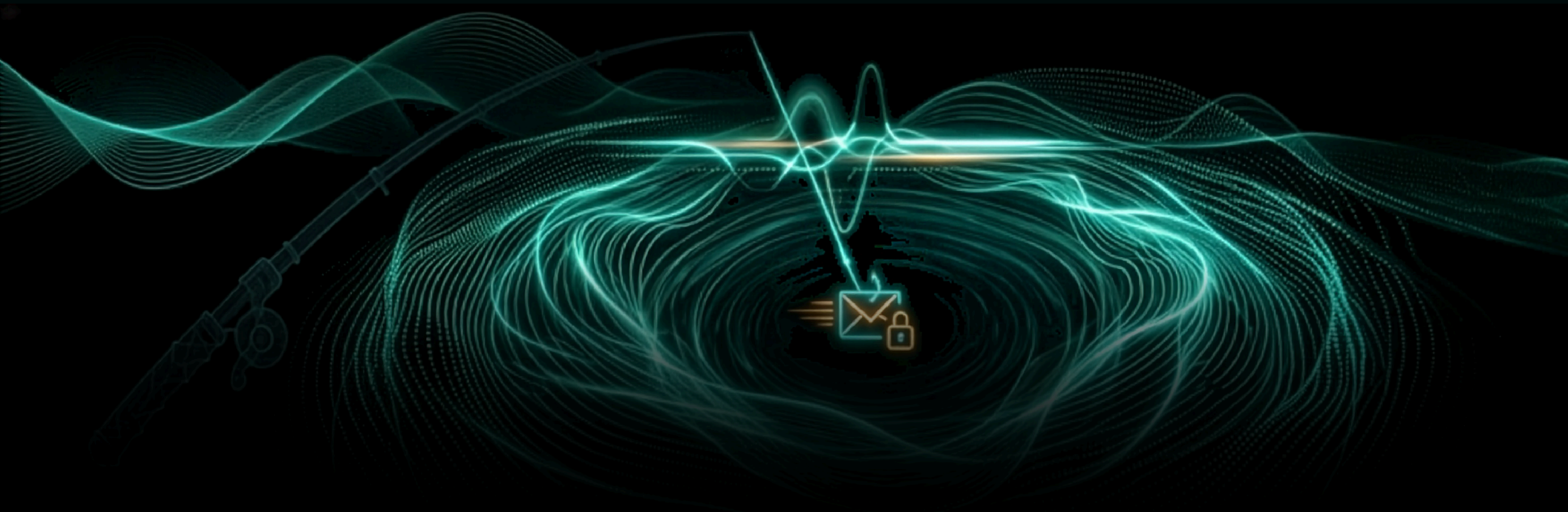
2026

SpyCloud

PHISHING
PULSE REPORT



CONTENTS

What's inside

▶ The data in this report is from a 2026 field survey of security leaders and practitioners unless specified otherwise. **Read about this report ›**

The attacks that make headlines are rarely the sophisticated ones.

They are, however, the predictable ones. A single employee receives a phishing email, clicks a link that looks exactly like the login page they're used to, and enters their credentials.

We know it happens. It's almost an old troupe – if it wasn't so true – that humans are our weakest link in security. Phishing attacks exploit human flaws with well-crafted messages arriving from what appears to be a trusted source. And despite extensive training and tools, we still have a major problem on our hands.

Today's phishing attacks are relentlessly successful. Packaged phishing-as-a-service (PhaaS) options and AI tooling generate phishing messages increasingly indistinguishable from legitimate ones.

Worse, the consequences now extend beyond the compromised account. A successful phish often hands the attacker a **session token and a refresh token** that grant authenticated, persistent access to the employee's inbox, contacts, calendars, and shared files – all without triggering a single MFA prompt, resetting when the password changes, or raising a behavioral flag in any monitoring tool.

> **At some point, an employee is going to click the wrong thing. The question now is what can security teams actually see *and* do in the window afterward?**

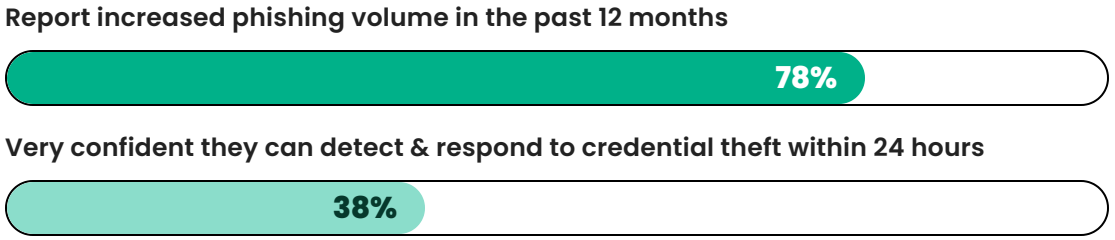
BY THE NUMBERS

The numbers prove the point

Three patterns surface again and again across the enterprise security teams we surveyed – the scale of the threat keeps climbing, while the capability to respond lags behind. The space between each pair is the exploitable gap.

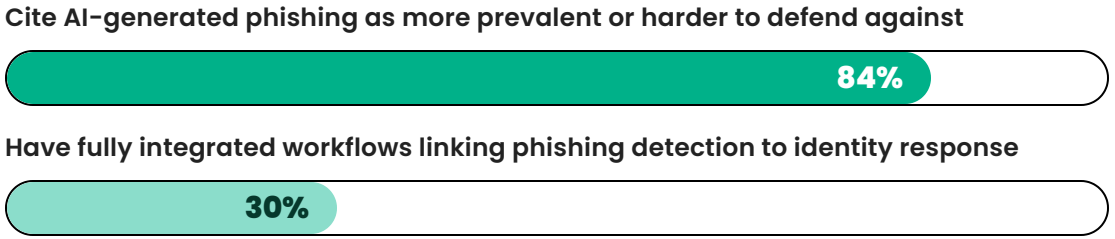
Volume is surging, but response capability lags

Phishing keeps coming – confidence in catching it fast does not keep pace.



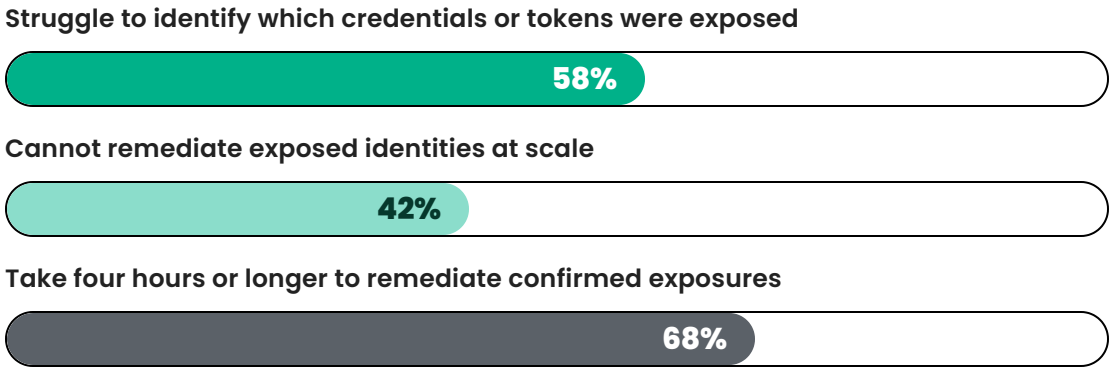
AI is redefining the landscape, but identity response stays siloed

Awareness of AI-driven attacks is near-universal; the connected workflows to act on them are not.



The detection-to-remediation gap creates exploitable windows

Three compounding shortfalls keep the door open after a successful phish.



Phishing is surging – and the barrier to entry has collapsed

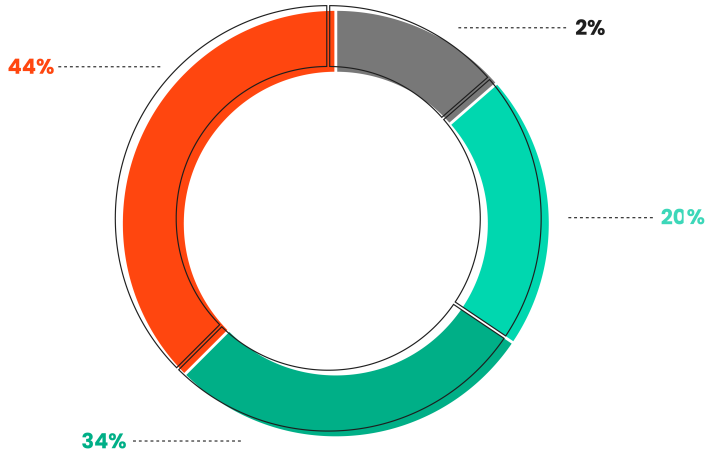
PhaaS has revolutionized the ease and speed with which bad actors can execute phishing attacks. These platforms operate on a subscription model that mirrors legitimate software-as-a-service – but with entirely criminal intent.

For as little as $50 to $250 USD, threat actors gain monthly access to fully managed kits that include sample phishing pages, one-click site deployment, and feature-rich admin panels with multiple exfiltration options. From purchase to active campaign, setup can take just minutes – without the need for any programming knowledge or technical expertise.

THE HEADLINE FIGURE

78% of organizations report phishing volume has increased moderately or significantly over the past 12 months.

REPORTED CHANGE IN PHISHING VOLUME OVER THE PAST 12 MONTHS



ENTERPRISE SPOTLIGHT

Fortune 100 & FTSE 100 in the crosshairs

SpyCloud analysis of PhaaS activity reveals a clear and deliberate focus on enterprise targets. Recent data from Tycoon 2FA shows minimal weekend engagement, with activity concentrated during the Western work week – a strong signal that corporate employees are the intended victims. Roughly 80% of credentials Tycoon captures belong to corporate accounts, not free providers like Gmail or Yahoo.

Broadening across PhaaS platforms, about **half of all phishing-sourced records are enterprise-tied**. By contrast, SpyCloud's infostealer malware data shows only ~11% of infected records are corporate – meaning phishing is roughly **five times more targeted** ↗ toward enterprises than malware.

WHY IT MATTERS

Phishing is now about **5x** more targeted toward enterprises than malware – up from **~3x** in December 2025. Remediation must match that reality, treating every successful phish as a potential credential, session, and token compromise.

86%

of the Fortune 100 had employee data exposed in phishing attacks in the last 12 months. The technology sector is hardest hit, followed by airlines and automotive.

47%

of the **FTSE 100** had employee data exposed. The energy sector is hardest hit, followed by telecommunications and financial services.

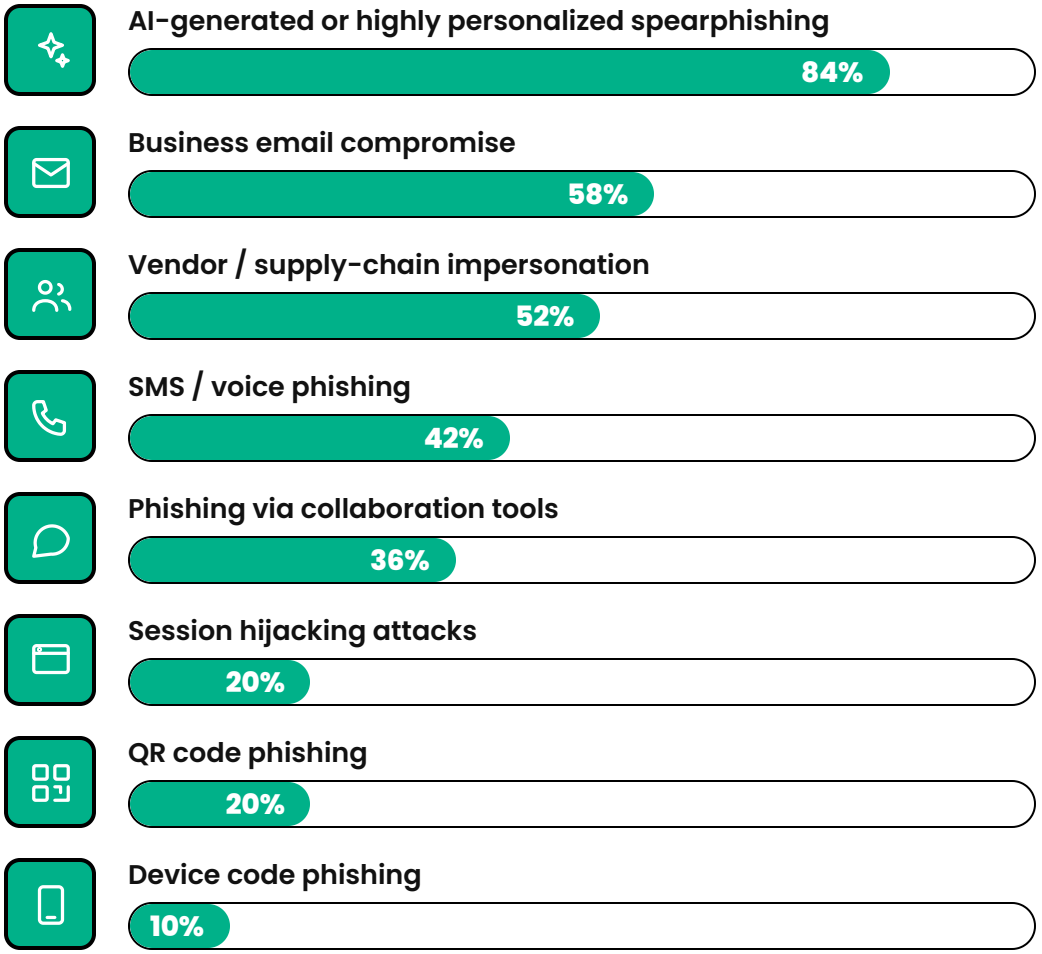
Information on this page is from a SpyCloud analysis of recaptured data from criminal underground sources.

The most prevalent – and hardest to defend – phishing attacks

To no one's surprise, **AI-generated phishing is the dominant concern**, cited by 84% of respondents – a clear signal that traditional email security is being outpaced by machine-generated personalization.

Business email compromise (58%) and vendor impersonation (52%) remain persistent. Emerging vectors like collaboration-tool phishing (36%) and session hijacking (20%) show teams are increasingly aware of what's at stake beyond the inbox.

Share of respondents citing each as most prevalent or most difficult to defend against.



ADVERSARY-IN-THE-MIDDLE SPOTLIGHT

Device code phishing is the threat to watch

Adversary-in-the-middle (AiTM) phishing is the latest threat to watch. A particularly nefarious variant – **device code phishing** – exploits the legitimate OAuth 2.0 Device Authorization Grant flow, tricking victims into entering an attacker-generated code that causes OAuth to issue valid access and refresh tokens directly to the attacker's device.

It's especially effective against enterprises because most workers keep an active Microsoft 365 session open all day – so that session satisfies the trust requirement and **no additional MFA challenge is triggered**. The stolen tokens then persist, which is why combating it requires **explicit token revocation** – a step most incident response playbooks don't yet account for.

KITS IN BROAD CIRCULATION

Device code phishing kits we actively track at SpyCloud include **Tycoon 2FA**, **FlowerStorm, Venom,** and **Kali365**.

THE OAUTH DEVICE-GRANT ABUSE, SIMPLIFIED

The lure

The victim is tricked into entering an attacker-generated device code.

Trust inherited

Their live Microsoft 365 session satisfies trust.

Tokens issued

The server issues valid tokens once the victim completes the OAuth process.

Silent persistence

Tokens persist for months and survive password resets – only explicit revocation closes the window.

Three stolen artifacts – and why refresh tokens are the most valuable to attackers

AiTM and device code phishing capture three distinct artifacts, each with its own risk profile.

1. Session cookies

Grant attackers **hours of immediate access**. The risk closes when the session expires or is revoked – the shortest-lived of the three.

2. Refresh tokens THE ONE TO WATCH

Operationally the most valuable to attackers. They **silently generate new session cookies for months** – no login, MFA prompt, or behavioral signal. In most enterprises a stolen refresh token **survives a password reset**; closing the window requires explicit token revocation through the IdP.

3. Session tokens

Represent the **authenticated state within the identity provider itself**, letting an attacker navigate to any SSO-connected application without being challenged.

What about phishing-resistant MFA?

A common question after learning about device code phishing: do FIDO2 hardware keys, YubiKeys, and passkeys solve this?

They do defeat the classic AiTM reverse-proxy relay. Origin binding prevents the key from signing on an attacker's proxy domain, so no token is ever issued.

But protection is only as strong as its weakest link. Origin binding protects you *only* when WebAuthn is enforced correctly – and there's no fallback to a phishable factor like a push, OTP, or password when the key fails. **That fallback gap is the usual real-world defeat.**

Device code phishing sidesteps origin binding entirely by keeping authentication on legitimate infrastructure – a real Microsoft domain – so the binding check never applies. SpyCloud researchers have observed a marked increase in this attack vector as of 2026 as threat actors adapt to wider FIDO2 deployment.

The same limitations apply to other post-authentication threats:

- **Infostealer malware** that steals tokens after a legitimate login – the key performs correctly, but tokens are extracted from the device afterward.
- **OAuth consent phishing** that tricks the user into granting delegated permissions through a legitimate flow. FIDO2 has no visibility into authorization decisions.
- **Primary Refresh Token (PRT) theft** on Entra ID-joined devices, extracted by malware outside the authentication flow.

Phishing-resistant MFA reduces one attack surface significantly – but it leaves the **token theft surface wide open**.

POST-COMPROMISE

What attackers do with phished access

Once tokens are stolen, attackers move fast. In a typical Microsoft 365 environment that means immediate access to a victim's full inbox and sent mail, contacts and calendar, SharePoint sites, shared drives, Teams channels, and any third-party apps connected via SSO.

AI has compressed the post-compromise timeline even further. Threat actors can now analyze entire mailboxes and draft convincing business email compromise (BEC) replies – matched to the victim's writing style – within minutes of initial token theft. Inbox rules are planted to hide the activity, and access is either monetized through BEC schemes or resold on criminal markets.

KEY TAKEAWAY

Continuous identity threat monitoring remains necessary regardless of MFA tier.

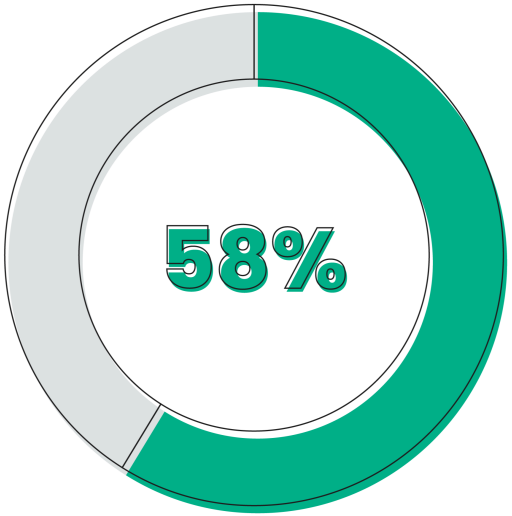
EXPOSED THE MOMENT A TOKEN IS STOLEN

- **Full inbox & sent mail**
- **Contacts & calendar**
- **SharePoint sites**
- **Shared drives**
- **Teams channels**
- **SSO-connected apps**

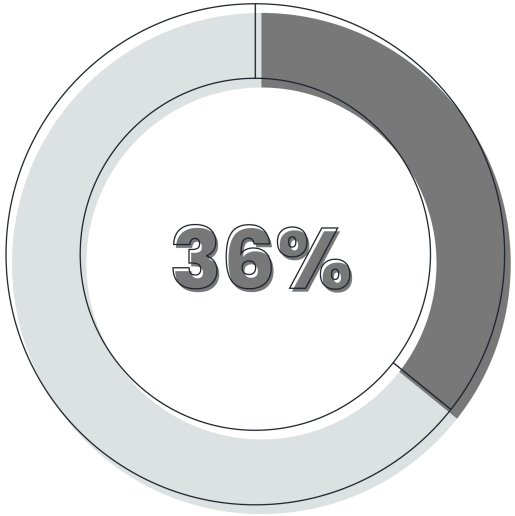
Each becomes a launch point for lateral movement, BEC, and resale – before a single behavioral alert fires.

The biggest post-phishing challenge: knowing what was actually stolen

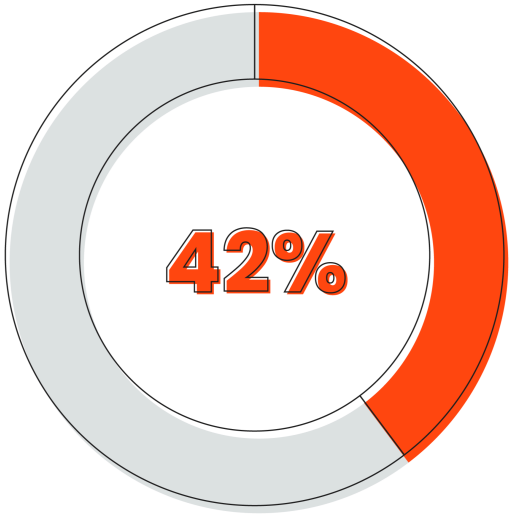
The core challenge in combating phishing is visibility. When nearly two-thirds of organizations can't reliably determine which credentials and authentication data were compromised, every downstream decision becomes a guessing game – and that uncertainty compounds quickly.



58% struggle to identify which **credentials or session tokens** were exposed



36% have **no reliable way to know** if stolen data was weaponized



42% struggle to remediate exposed identities **at scale**

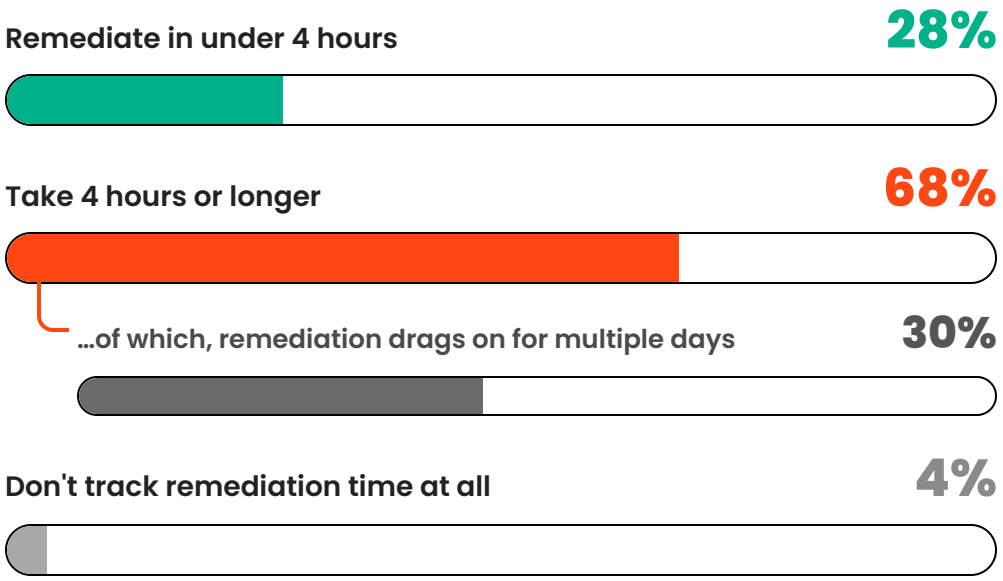
TOKEN VS. CREDENTIAL

In AiTM and device code phishing, the traditional credential may not have been stolen at all – what was taken is the post-authentication **session cookie and refresh token**. Teams that only look for exposed credentials after a successful phish are looking in the wrong place.

Remediation speed varies widely – and leaves windows open

When it comes to phishing remediation, time is the variable organizations can least afford to ignore. The vast majority operate with an open window during which stolen credentials and tokens remain active and exploitable.

Every hour without remediation is an hour threat actors can use to move laterally, escalate privileges, or monetize access. And for the **4% who don't track timelines at all**, the problem is more fundamental – you can't close a window you don't know is open.



Time to remediate after a confirmed phishing attack. "Multiple days" is a subset of the 68% taking four hours or longer.

How to modernize your post-phishing response

Effective response starts with a mindset shift: stopping a phishing email from reaching an inbox is only half the battle – and increasingly a losing one. Even the best detection tools miss what happens next, as captured credentials and post-authentication artifacts get repurposed for session hijacking, account takeover, fraud, and ransomware.

Visibility into what was compromised – credentials, session cookies, and tokens – and the ability to act before threat actors do is vital. That means resetting passwords, revoking cookies and tokens, and/or triggering enhanced authentication, and zeroing in on exposed users who appear on phishing target lists.

Speed and scale are equally critical. Manual workflows can't keep pace with modern campaigns. The most resilient organizations remediate phished identities automatically via native integrations or by triggering workflows in SOAR, IAM, or fraud detection platforms.

Reset passwords
On confirmed-exposed identities.

Revoke & re-issue MFA
To step up authentication.

Revoke sessions & refresh tokens
Through the identity provider.

Monitor phishing target lists
Watch exposed users proactively.

▶ PRO TIP – REFRESH TOKEN REVOCATION

For AiTM and device code phishing, credential reset alone is insufficient. The refresh token must be **explicitly revoked** through the IdP – a step separate from, and surviving, a password reset. Building it into the playbook is the single highest-impact change most teams can make.

THE BOTTOM LINE

Security teams must build a response capability that continuously monitors for evidence of compromise across both workforce and consumer identities – one that turns a successful phish into a dead end for attackers, every time.

WITH SPYCLOUD

What post-phishing response looks like with SpyCloud

SpyCloud recaptures phished artifacts directly from criminal infrastructure, targeting lists, and active campaigns – before stolen credentials, cookies, and tokens are used against you.

1

IDENTIFY THE EXPOSURE

SpyCloud detects that a specific employee's credentials, refresh token, or session cookie has appeared in criminal markets or active phishing infrastructure.

2

SIGNAL THE IDENTITY PROVIDER

SpyCloud automatically signals the IdP or directory service to reset passwords, step up authentication, and/or revoke all active sessions and tokens simultaneously – via integrations with Okta, Entra ID, Active Directory, Ping Identity, and more. **Session revocation** closes the active window; **refresh token revocation** closes the months-long persistence window that survives password resets.

3

RENDER THE DATA USELESS

All identity data associated with the victim is rendered useless to the attacker at once.

4

FORCE A CLEAN RE-AUTHENTICATION

The employee re-authenticates with full MFA on their next access attempt, establishing clean, verifiable sessions.

ABOUT THE DATA

This report features insights from a research survey of 50 enterprise security leaders and practitioners at organizations with 1,000+ employees, focusing on how they perceive and address phishing threats, plus unique research into SpyCloud's millions of recaptured phished records tied to enterprise organizations around the globe.

- **Roles:** 36% leadership, 34% mid-level managers, 30% analysts and specialists
- **Industries:** SaaS/software, IT services, manufacturing, financial services, healthcare, government
- **Regions:** United States, Canada, Europe

TURN EVERY PHISH INTO A DEAD END

SpyCloud recaptures phished credentials, cookies, and tokens from criminal infrastructure – then automatically resets passwords, revokes sessions, and explicitly revokes refresh tokens through your identity provider, shutting attackers out in minutes.

TALK TO AN EXPERT →

SEE HOW IT WORKS →

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations.