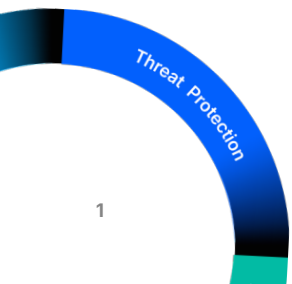
proofpoint.

WHITE PAPER

Email and Beyond—Threats Across Digital Platforms

How the expanding digital workspace affects the security landscape

This solution set is part of the Proofpoint human-centric security platform mitigating the four key areas of people-based risks.



Overview

While the cybersecurity landscape is always evolving, some things stay the same. One constant is attackers' focus on users. They use social engineering tactics to trick or coerce people into revealing their credentials, executing malicious code or taking actions that benefit the attacker. Their goals are to compromise accounts so that they can access critical data or pull off financial fraud—often through multistage attacks that unfold over time.

Email remains a primary threat vector for these attacks. However, in recent years, the attack surface has expanded. Digital transformation has given people new ways to communicate and collaborate. Today, they work across Microsoft Teams, Slack, cloud-based applications, social media platforms and file-sharing services. Not surprisingly, cybercriminals are developing new tactics to exploit these digital channels.

In response, many organizations are taking a fragmented, point-product approach to security. But this creates additional gaps in their defenses and leaves many risks unaddressed. What's more, managing and integrating all these tools is complicated.

In this white paper, we do a deep dive into how cybercriminals are exploiting digital workspaces. We also outline the essential capabilities that you need to effectively address these human-centric threats.

Attacks don't stop at email

Cybercriminals are no longer limiting their attacks to inboxes. They have followed users to expanding digital channels—just as they followed them to the cloud.

One of the most dominant ways to exploit these digital channels is distributing malicious URL attacks. In 2024, there was a 2,534% increase in URL threats delivered via smishing attacks.[1]

Threats like SocGholish take URL-based attacks to a new level. To reach users, this malware often uses broad, indiscriminate tactics such as SEO poisoning and compromising high-traffic websites. When an unsuspecting victim clicks a link that leads to a compromised site, it triggers the execution of a malicious payload.

Notably, social media platforms were the most frequently attacked sector—targeted by 37% of all phishing attacks in 2024..[2] One of the reasons these platforms are so popular with attackers is that people place a lot of trust in these tools. What's more, attackers can use these alternative entry points to bypass email security measures and compromise user accounts. They disguise their malicious activities as legitimate messages, shared files or system alerts.

1. APWG. *Phishing Activity Trends Report*. 2024.
2. Ibid.

Figure 1: Threats and risks across digital workspaces.

Cloud-based applications and remote work have further widened the attack surface. Cybercriminals exploit weak authentication methods, misconfigured cloud security settings and unmonitored collaboration tools. This enables them to gain unauthorized access or manipulate users through social engineering. For example, an attacker might share a phishing link with employees via Microsoft Teams or OneDrive. When employees click on the link, they unintentionally grant attackers access to sensitive systems.

Security teams find it difficult to detect and mitigate these threats because they don't have centralized visibility. Plus, security controls are typically designed to protect email. This leaves significant gaps in coverage.

Trusted communications can be hijacked

Another challenge is the hijacking of trusted business communications. Attackers can impersonate your brand to target your partners, suppliers or customers across email and various digital channels. Or they can trick employees by pretending to be these same third parties.

Domain spoofing, lookalike domains and compromised supplier accounts—these are just some of the ways that cybercriminals infiltrate trusted communications to launch highly convincing attacks.

Proofpoint research shows that an average of 44,000 unauthorized messages are sent from unprotected active domains every month. Attackers use these messages to insert themselves into ongoing business conversations. From there, they can manipulate transactions, redirect payments or steal sensitive data—often without being immediately detected.

Social engineering remains threat actors' primary weapon. But their attacks have expanded beyond inboxes. While employees might believe they are engaging with a familiar and trusted entity on platforms like Skype, LinkedIn or WhatsApp, they may unknowingly be interacting with a threat actor.

Attackers can also exploit a brand's reputation to steal from their business partners and scam their customers.

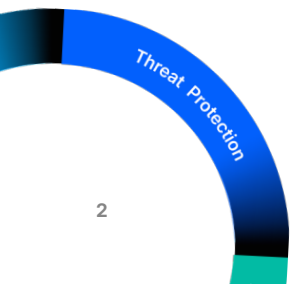


Figure 2: Attackers injecting themselves into business communications using impersonation.

To deceive partners, cybercriminals often use invoicing fraud and digital identity fraud. In these schemes, they pretend to be a legitimate business partner. Then, they request sensitive information or ask for a payment.

To deceive customers, bad actors use a variety of common themes. These include shipping scams, shopping scams, online banking scams and fake customer support. While the target organization may not suffer a direct financial loss, the long-term impact can be even more damaging. These scams erode trust, which ultimately leads to greater costs.

Modern business ecosystems are interconnected. That means a single compromised account or hijacked conversation can have widespread consequences. In other words, effects don't stop with one organization—they can spread across the supply chain.

Users knowingly bypass security

Despite the widespread adoption of security awareness programs, human error remains one of the biggest risks for organizations. Nearly 70% of data breaches are caused by human error.[3] Unfortunately, people don't always act in the best interests of their employers.

For a long time, security professionals assumed that people took risky actions because they lacked security awareness. As a result, they relied heavily on training and phishing simulations. The hope was that these methods would change people's behavior when they were faced with threats. However, 96% of employees who admit to taking risky actions are aware that their behavior poses a risk to their organization—and they do it anyway.[4]

This highlights a critical gap in traditional, compliance-based security training. Just because employees know the right thing to do doesn't mean that they will always do it. While security awareness training lays an important foundation, it is not enough to drive meaningful behavior change.

Moreover, it's more challenging than ever to protect employees. Social engineering tactics are increasingly sophisticated. Many threats are enhanced by generative AI. And digital workspaces are more difficult to protect than just email. You can't simply teach employees to recognize phishing emails. Successful training assignments or passed phishing tests do not guarantee that they will be resilient against threats across other digital channels.

3. Verizon. *Data Breach Investigations Report*. 2024.
4. Proofpoint. *2024 State of the Phish*. 2024.

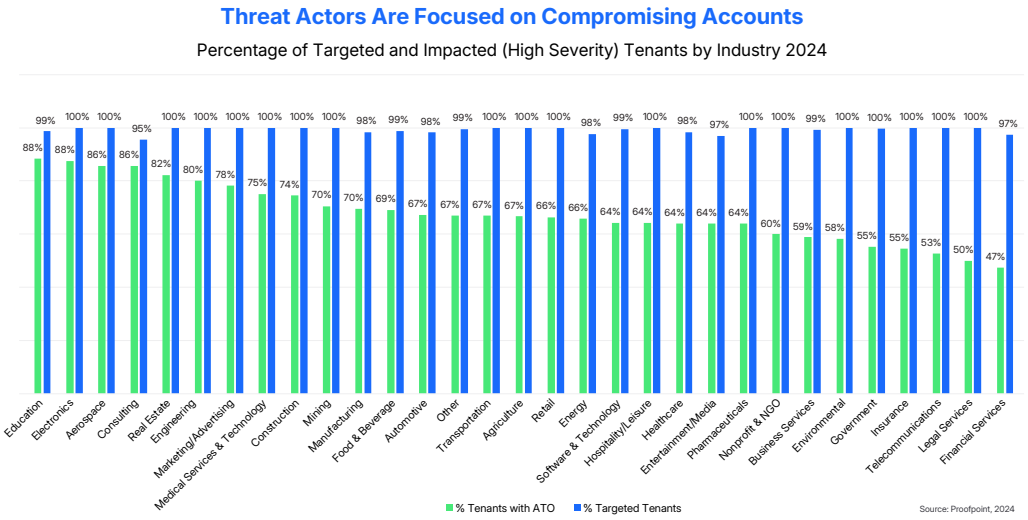


Figure 3: Threats and risks across digital workspaces.

There are multiple paths to account takeover

Compromising user accounts is the ultimate goal of human-centric attacks, as it grants attackers critical initial access to an organization. From there, attackers can execute multistage attacks, systematically escalating privileges, moving laterally and expanding their foothold to maximize damage. According to recent Proofpoint research, 99% of organizations are regularly targeted for account takeovers (ATOs)—and 62% are impacted by these attacks.

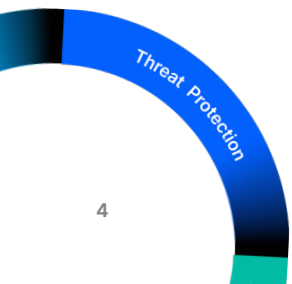
Phishing remains one of the most common entry points. But attackers use a variety of advanced tactics, including callback phishing, session hijacking (man-in-the-middle attacks), OAuth token abuse, multifactor authentication (MFA) bypass techniques, help desk social engineering and brute-force attacks. These techniques are often combined to enable a broader multistage attack, allowing cybercriminals to maintain persistence and deepen their control within an environment.

Employees now access corporate systems from multiple devices, applications and locations—often reusing credentials across platforms. This poor password hygiene, combined with an ever-expanding digital footprint, increases the risk of credential exposure. Even with strong security measures in place, human error remains a major risk factor. Studies show that employees frequently approve suspicious authentication requests despite understanding the risks, creating further opportunities for attackers to escalate their attacks.

Generative AI and automation have made phishing lures and social engineering schemes more sophisticated and convincing. Attackers exploit this to deceive users into revealing their credentials or approving malicious access requests.

But employee ATOs are only one piece of the puzzle. Organizations today are deeply interconnected, relying on digital communications with trusted business partners. Cybercriminals take advantage of this by compromising supplier accounts to conduct reconnaissance and launch further attacks. These supplier-based compromises serve as an entry point for multistage attacks can spread across an organization's entire ecosystem.

The more interconnected a digital ecosystem is, the harder it becomes to monitor and protect every access point. This makes takeovers of both employee and supplier accounts a persistent and unavoidable challenge. Once cybercriminals have taken control, they can move through an environment



unnoticed, steal sensitive data and launch additional attacks. Given the potential for widespread damage, it's crucial to detect and remediate both types of ATO swiftly.

Fragmented tools create gaps

Multiple stand-alone point products are often adopted to mitigate risks across email and other platforms. However, this siloed approach creates security gaps as well as operational inefficiencies.

One drawback of this approach is that it leads to security blind spots. When tools aren't seamlessly integrated, it's harder for security teams to get visibility across the security environment. This increases the chances that threats will go undetected, and it delays incident response.

What's more, this approach wastes resources and drives up operational costs. It's time-consuming and ineffective for teams to manage multiple security tools. They also must correlate data across siloed control points. And the overwhelming number of alerts that these platforms generate can lead to alert fatigue and missed threats.

Conclusion

Like AI, digital transformation is a double-edged sword. One edge cuts through inefficiencies, unlocking seamless collaboration and boosting productivity. The other exposes new vulnerabilities, expanding the attack surface and complicating cybersecurity. Without a unified approach to stopping human-centric threats, organizations are increasingly at risk.

When you are looking for a comprehensive security solution, here's what to look for:

- **Visibility** across email and digital channels, such as collaboration tools, messaging apps, cloud applications and social media platforms
- **Automated threat protection** that goes beyond email
- **Security over trusted business communications** to stop attackers from impersonating your brand
- **Guidance for employees** to help them avoid risky behaviors
- **Actionable insights** into risky suppliers and partners
- **Quick threat response** to account takeovers with automated detection, investigation and remediation

To address human-centric challenges, you need to adopt a holistic security strategy. Consider consolidating your fragmented point products into a pre-integrated threat protection platform. This will strengthen your overall security posture, stop human-centric threats and improve cost efficiency.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →