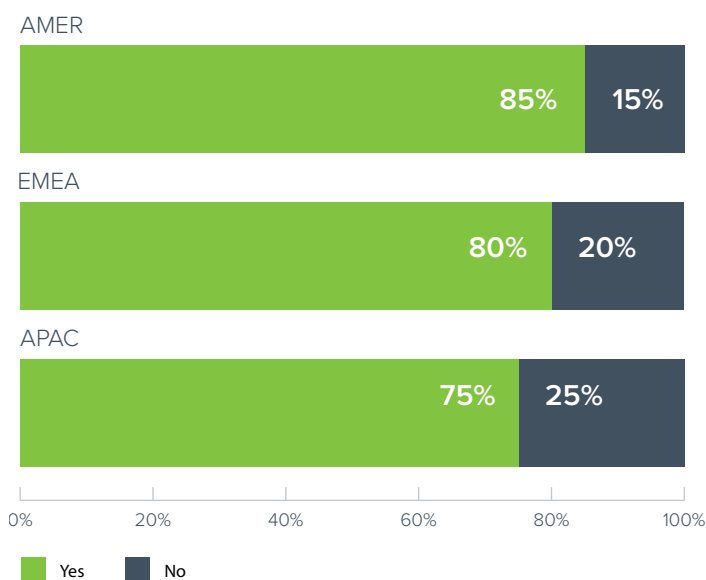
How secure do you feel your company's systems and data are compared to 12 months ago? N=660



The good news is that 63% of global security professionals feel their organization's data and systems are more secure than they were a year ago. But it should also be treated with caution: if an organization lacks the tools to accurately detect threats, it may have a false sense of security.

APAC companies are the most likely to feel their security has improved, while EMEA companies are the least likely.

Has your company faced any attempted email-based security threats in the past year? N=660



Despite the overall positive outlook, phishing and ransomware top the list of security risks that organizations are not fully prepared to deal with, along with spear phishing, malware, viruses, data loss, spam, smishing, email account takeover and vishing. Only 7% of organizations are not worried about any of these risks.

In fact, email threats continue to proliferate and have a major impact: On average, more than four-fifths (82%) of organizations claim to have faced an attempted email-based security threat in the past year, although the figures differ slightly by global region.



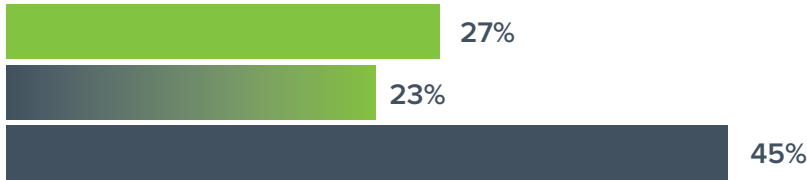
The stress of my job has increased



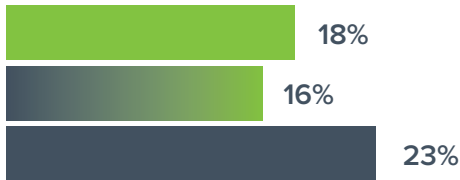
I worry about potential email security issues even when I am not at work



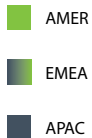
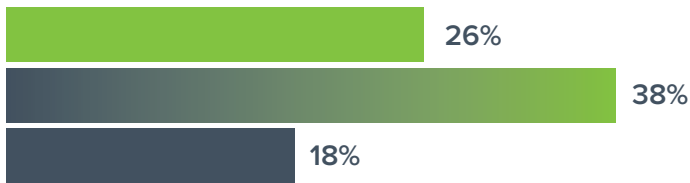
I have had to work evenings or weekends to address issues



I have had to cancel personal plans to respond to attacks



There has been no impact on me

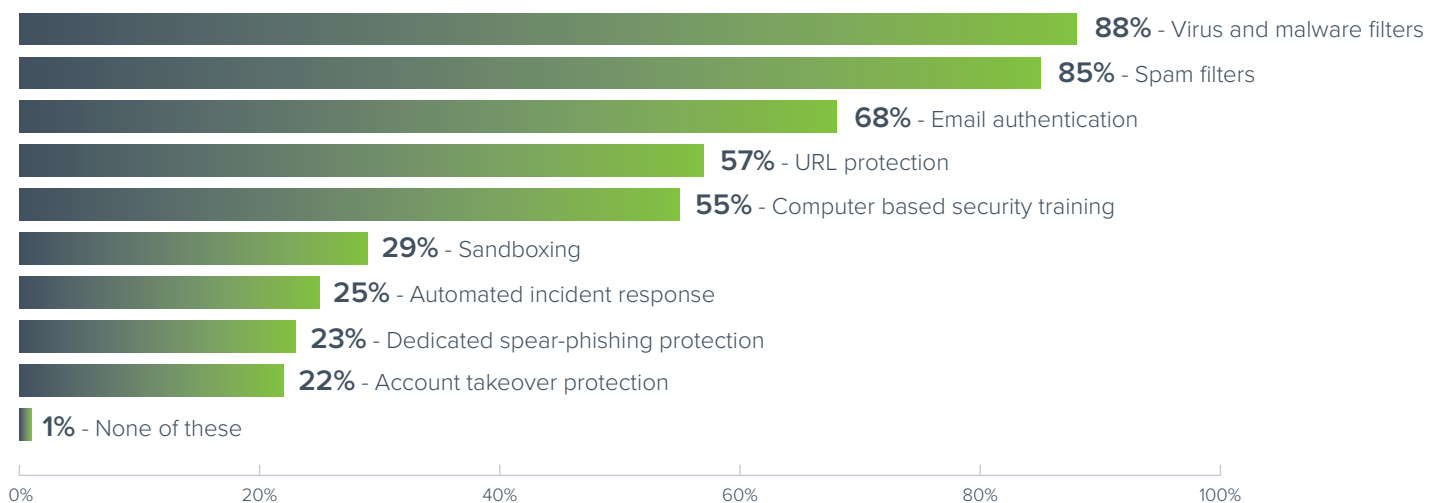


What has been the impact of these email security attacks on you personally? N=660

While 74% of organizations report that email security attacks have had a direct business impact, as detailed in the Key Findings, they are also impacting the personal lives of IT security professionals, with nearly three-quarters experiencing higher stress levels, worrying outside the office and being forced to work nights and weekends. APAC reports the highest levels of personal impact from email security attacks.

Security spending

Which of the following types of email security technology does your organization have in place today? N=660



Spending on email security is another positive sign, underscoring the fact that organizations understand the seriousness of current threats. 45% of organizations are spending the same as last year, and 48% are spending more. Only 7% are spending less.

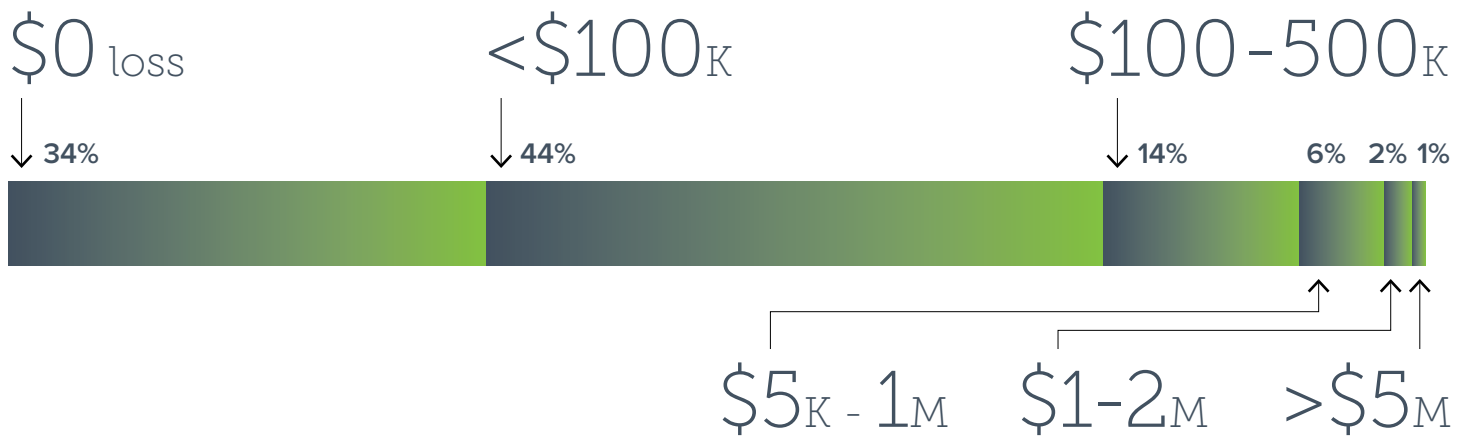
IT has invested in a wide range of tools for email security. The increased investment reflects the growing sophistication of the attacks and the need to protect against

potential damage from evolving threats.

There's one potential pitfall: organizations are clearly underinvesting in tools designed to protect email beyond the traditional security gateway. Just a quarter or fewer had automated incident response, dedicated spear-phishing protection or tools to prevent account takeover.

Costs of breaches

Think of the email attack in the past 12 months that has cost your company the most. Approximately what was the total cost of this attack? N=660

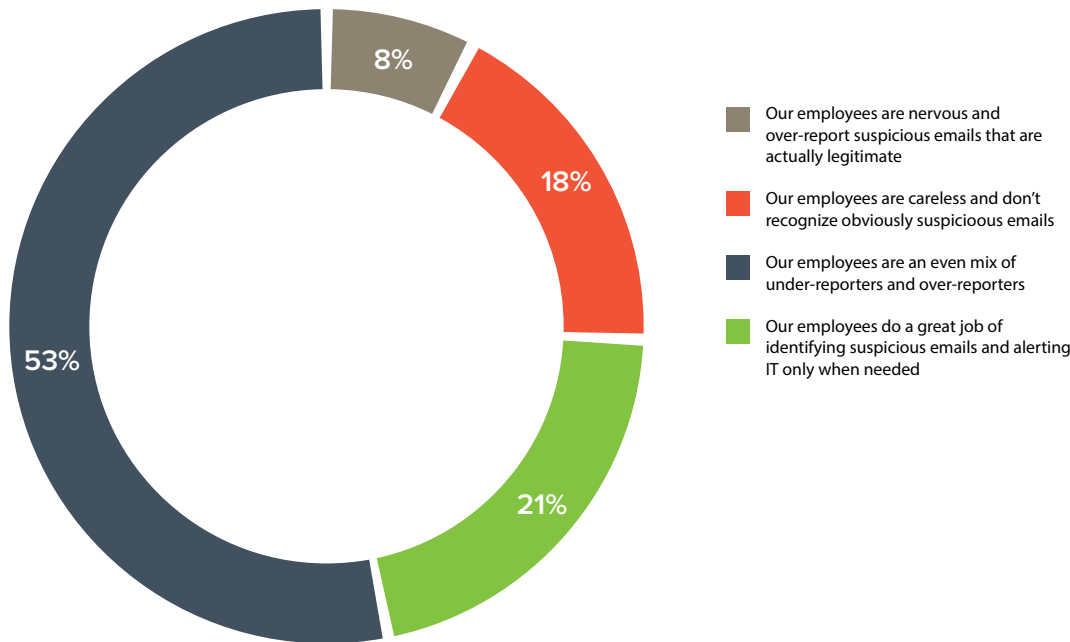


An overwhelming 78% of organizations say the cost of email breaches is increasing. A fifth say they are increasing dramatically. Identifying and remediating threats, communicating with those impacted, business interruptions and IT productivity losses are all factors, as well as potential data loss, regulatory fines and brand damage.

As a result, it's not surprising that 66% claim that attacks have had a direct monetary cost on their organization in the last year. Nearly a quarter say attacks have cost their organization \$100,000 or more.

Incident response

Which of the following statements best describes most of the employees at your company? N=660



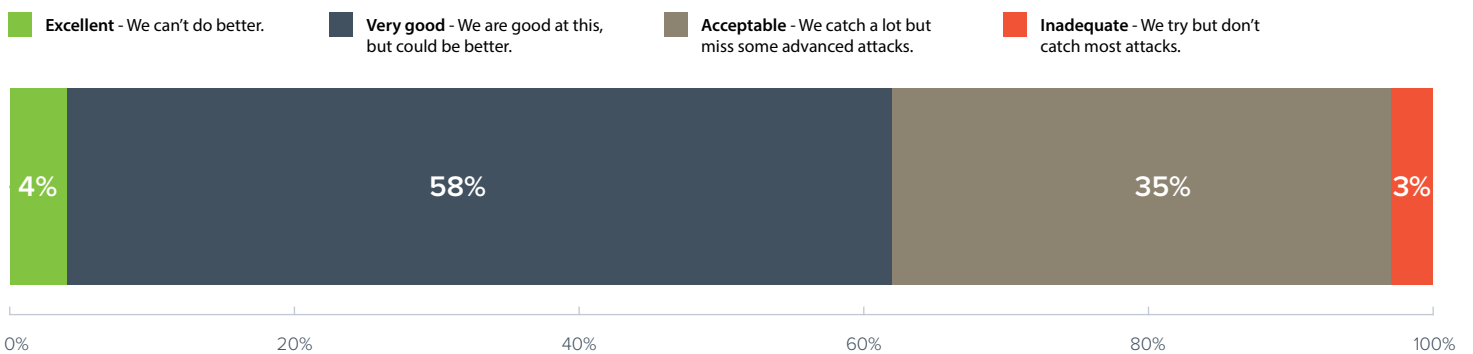
94% of organizations say employees are reporting suspicious emails to IT on a daily basis, but 58% say most emails reported to IT aren't actually fraudulent.

More than three-quarters of organizations say their employees aren't good at spotting suspicious emails for a number of reasons.

These findings are concerning, considering phishing emails that prey on the poor security awareness of end users is one of the most common ways for attackers to download

malware and steal data from organizations. Plus, reporting the wrong types of emails only wastes the time of already-stretched IT security teams. In addition to better awareness training, improved tools are needed to filter potentially dangerous emails and ensure they never make it into inboxes of end users in the first place.

How would you rate the remediation capabilities your company has in place to address malicious emails that reach users' inboxes? N=660



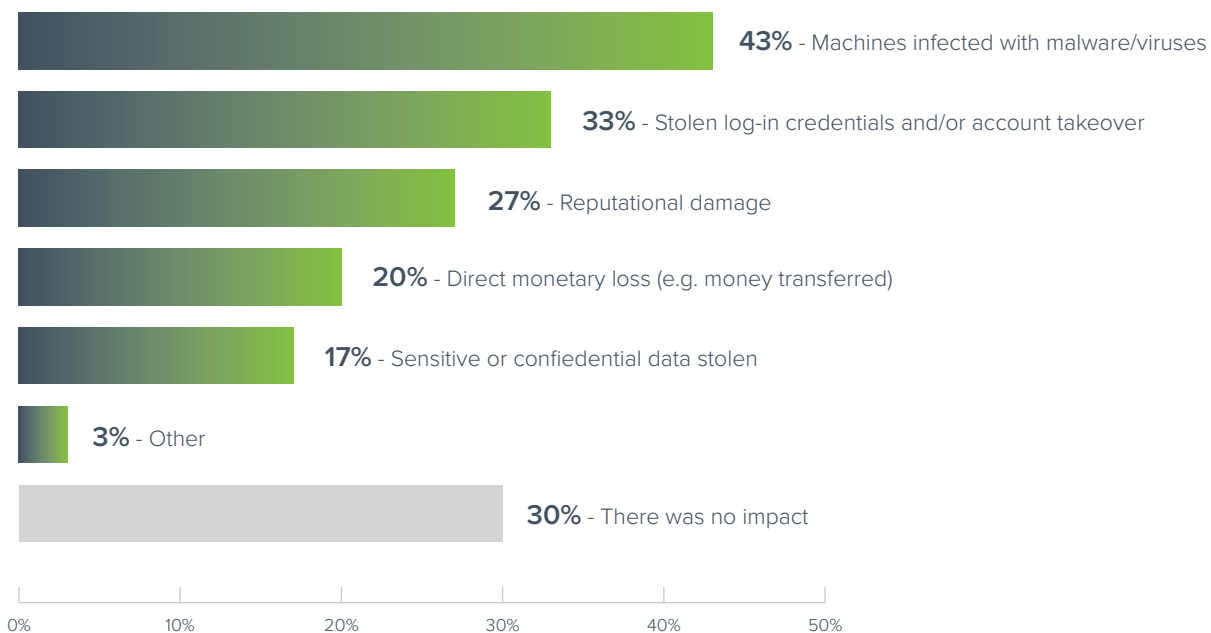
The amount of time spent to investigate and remediate attacks is also cause for alarm: 55% of firms take more than an hour to do so. A delayed incident response could be enough time for hackers to infect an entire organization with ransomware or steal sensitive data. Organizations increasingly need automated

incident response to cut through complexity, accelerate time-to-detection and free up stretched and stressed security staff.

Despite the one-hour average, 62% or organizations give themselves high marks when it comes to the remediation capabilities in place to address malicious emails that reach users.

Phishing

What was the impact of spear-phishing attacks that occurred in the past 12 months? N=660

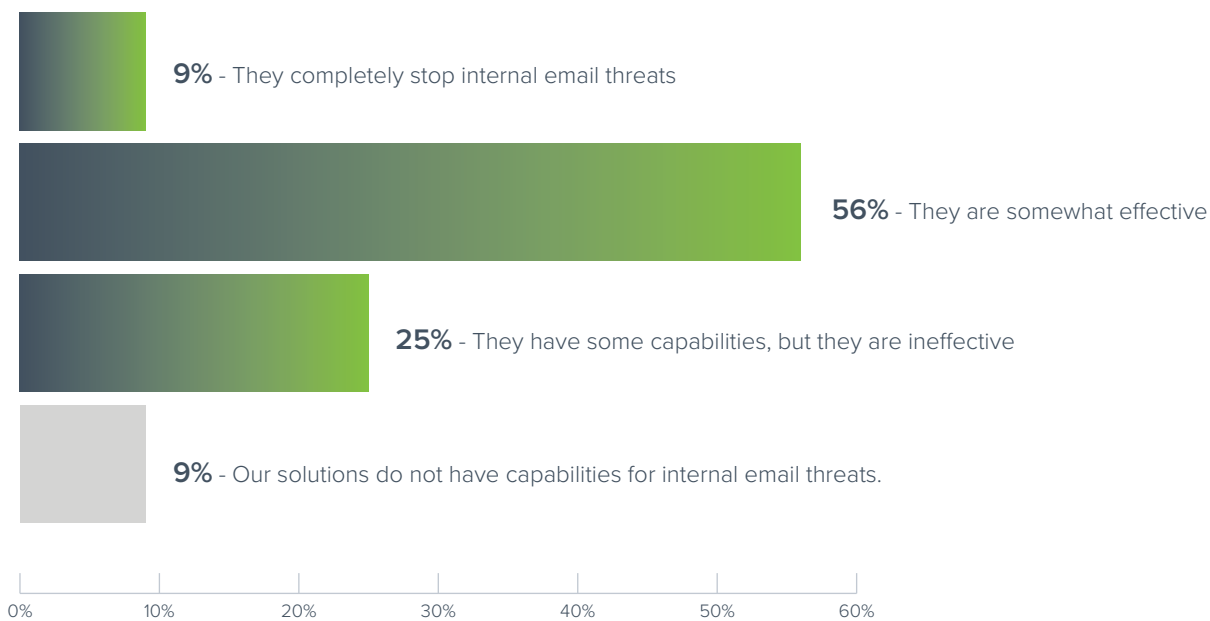


43% of organizations have been the victim of a spear-phishing attack in the past 12 months.

75% of IT security professionals have personally received training about phishing in the last year, which is much needed considering that 70% of organizations have experienced a variety of direct business impacts as the result of attacks.

Insider threats

How effective are your existing email security solutions in addressing internal email threats? N=660

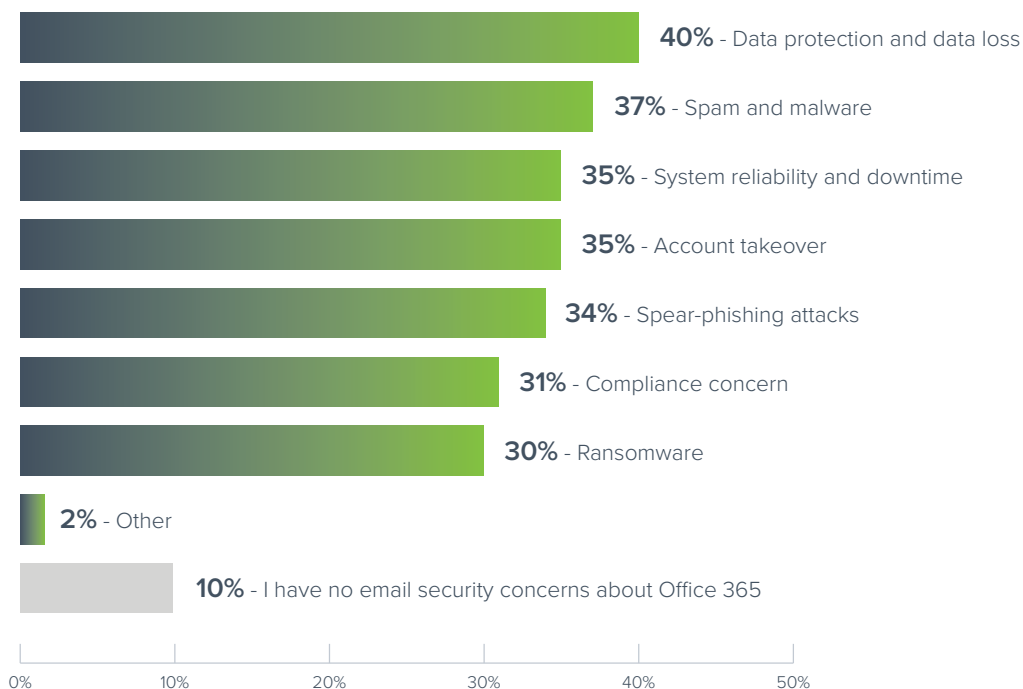


Most IT professionals—79%—say they are worried about attacks and breaches stemming from inside the organization. Their fears are valid: a hacker could compromise an employee’s email account via spear phishing and use it to target other with business email compromise attacks or phishing emails that appear very authentic.

These types of breaches and attacks are hard to spot, which makes it important for an organization to invest in advanced security tools. Unfortunately, most report that their existing tools for addressing insider threats are lacking.

Office 365

What are your biggest email security concerns with using Office 365? N=660



An overwhelming 90% of Office 365 users have security concerns.

86% of organizations agree that third-party email security solutions are essential to keep an

Office 365 environment secure. Organizations have a wide variety of email security technology in place.

Looking ahead

Expect email to remain the top vector for cyberthreats. Based on the success and proliferation of email-based attacks, IT security professionals will need to stay focused on the evolution and escalation of phishing, ransomware and other threats.

The continued adoption of advanced behavioral techniques to spot and stop spear phishing and other attacks will help improve email security overall and reduce the major negative impacts on businesses and the personal lives of IT professionals. Along those lines, automated incident response tools can help cut the workload and pressure on IT security teams. Improved phishing awareness, using real-life simulation tools, is essential to ensure that every end user is a strong first line of defense against cyberattacks.

Reducing opportunities for cybercriminals, including improving email security that goes beyond the traditional gateway, helps every organization protect its data, bottom line and reputation in the marketplace.

Expect email to remain the top vector for cyberthreats. »

Related resources

Product information

[Barracuda PhishLine](#)

Fight phishing with continuous simulation and training

[Barracuda Sentinel](#)

Get AI-based protection from phishing and account takeover

[Barracuda Forensics and Incident Response](#)

Limit damage and accelerate remediation with automated response to email attacks

White paper

[Best Practices for Protecting Against Phishing, Ransomware and Email Fraud](#)

Video

[Barracuda Total Email Protection](#)

Multi-layered protection that goes beyond the gateway

Threat reports

[Spear Phishing: Top Threats and Trends](#)

[Threat Spotlight: Lateral Phishing](#)

[Threat Spotlight: Modular Malware](#)

[Threat Spotlight: Account Takeover](#)

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 150,000 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.

