Dune

SEPTEMBER 2025

Inside Access: CISOs on the Emerging Threats Redefining Human Cyber Risk

Insider Manipulation, Encrypted Channels, and the Multi-Vector Attack Surface No One Trains For

Executive Summary

Large enterprises invest billions in cybersecurity technology to prevent breaches. Yet breaches persist, expanding in scale, speed, and sophistication, with over 90% of these incidents still originating from user behavior rather than technical failure.

Today's attackers no longer exclusively rely on malware or infrastructure exploits. They target people, using urgency, familiarity, and trust to manipulate user behavior across the channels employees rely on every day. Over the past 12 to 18 months, attacker behavior has increasingly focused on multi-channel social engineering campaigns, exploiting real-time communication tools that often fall outside traditional security visibility. These campaigns use impersonation, urgency, and procedural familiarity to manipulate users before escalating access or triggering downstream compromise.

Groups like Scattered Spider, which we profile in detail within this report, exemplify this shift. Their coordinated, AI-assisted campaigns impersonate internal roles, exploit procedural trust, and pressure users into action. These highly effective tactics bypass technical defenses by exploiting user behavior directly, often leading to costly, high-impact breaches.

For the first time, Dune Security R&D and Product teams conducted the 2025 CISO Risk Intelligence Survey, collecting insights from enterprise security leaders across high-risk industries. The results expose a widening readiness gap between evolving attacker tactics and enterprise defenses. While nearly all organizations test users for traditional phishing attacks over email, only a few extend simulation or monitoring into high-risk vectors like encrypted messaging apps, collaboration platforms, and unmanaged mobile devices. These blind spots expose users to social engineering threats that feel routine, internal, and urgent, while evading traditional controls entirely.

Defenses at the User Layer remain critically misaligned. While most organizations simulate basic email phishing, only few extend testing to the full spectrum of modern attack channels. Attackers increasingly target encrypted messaging, collaboration

tools, and mobile devices that often fall outside standard monitoring. As a result, many enterprises remain exposed in the environments where users are most vulnerable to manipulation.

Training programs are also falling behind modern risk. 91% of CISOs agree that simulations and awareness content should be tailored by user role and by behavior, yet only 18% actively do both, and 44% have yet to implement either role- or behavior-based personalization in phishing simulations. Worse, 64% of CISOs confirmed social engineering attempts through encrypted or informal channels in the past 12 months, despite limited or no coverage in their training programs.

Enterprise leaders increasingly recognize the scale of the challenge. Rather than focusing solely on compliance metrics or generic training completion, leading organizations are prioritizing behavior-based simulation, adaptive controls, and user-specific risk intelligence. These intelligent programs allow teams to pinpoint who is vulnerable, understand why, and respond proactively to evolving exposure.

Drawing on data from the 2025 CISO Risk Intelligence Survey and behavioral threat telemetry from Dune Security's simulation engine, this report analyzes the disconnect between attacker behavior and enterprise defense. It identifies where simulation efforts fall short, how user readiness breaks down across channels, and what forward-looking organizations are doing to close the gap.

The findings confirm a broader shift in strategy: reducing User Layer risk requires more than awareness. It requires visibility, context, and the ability to act precisely, before a single decision becomes a breach.

Key Findings

Enterprise Risk Quantified

64%
of enterprises experienced confirmed or suspected attacks via encrypted or informal channels in the past year.

AI-personalized phishing emails now drive
3x more
user interaction than traditional, templated variants.

30%
of users who clicked on Dune's AI-personalized phishing email simulations submitted MFA credentials, showing how modern attacks drive deeper compromise than legacy templates ever did.

Just
6%
of CISOs regularly simulate executive impersonation attacks, while
74%
want to add them.

Only
18%
of organizations tailor phishing simulations by both role and behavior, though
91%
say it's important.

Only
12%
of CISOs believe their current SAT platform is sufficient;
38%
disagree or strongly disagree.

0%
of surveyed CISOs simulate attacks via encrypted messaging apps like WhatsApp or Signal, and only
6%
of CISOs express high confidence in their employees' ability to detect threats in these channels.

Only
15%
of enterprises simulate voice-based phishing (vishing), even though
59%
of CISOs rate it as a top concern.

Reward-based phishing was the least effective persuasive tactic, driving nearly
5x fewer
clicks than the highest-performing behavioral trigger: authority.

Only
27%
of enterprises simulate SMS-based phishing (smishing), even though
71%
of CISOs cite it as a top concern.

36%
of CISOs say their top barrier to improving user readiness is the difficulty of measuring user-level risk.

91%
of enterprises do not simulate attacks in collaboration platforms like Slack, Teams, or Zoom Chat.

100%
of surveyed enterprises simulate email phishing, yet
85%
still cite it as a top concern.

26%
of CISOs rate their insider threat readiness as high.

Introduction

Social engineering is the most common method attackers use to breach enterprises, with user behavior still driving 90% of breaches. Attackers have evolved from using typo-filled emails and generic phishing templates to deploying multi-channel campaigns that imitate internal processes and take advantage of user actions across email, SMS, voice calls, encrypted applications, and collaboration platforms.

These attacks are no longer random or opportunistic. They are coordinated, context-aware, and AI-assisted, aiming to impersonate colleagues, escalate urgency, and push for immediate action from the user. Multiple channels can be used simultaneously – for example, one to initiate contact, another to reinforce pressure, and a third to finalize the request. Each user touchpoint is engineered to feel routine, familiar, and legitimate.

Dune Security's 2025 CISO Risk Intelligence Survey offers CISOs and security leaders a sharper understanding of today's evolving attacker tactics. Drawing on responses from enterprise CISOs across high-risk sectors, including financial services, healthcare, manufacturing, and technology, Dune Security's Research and Product teams captured firsthand insight into how adversaries continue to adapt. The findings provide a detailed, data-backed overview of how untested vectors, varying simulation practices, and traditional training methods affect user exposure across email, SMS, voice, collaboration tools, and encrypted messaging platforms.

While email-based phishing remains the most tested and well-known threat vector, continuing to drive a significant share of real-world breaches, attackers are now actively expanding into under-tested channels like mobile messaging, encrypted apps like WhatsApp and Signal, voice messages, and internal collaboration platforms like Slack. These new vectors operate outside traditional security visibility and controls, giving adversaries direct, unmonitored access to users in moments where they may be in a rush, facing pressure, or distracted.

In 2025, attackers are already exploiting those gaps in visibility and protection. According to Dune's

survey, 64% of enterprises experienced a confirmed malicious social engineering attempt via encrypted or informal channels in the past 12 months. These encrypted or informal channels, like Telegram, WhatsApp, Signal, and Messenger, are environments in which virtually no organizations simulate attacks, monitor failure rates, or prevent user breaches.

Phishing attempts now often come as WhatsApp messages from fake executives, Teams chats impersonating IT support, or deepfake voice calls authorizing transfers. These attacks evade technical defenses by manipulating trust, urgency, and routine to prompt hasty, unchecked actions.

Our survey made one thing especially clear: social engineering has evolved beyond email. It is now a behavioral challenge spanning mobile and unmonitored devices. This increased threat has left most enterprise security programs underprepared.

The User Layer Is Now the Primary Risk Surface

Social Engineering and Insider Threats Are the Leading Cause of Breaches

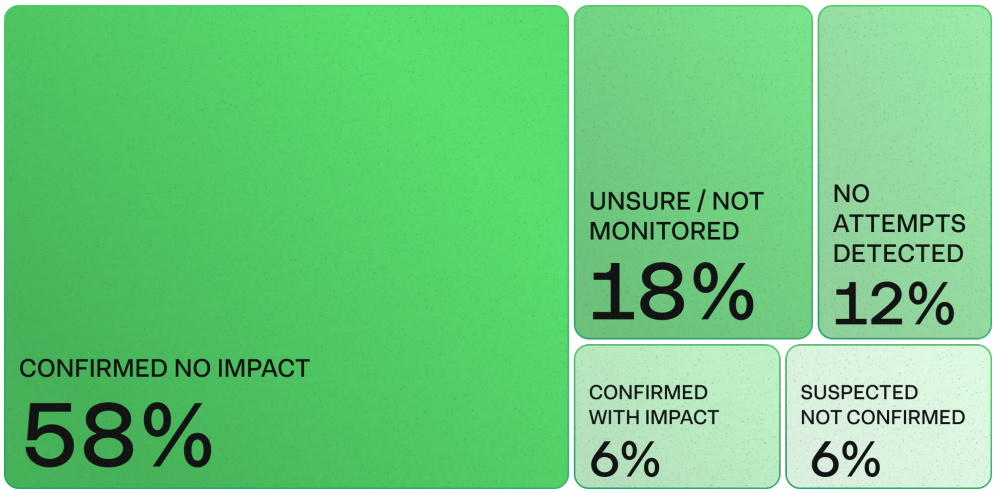
The vast majority of modern cybersecurity breaches start with a user who believed they were acting correctly.

Today's social engineering campaigns don't rely on malware or zero-day exploits. They manipulate real people, in trusted roles, through trusted channels, prompting them to complete what appear to be ordinary business tasks.

According to Dune Security's 2025 CISO Risk Intelligence Survey:

- → 64% of respondents confirmed social engineering or solicitation attacks against their users via encrypted or informal apps like WhatsApp, Signal, Telegram, Slack, Teams, or SMS.
- → 6% experienced a verified incident with measurable business impact.
- → 24% reported suspected encrypted or informal app attacks or did not have the necessary tools to verify or monitor these incidents.
- → Only 12% of enterprises detected no attacks via encrypted or informal apps.

Enterprise Exposure to Social Engineering via Encrypted and Informal Channels



Dune Security's 2025 survey finds that most large organizations experienced confirmed social engineering attacks through apps like WhatsApp, Signal, Slack, Teams, or SMS in the past 12 months.

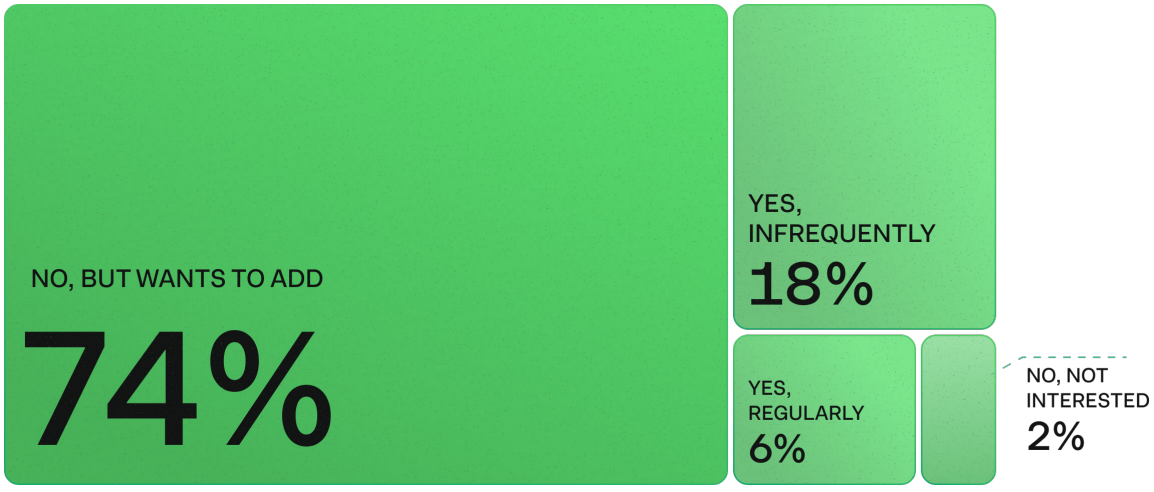
Modern attacks target channels where security controls are weakest: informal channels, personal devices, and off-channel communication platforms that are unmonitored. Attackers use AI to analyze internal tone, role hierarchies, and communication patterns, mimicking internal workflows and delivery across channels. This makes large-scale manipulation easy and efficient.

Despite recent advances in adversary tactics, most enterprise security programs still rely on outdated, standardized awareness training that is not tied to robust user risk quantification. Security readiness is typically judged by simple data points such as phishing click rates and inbox threat training completion, while attackers target behavioral patterns in channels that organizations rarely simulate.

CISOs recognize this gap:

- → 53% found their current awareness platform insufficient.
- → 41% were neutral about its effectiveness.
- → Only 6% were confident in its impact.
- → Average SAT effectiveness for preparing users against multi-channel attacks (SMS, voice, encrypted apps): 2.38/5.

Enterprise Simulation of Executive Impersonation Attacks



Dune Security's 2025 CISO Risk Intelligence Survey shows that very few enterprises run regular executive impersonation simulations today, though most want to add them.

Awareness efforts are too narrowly focused to address modern threats. None of the enterprise CISOs surveyed currently simulate attacks over encrypted messaging apps, and only 6% run regular executive impersonation scenarios, even as deepfake voice and spoofed messages increasingly cause real breaches.

The disconnect between attacker tactics and enterprise readiness leaves users vulnerable to threats they have never encountered. Without security programs that address today's increasingly complex, multi-channel social engineering risks, the User Layer will remain exposed to social engineering attacks.

Insider Threat

Insider Threat Is Shifting: From Malicious Intent to Manipulated Access

Insider threat refers to any risk that originates from a user within an organization, including careless, compromised, and malicious employees or third-party contractors.

Malicious insiders are the most traditionally recognized type of insider threat. These individuals act with intent, often driven by personal monetary gain, retaliation, or espionage. Insiders' direct access to internal systems and deep familiarity with organizational processes make them particularly dangerous.

However, not all insider threat today is the result of intentional sabotage. Insider threats also arise from compromised or negligent users. Compromised users fall victim to social engineering and unknowingly facilitate attacks. Negligent users introduce risk by mishandling data, misconfiguring access, or overlooking basic security practices. In both scenarios, these unintentional actions can expose the organization to serious harm.

Despite the scale of this risk, enterprise readiness remains dangerously limited. According to Dune's survey, only 26% of CISOs rate their insider threat readiness as high. The rest fall into moderate or low categories, exposing a critical maturity gap in how insider risk is understood, measured, and mitigated.

The core issue preventing progress is visibility. Most enterprises still don't monitor behavioral signals across mobile, collaboration, or encrypted messaging apps. They don't simulate impersonation over WhatsApp or test high-pressure approval scenarios in Slack, even though those are the same platforms attackers use to gain manipulated access.

Until security teams gain real-time insight into who's most exposed – and why – insider risk will remain invisible until it's too late.

Meet Scattered Spider

The Most Dangerous Cybercrime Group is Redefining Insider Risk

Scattered Spider represents one of the most advanced and dangerous cybercrime groups targeting the User Layer today, and they have perfected exploiting insider access.

Active since at least 2022, this financially motivated group specializes in targeting help desk agents, contractors, support teams – users with just enough access and just enough urgency to be weaponized. Rather than exploiting systems, their manipulation reaches users through encrypted apps, SMS, collaboration platforms, and deepfake voice calls, turning routine workflows into breach pathways through social pressure and procedural mimicry.

In 2025, Scattered Spider is reported to have bribed employees to gain unauthorized access to major American firms, resulting in hundreds of millions of dollars in potential losses or liabilities.[1] A single successful bribe – often involving urgent multi-factor authentication resets communicated via Telegram or WhatsApp – can convince an employee to provide attackers with access to critical infrastructure.

These attacks don't involve brute force or a malware exploit. They leverage insider access through real-time social engineering.

Scattered Spider has successfully breached companies across finance, retail, technology, insurance, aviation, and more, and the group's continued success highlights a critical truth: **modern insider threat can be initiated externally rather than solely originating from within the organization.**

Aliases: Scattered Spider, UNC3944, Octo Tempest, Muddled Libra, Scatter Swine

1 Sergiu Gatlan, "Coinbase Data Breach Exposes Customer Info and Government IDs," BleepingComputer, May 15, 2025, https://www.bleepingcomputer.com/news/security/coinbase-discloses-breach-faces-up-to-400-million-in-losses/.

Scattered Spider is already responsible for:

- → **$1B+ in conservative estimated financial loss across all sectors**: Publicly reported incidents and sector-wide analysis confirm that Scattered Spider has caused at least $1 billion in direct, confirmed and estimated financial losses since 2022, with the true total likely higher due to unreported and ongoing incidents.[2][3][4]
- → **71+ million customer records exposed in confirmed incidents:** Major breaches attributed to Scattered Spider include the exposure of over 65 million records at Caesars Entertainment (2023) and 5.7 million at Qantas Airways (2025), with additional exposures at other global brands.[5][6]
- → **100+ confirmed organizational breaches, including Fortune 500 companies:** High-profile victims include MGM Resorts, Aflac, DoorDash, Marks & Spencer, Co-op Group, Harrods, Qantas Airways, Twilio, Cloudflare, MailChimp, Riot Games, and others. [7][8][9]

2 The Hacker News, "Scattered Spider Behind Cyberattacks on M&S and Co-op, Causing up to $592M in Damages," n.d., https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html.
3 Chainalysis Team, "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," Chainalysis, June 23, 2025, https://www.chainalysis.com/blog/ransomware-2024/.
4 Brian Krebs, "Fla. Man Charged in SIM-Swapping Spree Is Key Suspect in Hacker Groups Oktapus, Scattered Spider," January 30, 2024, https://krebsonsecurity.com/2024/01/fla-man-charged-in-sim-swapping-spree-is-key-suspect-in-hacker-groups-oktapus-scattered-spider/.
5 Suzanne Rowan Kelleher, "2 Casino Ransomware Attacks: Caesars Paid, MGM Did Not," Forbes, September 14, 2023, https://www.forbes.com/sites/suzannerowankelleher/2023/09/14/2-casino-ransomware-attacks-caesars-mgm/.
6 Anthony Cuthbertson, "M&S Hackers Scattered Spider Stole Personal Data of 5.7 Million Qantas Customers, Airline Reveals," The Independent, July 11, 2025, https://www.the-independent.com/tech/security/hackers-scattered-spider-qantas-cyber-attack-m-s-b2787130.html.
7 Steve Alder, "Aflac Latest Insurer to Suffer Cyberattack and Data Breach," The HIPAA Journal, June 23, 2025, https://www.hipaajournal.com/aflac-data-breach/.
8 William Altman, "CyberCube: 2% of Large Firms at Highest Scattered Spider Risk," July 4, 2025, https://insights.cybcube.com/en/firms-highest-scattered-spider-risk.
9 "Alleged Boss of 'Scattered Spider' Hacking Group Arrested," June 16, 2024, https://krebsonsecurity.com/2024/06/alleged-boss-of-scattered-spider-hacking-group-arrested/.

Understanding the User Risk Surface

User Risk Extends Across Every Channel

Attackers now exploit every communication channel where users operate, including email, SMS, voice, collaboration platforms, and encrypted messaging apps. Each of these vectors presents unique behavioral risks, shaped by context, urgency, and trust.

The following pages analyze how groups like Scattered Spider exploit each major attack channel to compromise the enterprise from the inside out, revealing where social engineering succeeds, where user defenses break down, and why most organizations remain unprepared.

CISO Assessment of Threat Exposure and User Readiness Across Attack Vectors

Attack Vector	Simulation Coverage	CISO Concern	CISO Confidence
Email (Phishing)	100%	85%	27%
SMS (Smishing)	27%	71%	9%
Voice (Vishing)	15%	59%	9%
Collaboration Tools	9%	32%	15%
Encrypted Messaging	0%	38%	6%

Despite high concern and low confidence among enterprise CISOs, most organizations still fail to test or prepare users for attacks beyond email.

Phishing (Email)

Phishing 3.0: AI-Personalized Deception and the MFA Failure Chain

Among users who clicked on Dune's AI-personalized phishing simulations, 30% proceeded to submit their multi-factor authentication (MFA) credentials, proving how easily modern phishing can escalate to full compromise.

Phishing remains the most common entry point for enterprise attacks, and it continues to evolve in both speed and sophistication. In 2024, AI-generated phishing increased by 126%,[10] fueled by large language models that allow adversaries to craft messages with a level of precision previously unseen in social engineering. These attacks now mirror internal tone, replicate workflow patterns, and deliver platform-authentic visuals, all while adapting to business context, industry norms, and individual user roles with near-perfect accuracy.

In 2025, 85% of CISOs surveyed by Dune Security report phishing as a top social engineering concern, making it the most consistently cited threat vector. The reason is simple: attackers no longer rely on generic templates or broken English. Phishing has matured into a precision-crafted, AI-powered vector capable of bypassing technical controls and manipulating user behavior with alarming accuracy.

For the first time, Dune Security is releasing behavioral simulation data from phishing attack scenarios conducted across our platform, offering an inside look at how users actually respond under real-world conditions. The behavioral simulation data confirms a sharp rise in the effectiveness of AI-personalized phishing campaigns. These simulations, which replicate real-world attack vectors, show that AI-personalized emails now drive three times more user interaction than traditional, templated variants.

10 Jason Miller, "Struggling to Prevent Sophisticated Phishing Scams? Here's What You Can Do," n.d., https://www.bitlyft.com/bitlyftnews/struggling-to-prevent-sophisticated-phishing-scams-heres-what-you-can-do.

Even more troubling is the depth of user compromise. In our controlled simulations, 30% of users who engaged with AI-personalized phishing progressed all the way through the failure chain, ultimately submitting valid MFA credentials and granting attackers direct access to enterprise systems.

The four-stage breakdown is consistent across campaigns:

→ URL clicked (initial interaction)

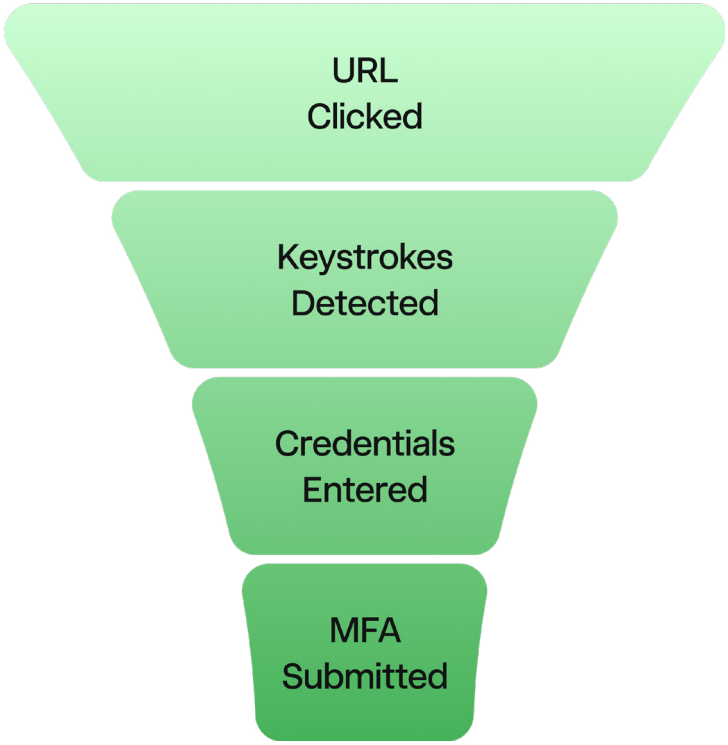
→ Keystroke detected (typing input)

→ Credentials entered (successful data match)

→ MFA submitted (OTP or authentication token)

Despite near-universal simulation coverage – 100% of enterprises surveyed currently test phishing – user readiness remains deeply inconsistent. Only 26% of CISOs express high confidence in their users' ability to detect and resist real-world phishing, while 15% report no confidence at all. This gap shows that even the most common and most tested threat remains fundamentally unsolved at the User Layer.

Behavioral Simulations Reveal the True Depth of Compromise



30% of users who clicked on Dune Security's simulations completed the full attack chain, including MFA submission.

Credential Phishing: The Most Effective – and Dangerous – Variant

Credential-based phishing outperformed link-based attacks by 21% in Dune Security's simulations, making it the most dangerous and consistently effective form of phishing.

Phishing campaigns pursue two primary objectives: credential theft and link engagement. Both carry significant operational risk, but credential harvesting remains the most direct, persistent, and difficult-to-detect route to enterprise compromise. Credential harvesting is the main goal in nearly 80% of phishing attacks,[11] and in the second half of 2024 alone, there was a 442% increase in social engineering campaigns aimed specifically at stealing credentials.[12]

The reason is straightforward: a single set of valid login credentials can unlock broad enterprise access, allowing attackers to move laterally, escalate privileges, and maintain persistence without triggering traditional security alerts.

This context makes Dune Security's simulation findings especially worrisome. When Dune ran controlled simulations that exposed users to both link-based and credential-based phishing attempts, users were 1.2 times more likely to engage with the credential variant. This means the tactic most likely to lead to full system compromise is also the one that users are most likely to fall for.

Unlike link-based phishing, which often ends at a click or download, credential phishing escalates user interaction. Credential attacks prompt users to submit sensitive information

Comparative Effectiveness of Credential and Link-Based Phishing Tactics

Users were 1.2x more likely to engage with credential harvesting than link-based attacks in Dune Security's simulations.

11 Kaseya and Kaseya, "Top 5 Types of Credential Harvesting Attacks," Kaseya, June 11, 2025, https://www.kaseya.com/blog/top-5-types-of-credential-harvesting-attacks/.
12 CrowdStrike, CrowdStrike 2025 Global Threat Report, CrowdStrike, 2025, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf.

like usernames, passwords, and MFA tokens into spoofed login portals that closely mimic trusted platforms, such as Microsoft 365, Okta, or internal HR systems.

Once a user submits their credentials, that data becomes the attacker's entry point, enabling authenticated access to core business systems, financial platforms, executive communications, and operational tools.

These outcomes are further reinforced when analyzing specific phishing methods. While credential and link phishing define the core attack depths, they are delivered through varied techniques, with some significantly more likely to drive user interaction than others.

Understanding which methods users engage with most is essential to building effective defenses. It reveals where users are most vulnerable to deception and where preventative controls and simulation efforts should be focused.

Some phishing methods are designed for scale, others for precision; but a few consistently produce higher failure rates, making them the most dangerous vectors by interaction probability.

Baiting led all phishing attack methods in user failure rate, with users nearly twice as likely to fall for these lures compared to any other tested method. These attacks are engineered to provoke immediate emotional responses – curiosity, fear, urgency – often through fake security alerts, expired password warnings, or rewards like bonus payouts and digital vouchers. Their strength lies in instinctive manipulation: users are prompted to act before thinking, bypassing scrutiny in favor of speed.

Link manipulation followed as the second most successful attack method. These attacks disguise malicious URLs behind familiar-looking anchors, making them difficult to detect at a glance, especially when business context or pressure is applied—a dynamic explored in detail in the next section.

Importantly, user interactions with attacks do not always correlate with business impact. For example, while business email compromise (BEC) engaged fewer users than baiting, it remains one of the costliest threats in the real world due to its targeted nature of high-value users, who have a much higher business impact upon breach. The same applies to spoofing and pretexting tactics, which are less frequent types of attacks, but frequently used in high-value fraud and executive impersonation.

While some techniques drive broader interaction, others, though less clicked, carry outsized business risk.

Behavioral Triggers: Pressure Drives User Failure

Users are five times more likely to fall for phishing emails that create pressure than those offering rewards.

Phishing now extends far beyond the typo-ridden, “spray and prey” emails of earlier years. Modern attacks succeed by manipulating behavior. AI-powered social engineering enables attackers to craft messages that feel urgent, authoritative, and personally relevant, mirroring the tone, timing, and context each user expects in their role. This behavioral precision suppresses skepticism and increases failure rates at the exact moment users are most likely to act without thinking.

To identify which emotional triggers drive user compromise most effectively, Dune Security analyzed user behavior across a massive dataset of phishing simulations. The study compares how five motivational factors – authority, urgency, curiosity, fear, and reward – influence user interaction.

Surprisingly, reward-based phishing performs the worst. Despite attackers continuing to use incentive-driven lures in both real-world attacks and training scenarios, these attacks generate nearly five times fewer clicks than the top-performing emotional triggers. Messages like “*Complete our eBay survey for a Visa gift card*” or “*$15 off your next Uber Eats order*” rank lowest across all user groups and industries.

Relative Effectiveness of Motivational Factors in Phishing

Based on Dune Security’s behavioral simulations, authority and urgency were most likely to drive user interaction, while reward-based lures were least effective across all user groups.

What works instead of reward-based phishing is emotionally charged messages, particularly those that apply pressure:

→ Authority was the most effective, generating 4.7 times more interaction than reward, nearly 2 times more than curiosity, and over 1.5 times more than fear.

Example:
"DocuSign request from IT: Complete contract acknowledgment"

→ Urgency ranked a close second, with a success rate 4 times higher than reward and nearly 1.7 times higher than curiosity.

Example:
"SharePoint contract pending review. Immediate action required"

→ Curiosity and fear also drove meaningful interaction. While less effective than authority or urgency, both were still more than 2 to 3 times stronger than reward-based lures.

Examples:
"New project assignment: View details in Asana"
"Google sign-in alert: Suspicious activity detected"

The results of Dune's dataset reinforce a critical behavioral insight: employees fall for phishing attacks not because they're careless, but because the message feels plausible. Authority, urgency, and curiosity resonate with daily workflows and prompt users to act reflexively, especially when presented under pressure.

For CISOs, understanding these emotional triggers is essential. It allows security teams to move beyond generic phishing templates and design programs that reflect the real decisions users face under stress – where instinct overrides inspection, and user behavior becomes the point of compromise.

User Readiness Drops Sharply When Attacks Go Mobile

Phishing Doesn’t Stop at the Email Inbox or Desktop

Mobile devices have become one of the most dangerous entry points for modern social engineering because they reach users outside of enterprise visibility.

On mobile devices, behavior changes. Users react faster, lower their guard, and make decisions without traditional monitoring. Attackers send phishing requests during commutes, between meetings, or after hours, making the message feel more urgent, informal, and routine. This compresses the decision-making process and nudges users to act on instinct.

Attackers understand this behavioral shift and are increasingly leaning into it. They deliver social engineering payloads over SMS and live voice calls, often targeting personal or unmanaged devices that sit outside corporate control.

Mobile-based attacks succeed not because users lack awareness, but because they force users into fast, high-pressure decisions, often without support or verification tools. Attackers exploit these conditions, and most security programs still fail to respond proactively.

The following pages examine smishing (SMS-based phishing) and vishing (voice-based deception), both of which use similar tactics: attackers pressure isolated users into making decisions with little time to think and even less protection.

Smishing (SMS)

Despite widespread attacks over SMS, only 9% of CISOs express high confidence in their users' ability to detect them.

SMS-based phishing, or smishing, has become a standard component of modern social engineering campaigns. Smishing attacks exploit the speed and informality of texting to deliver urgent, seemingly legitimate messages that prompt fast action, often impersonating a known executive, IT system, or vendor.

Organizational readiness remains dangerously limited. Despite the fact that 76% of enterprises experienced smishing attacks in 2024,[13] only 27% of surveyed organizations currently simulate smishing attacks and just 9% report high confidence in their users' ability to detect them. The attack surface is expanding, but simulation coverage and user preparation have not kept pace, leaving a widening visibility gap where mobile risk continues to grow unchecked.

Most SMS-based attacks target personal or unmanaged devices, where traditional monitoring tools cannot detect risky interactions. On these devices, links are harder to inspect, messages lack authentication cues, and users – often isolated from formal workflows – are more prone to act on instinct.

Smishing messages are deliberately designed to exploit these conditions. They create urgency ("Approve this payroll update"), leverage authority ("IT support needs your confirmation"), or spark fear ("Your account is locked. Verify immediately"). Users are more likely to react reflexively to these attacks because they often receive them when their guard is down – in transit, between meetings, after hours, or while distracted.

Until simulation and detection efforts extend into mobile channels, attackers will continue to exploit this behavioral blind spot – one that CISOs overwhelmingly acknowledge, but few have operationalized protection against.

13 Proofpoint, 2024 State of the Phish Report, Proofpoint, 2024, https://assets.contentstack.io/v3/assets/blt9e072702140c498e/blt9dea8b450bace030/673b57969cb794dccfa2edf0/2024_State_of_the_Phish_Report_US.PDF

Vishing (Voice)

Voice-based phishing now ranks as a top concern for 59% of CISOs – yet just 15% of enterprises simulate it.

Vishing, or voice-based phishing, now ranks as the third most concerning social engineering threat among CISOs, falling just behind email and SMS-based attacks. Dune Security's 2025 CISO Risk Intelligence Survey shows that 59% of CISOs rate vishing as a top social engineering threat, reflecting a clear rise in executive attention as attackers shift from static messages to real-time, human-sounding deception.

That concern is well-founded. Vishing-related financial losses have surged 550% since 2022,[14] and attack volume rose 442% in the second half of 2024 alone.[15] These attacks are scaling faster than enterprise defenses are adapting, amplified by AI tools that spoof voices, mimic internal workflows, and apply social pressure in real-time.

Despite this rising business risk, preparation remains dangerously misaligned. Only 15% of surveyed organizations simulate vishing scenarios, compared to 27% for smishing, revealing a 12-point readiness gap between two vectors that CISOs rate nearly equal in perceived risk. The result is a growing disconnect between threat awareness and operational readiness.

User readiness is similarly concerning. One-third of CISOs report they are not at all confident in their workforce's ability to detect vishing attacks, none express extreme confidence, and 56% rate user readiness as only moderate or limited. This is a clear signal that most employees remain unprepared for the manipulative tactics embedded in voice-based deception.

Attackers are leaning into vishing for a reason: it works. AI has made these campaigns faster to launch, harder to detect, and more effective at earning user trust. Voice lends

14 Federal Bureau of Investigation, 2024 Internet Crime Report, Internet Crime Complaint Center (IC3), 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
15 CrowdStrike, CrowdStrike 2025 Global Threat Report, CrowdStrike, 2025, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf.

urgency, credibility, and familiarity. AI-generated calls can convincingly replicate known voices, roles, and communication styles. Whether it's a spoofed IT helpdesk requesting an MFA reset or a fake CFO issuing a verbal wire request, these attacks exploit the trust users instinctively place in recognizable voices and real-time requests.

Still, few enterprises actively prepare users for this type of attack. The result is a widening readiness gap between how voice-based attacks are delivered and how users are trained to respond.

CISOs are right to be alert. The volume of vishing attacks is rising, business impact is escalating, and most employees remain unprepared. Until testing and simulation efforts extend into voice channels, vishing may become the next major point of enterprise failure.

Your Biggest Blind Spot

Encrypted and Internal Channels Are the Least Defended

As attackers refine real-time deception tactics across voice and mobile, they are also expanding into even less visible territory: trusted collaboration platforms and encrypted messaging apps. Tools like Slack, Teams, WhatsApp, and Telegram have become core to daily workflows, yet because they feel internal, familiar, or "consumer-grade," they're too often treated as mere extensions of team communication rather than vectors for social engineering. That misplaced trust is exactly where the blind spot begins.

A recent wave of attacks brings this shift to light. Storm-2372, a nation-state threat group, reportedly bypassed traditional phishing defenses by pushing genuine Microsoft 365 device-authentication prompts through Slack, Teams, and WhatsApp. Users saw what appeared to be normal login requests and entered their credentials into real Microsoft portals, unaware that Storm-2372 was harvesting their authentication tokens in real-time. Once access was granted, the group quietly escalated privileges, moved laterally, and extracted sensitive data, all without triggering a single phishing alert.[16]

This tactic reveals a deeper truth: attackers now target the systems where trust is assumed and visibility is low – tools employees rely on daily, but security teams often overlook.

Dune Security's 2025 CISO Risk Intelligence Survey confirms the scope of this gap. Despite their ubiquity, collaboration platforms and encrypted messaging apps remain among the least tested and least visible channels in the enterprise. On these platforms simulations are rare, monitoring is limited, and user confidence is dangerously low.

What follows is a closer look at how attackers are exploiting these channels to bypass scrutiny, hijack workflows, and exploit trust where it's least expected.

16 Matt Kapko, "Threat Researchers Spot 'Device Code' Phishing Attacks Targeting Microsoft Accounts," CyberScoop, February 14, 2025, https://cyberscoop.com/russia-threat-groups-device-code-phishing-microsoft-accounts/.

Collaboration Platforms (Slack, Teams, Zoom Chat)

Collaboration platforms are central to how work gets done, yet 91% of enterprises do not run simulations on them.

Collaboration platforms like Slack, Microsoft Teams, and Zoom Chat have become core to how work gets done. Fast and informal, they're deeply embedded into daily workflows and often replace email as the default space for decision-making, approvals, and sensitive communication. That fluidity is a strength, but it is also a vulnerability.

According to Dune Security's 2025 CISO Risk Intelligence Survey, only 9% of enterprises currently simulate social engineering attacks on collaboration platforms. That means more than 9 out of 10 organizations are leaving platforms like Slack, Teams, and Zoom Chat completely untested, despite their everyday reliance for business-critical tasks. User readiness is no better: just 15% of CISOs expressed high confidence in their workforce's ability to spot threats inside collaboration platforms. In systems used for approvals, sensitive conversations, and decision-making, this combination of low testing and low confidence represents a critical blind spot that attackers are already exploiting.

In a 2025 campaign, former Black Basta affiliates weaponized that blind spot by posing as IT support on Microsoft Teams and coaxing users into installing legitimate remote-access tools like Quick Assist or AnyDesk. Once granted access, the attackers ran scripts to harvest credentials and move laterally, bypassing traditional phishing defenses by exploiting the implicit trust in enterprise collaboration channels.[17]

What makes collaboration platforms particularly dangerous is not just their frequency of use, but the implicit trust they carry. Attackers pose as colleagues, vendors, or IT support to share malicious links, solicit sensitive information, or initiate fraudulent actions, often without raising suspicion. Without simulations that reflect the internal dynamics of collaboration platforms, security teams have no clear visibility into user behavior or response readiness in this critical layer.

17 The Hacker News, "Former Black Basta Members Use Microsoft Teams and Python Scripts in 2025 Attacks," n.d., https://thehackernews.com/2025/06/former-black-basta-members-use.html.

Encrypted Channels

The Most Dangerous Blind Spot in the Enterprise

Encrypted messaging apps like WhatsApp, Signal, Telegram, Facebook Messenger, and Viber were designed for privacy and speed, not enterprise control. Today, that design is being exploited at scale. These platforms offer attackers direct access to employees through private channels that operate entirely outside traditional monitoring, simulation coverage, and policy enforcement.

The impact is already visible. Fraud originating from encrypted apps now accounts for nearly 40% of global scam reports. Telegram-based scams alone surged 121% in the second half of 2024, while WhatsApp scams rose 67%, reflecting aggressive attacker adoption.[18]

Yet organizational defenses remain almost nonexistent. Dune Security's 2025 CISO Risk Intelligence Survey found that not a single organization reported simulating attacks on encrypted messaging platforms, making it the only channel in the survey with zero testing coverage despite its growing role in real-world attacks.

Users are not prepared for encrypted channel attacks. Only 6% of CISOs express high confidence in their employees' ability to detect threats in these apps, while over 42% report no confidence at all – the weakest score of any channel we measured.

This gap is exactly what attackers exploit. Malicious messages land on personal devices, often outside business hours, and carry the illusion of informality and trust. A fake CEO might request a document over WhatsApp; a spoofed Signal message might initiate a password reset. Either way, there's no second layer of scrutiny: no filters, no warnings, and no oversight. These manipulations are fast, direct, and nearly impossible to detect after the fact.

18 Revolut, "Scammers Are Shifting to Encrypted Apps Like WhatsApp and Telegram," Revolut, March 31, 2025, https://www.revolut.com/en-US/news/scammers_shifting_to_secure_encrypted_apps_whatsapp_telegram_reports_revolut_meta_still_biggest_overall_source_of_scams/.

Despite this, fewer than 4 in 10 CISOs consider encrypted apps a top concern, leaving a nearly 40-point gap between perceived risk and simulation coverage, the largest disconnect in the entire survey.

This is what makes encrypted messaging uniquely dangerous. These platforms are widely used, but the enterprise has no visibility, no preparation, and no margin for instinctive user error. It is the most overlooked – and most actively exploited – behavioral blind spot in the modern enterprise.

What's Holding Teams Back

Leadership is aligned, but operational reality is holding security teams back.

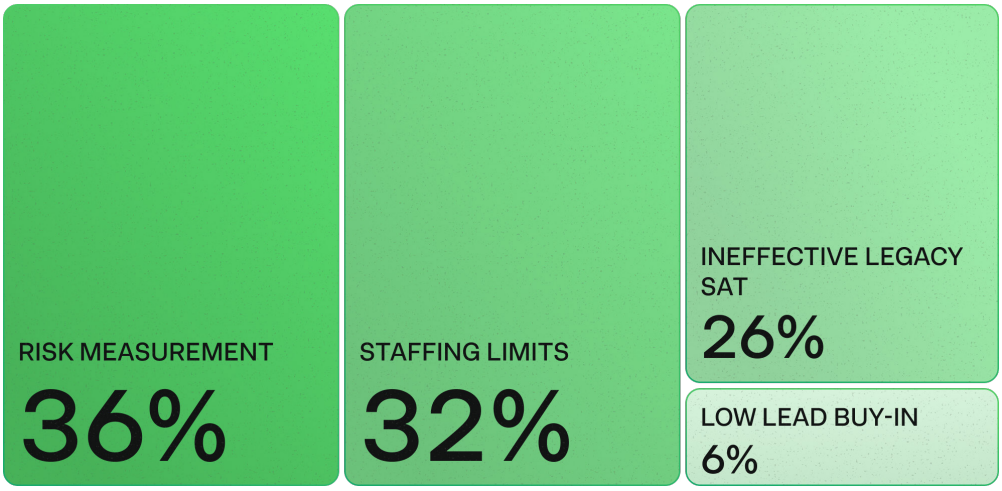
Dune Security's 2025 CISO Risk Intelligence Survey finds that the real barriers to user readiness are operational: limited visibility, constrained teams, and outdated tools.

Security leaders broadly agree that the User Layer is dangerously exposed. Nearly every organization runs phishing simulations. Many acknowledge that modern attacks span far beyond email. Yet readiness remains low because most teams are blocked by persistent, systemic barriers that make it difficult to pinpoint risk and act where it's needed the most.

Dune's Survey reveals that 93% of CISOs cited one of three operational constraints as the biggest obstacle to improving user readiness:

- → Difficulty measuring user-level risk or points of exposure (36%)
- → Insufficient time or staff to manage and act on insights (32%)
- → Legacy tools that fail to engage users or educate against real-world attack vectors (26%)

What's Blocking User Readiness?



Reasons enterprise CISOs attribute to preventing User Layer readiness, according to Dune Security's 2025 CISO Risk Intelligence Survey.

By contrast, only 6% cite lack of executive buy-in or leadership prioritization, making it the survey's least-cited barrier by a wide margin.

The operational challenges CISOs face today are not isolated. They are overlapping, compounding, and deeply operational. CISOs aren't struggling with awareness or intent, they're struggling to scale execution. Without visibility into which users are vulnerable, without the time to manage insights, and without tools that are purpose-built to prevent social engineering and insider threat, security teams are left flying blind.

This confirms a crucial industry insight: support for user risk programs exists at the top, but most organizations lack the operational precision, behavioral insight, and simulation depth needed to drive change at scale.

What Leading CISOs Are Prioritizing Next

Modern Threats Demand a Solution that Evolves as Quickly as Attackers

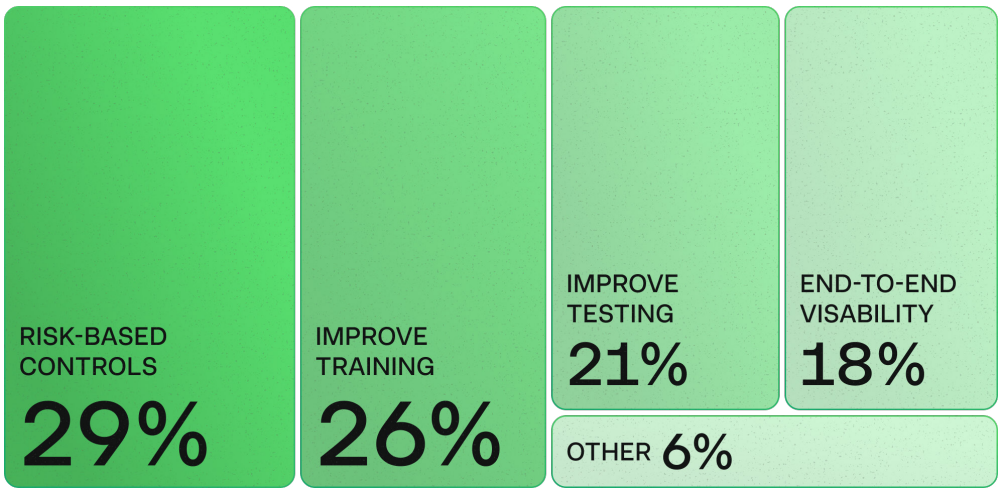
CISOs are now advancing toward a more intelligent and behavior-based model of User Layer defense to overcome persistent constraints in visibility, resources, tooling, and execution.

With legacy awareness programs falling short, security leaders are reorienting around what matters most: gaining user- and department-level intelligence that enables insight, precision, and meaningful intervention, rather than static compliance.

To better understand how this shift is taking shape, Dune's 2025 CISO Risk Intelligence Survey asked enterprise CISOs to identify their top User Layer priority for the remainder of the year. The results, shown below, reveal a decisive shift in strategic focus.

Rather than relying on static training or generic simulations, CISOs are prioritizing dynamic, behavior-driven capabilities that surface real-time exposure and drive intelligent intervention.

CISOs' Top User Risk Priorities for 2025



Based on Dune Security's 2025 CISO Risk Intelligence Survey, what matters most is the ability to identify, understand, and reduce User Layer risk.

29% of CISOs ranked implementing risk-based controls that trigger adaptive actions or restrictions based on real-time user behavior as a top priority. Close behind, 26% prioritized improving training with more personalized, engaging content based on user behavior and risk.

Together, these survey findings signal a clear pivot: modern user risk programs must be real-time, behavior-driven, and operationally integrated.

While CISOs still value efficiency, it is not their central focus. Only 3% of CISOs prioritize automation to reduce administrative burden, and another 3% place minimizing user time spent on training at the top of their agenda. Instead, security leaders prioritize what matters most: gaining real-time insight and deploying capabilities that directly expose and reduce User Layer risk.

The message is clear: CISOs are no longer focused on generic awareness programs or static simulations. They are ready to execute intelligent user risk strategies that deliver visibility, surface exposures, and trigger targeted intervention exactly where it's needed most.

The Future of User Layer Defense Starts Here

Dune Security was built to address the exact barriers holding teams back: lack of visibility, outdated tooling, and the inability to act precisely where risk lives.

Our User Adaptive Risk Management solution automatically prevents insider threats and social engineering by simulating multi-channel attacks, scoring user risk, and adapting training and controls in real-time.

With Dune, security teams gain continuous visibility into User Layer exposure: who's vulnerable, why, and how that risk is evolving.

Our platform scores each user across four critical dimensions: business impact, behavioral signals, training activity, and real-world performance.

This allows CISOs to do what traditional tools can't:

- → Run User Adaptive phishing, smishing, deepfake, and encrypted channel simulations to see how far users progress down the failure chain.
- → Deliver behavior-based training that's personalized to the user's role, risk level, and company policies.
- → Trigger adaptive controls like access restrictions, step-up authentication, or SecOps escalation to lock down high-risk behaviors.
- → Respond precisely where risk is concentrated, without wasting time on users who don't need intervention.

Instead of generic simulations and static awareness programs, Dune empowers security teams with the insight and control they need to reduce User Layer risk at scale – measurably, intelligently, and without added strain on staff.

The result is a defense model that reflects today's attack surface and tomorrow's readiness standard.

Madeira Security, Inc.
New York, NY
Printed in the United States of America | September 2025

This report includes proprietary analysis developed by Madeira Security, Inc. It contains data from the 2025 Dune CISO Risk Intelligence Survey, along with insights from the company's behavioral simulation platform and internal research. All survey data reflects self-reported responses and is presented in aggregate. Where third-party data or references are included, they are cited accordingly and remain the property of their respective organizations. Madeira Security, Inc. does not independently verify, validate, or audit third-party data, and all results based on such data are provided on an "as is" basis without representation or warranty as to accuracy, completeness, or suitability. Madeira Security, Inc. disclaims any liability arising from the use or interpretation of third-party content included herein.

This report is intended for general guidance only. It is not a substitute for independent research, legal advice, or the exercise of professional judgment. Madeira Security, Inc. shall not be responsible for any financial loss, reputational harm, security incident, or other consequences resulting from reliance on this publication.

For questions, citations, or permissions, contact:
legal@dune.security
dune.security

Ready to Quantify and Reduce User Risk at the Source?

See how leading teams prevent Insider Threats and Social Engineering with Dune Security.

Learn more at:
dune.security