

Cyber Threat Report Q3 2026

The SMB Threat Playbook.

Told Through the Data

Using Cyber Threat Intelligence to understand why small businesses become targets—and how Telcos can reduce their exposure.



Table of Contents

Introduction	The Question We're Asking Wrong	03
Reality	Cyber Protection KPIs for SMBs	04
Opportunity	What Makes an SMB Attractive?	06
Five Dimensions	Access, Money, Routine, Trust, Action	09
Allot Solution	Protection Without More Complexity	21
Closure	Main Conclusions	22
About this Report	Methodology and external references	23

The Question we're Asking Wrong

INTRODUCTION

Why do cybercriminals target small businesses?

The usual answers are familiar: limited security budgets, fewer IT resources, and less sophisticated protection. But those explanations focus on who the victim is, rather than what the attacker sees.

Attackers see something different: valuable business accounts, payments moving between companies, employees logging into trusted platforms, files being downloaded, and dozens of everyday digital interactions they can imitate, redirect, or exploit.

And those opportunities are widespread. In just three months, almost 50% of the SMBs we protected encountered at least one live cyber threat that the solution stopped.

So perhaps the more useful question isn't "Why small businesses?"

It's: **What makes everyday SMB activity exploitable?**

That's the question this report investigates.

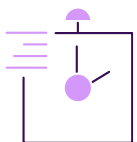


REALITY

Exposure Builds Over Time

Look at SMB cyber exposure over a single month, and the risk is already significant. But the real picture emerges over time.

As the observation window expands from one to three and then to six months, across millions of protected SMBs worldwide, the share of those encountering at least one live cyber threat rises steadily.



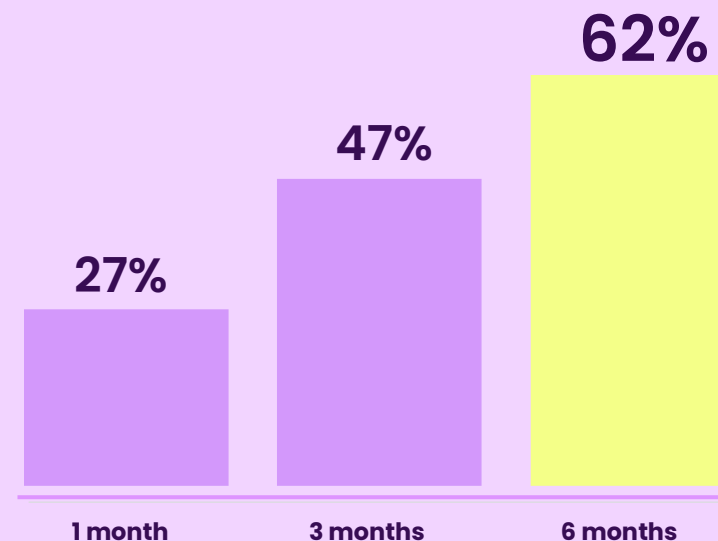
Within 6 months, exposure becomes more common than non-exposure.

The takeaway is simple:

Cyber exposure is not limited to a small group of particularly vulnerable SMBs. Given enough time, it becomes part of the reality of operating online.

Share of SMBs encountering a live threat

By observation window · 1, 3, and 6 months



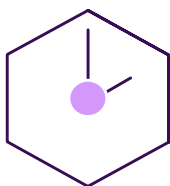
REALITY

Exposure Is Only the Beginning

Encountering a threat is one thing. What happens next reveals a more demanding reality.

For exposed SMBs, malicious activity is rarely an isolated event. Threats repeat, come from many sources, and keep evolving. The businesses in our analysis faced hundreds of blocked attempts across dozens of distinct malicious domains, while nearly half of the threats observed were new.

Together, these signals point to a different way of thinking about SMB cyber risk: exposure isn't a single event to recover from. It's a recurring condition that requires continuous protection.



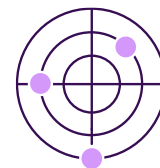
1.83

HOURS BETWEEN THREATS

On average, an exposed SMB faces a threat less than every two hours

SMB CYBER THREAT LANDSCAPE

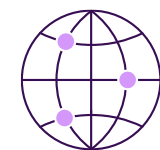
Attacks **Intensity**



393

Attack attempts per exposed SMB
Attackers don't stop after one try. They persist.

Attacks **Diversity**



For every 1000 exposed SMBs, we stop

549

different threats

Attacks **Novelty**



46%

Of blocked threats in a month are new
A rapidly changing threat landscape.

Source: Allot protection telemetry; millions of protected SMBs worldwide; monthly average for Q2 2026.

OPPORTUNITY

What Makes an SMB Attractive?

Attackers don't choose SMBs at random. They look for opportunities created by the normal way businesses operate. Our threat intelligence reveals five dimensions that they consistently exploit.



01

ACCESS

Accounts that unlock the business

Email, cloud platforms, and remote access give attackers a gateway to people, data, and critical systems.

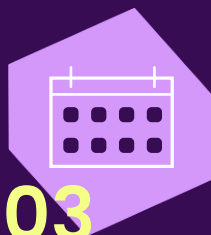


02

MONEY

Transactions worth intercepting

Payments, invoices, and refunds move money between businesses every day, creating attractive opportunities for fraud.



03

ROUTINE

Everyday activities attackers can predict

From tracking deliveries to downloading files, attackers exploit the digital habits that keep businesses running.



04

TRUST

Brands employees recognize

Trusted brands and familiar services lower suspicion and make malicious content far more convincing.



05

ACTION

The moment exposure turns into compromise

A click, login, or payment can turn exposure into compromise when the experience feels familiar enough to act on.

These factors often overlap and reinforce each other,

giving attackers multiple ways in and more chances to succeed.

The following sections explore each dimension in detail, backed by real threat intelligence and campaign examples.

Work no longer stops at the desk

Business activity has moved to mobile. So has the opportunity for attackers. Email, payments, cloud applications, messaging, file sharing, and authentication increasingly occur on smartphones as naturally as on computers.

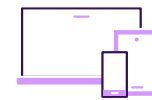
Employees can review an invoice, approve a login, or open a shared document from almost anywhere.

That convenience also changes the conditions in which threats are encountered. Smaller screens make URLs harder to inspect, links move easily between email, SMS, and messaging apps, and users often act quickly while away from their normal working environment.

The same opportunities attackers exploit across Access, Money, Trust, Routine, and Action increasingly extend beyond the desk, **following employees wherever business gets done.**

Source: Allot, "SMB Cybersecurity Concerns Q1 2026," survey conducted by Dynata, n=733 SMB decision-makers across 7 markets (USA, Canada, UK, Germany, Japan, South Korea, Indonesia), fieldwork March 2026

Share of SMBs using their mobile for day-to-day activities



35%

for accessing desktops and other remote work activities



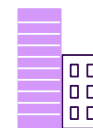
49%

for financial transactions



44%

for accessing work documents



58%

for business communication and work emails

The Language Behind the Threat

How human-readable threat domains help reveal what attackers reference, imitate, and ask users to do.

Not every malicious domain is designed to make sense to a person.

- Some use random or machine-generated combinations of characters.
- Others use recognizable language: words, brands, services, and activities that can provide clues about the threat behind them.

In the Allot Threat Intelligence Lab, we classify this second group as **human-readable threat domains** to identify recurring language around familiar business activities—from accessing accounts and making payments to opening documents and using trusted services.

Where available, we complemented these signals with captured threat sites and additional threat intelligence, allowing us to connect what appears in the domain with the experience presented to the user.

Throughout the next sections, these signals help us look beyond where threats are found and explore **what they are designed to resemble, communicate or encourage users to do.**

FROM

Malicious domains we block

WE IDENTIFY

Words · brands · activities · actions

WE GET

CTI insight into what attackers imitate and ask for

69% of threats stopped for SMB customers in Q2 2026 were human-readable



01 ACCESS

One account can open many doors

For a small business, an account is rarely just an account. A single set of credentials can provide access to email, documents, cloud applications, customer information, and conversations with colleagues, suppliers, and clients.

Rather than attacking each asset separately, stealing the right credentials can give them a legitimate-looking entry point to several parts of the business at once.

The value of a business account lies not in the password itself, but in everything that account can unlock

33%

Of the blocked events in human-readable threats were related to an **access-**related brand or keyword

	login-goooogle.com		
	amazon.signin-access.com		
	teams.ourlogin.co.uk		
	outlook.office365.com		

*Examples observed in threats blocked for SMB subscribers during Aug-26.

Top access-related brands observed

	Baidu	Digital Services		Facebook	Social Account
	Apple	Digital Identity		WhatsApp	Business Messaging
	Google	Workspace Access		Adobe	Creative Software
	Microsoft	Business Access		Github	Code Access

Most common access-related words

login signin account auth verification verify authentication

2fa reset password mail email user access credential

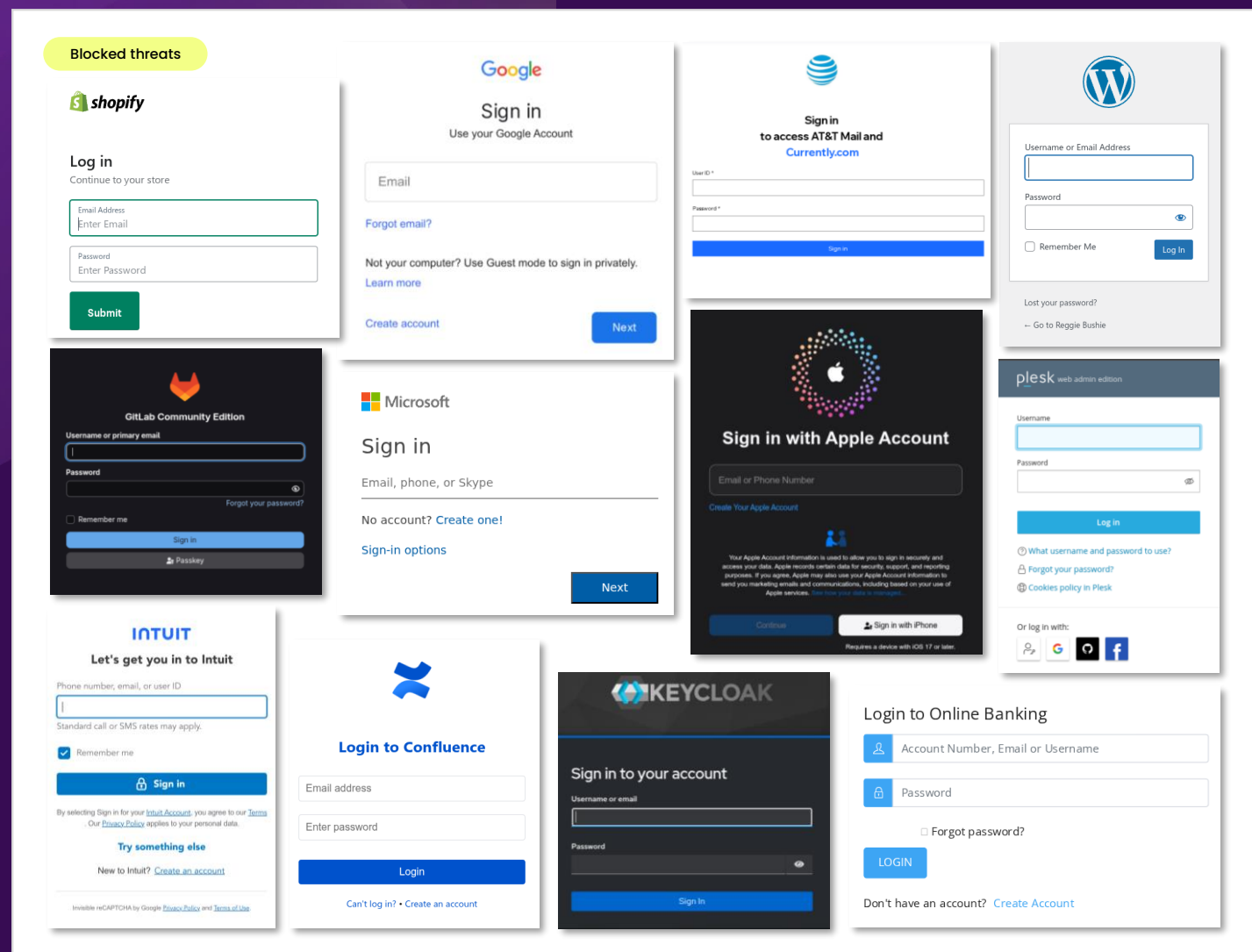


01 ACCESS

Multiple platforms.
The same objective.

From productivity suites to development and hosting platforms, attackers recreate the sign-in experiences employees use every day. Behind the different brands and services is a common objective: **convince a legitimate user to hand over access to valuable business resources.**

These examples show how broadly attackers can look for that opportunity wherever employees are accustomed to signing in.



Case Study

A Real Login. A Fake Way In.

Modern phishing can capture more than a password, even when the employee uses MFA.

1. WHAT HAPPENS



01

A convincing link — An employee clicks through to what looks like the normal Microsoft authentication service.



02

A copy in the middle — The page is fake. It quietly passes everything typed straight to the real Microsoft, so the login genuinely works.



03

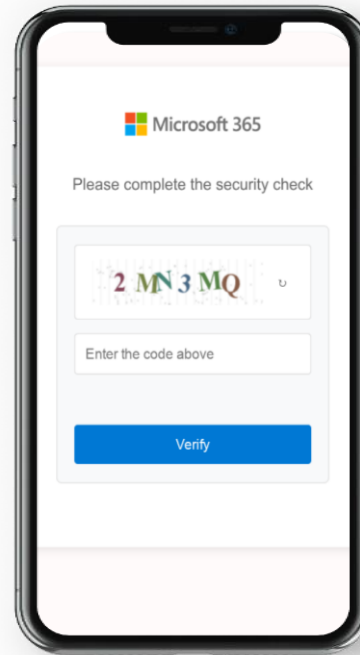
MFA can still succeed — The employee completes the usual verification step. Nothing appears to fail because the authentication request is being relayed to the legitimate service.



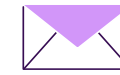
04

The attacker gains the session — Once authentication succeeds, the attacker can capture the active session and potentially access the account without asking the employee to sign in again.

2. WHAT THE EMPLOYEE SEES



3. WHAT THE ATTACKER GAINS



EMAILS

Business communications



CLOUD

Files and apps



IDENTITY

Connected services



TRUST

Business impersonation

NETWORK PROTECTION — When the network identifies and blocks the malicious destination, the chain can stop before the employee decides whether the login is real.

Adversary-in-the-Middle (AiTM) phishing: attacker-controlled infrastructure sits between the employee and the legitimate service, relays authentication in real time, and can capture the authenticated session, even when the user completes non-phishing-resistant MFA



02 Money

Attackers follow the flow of business value

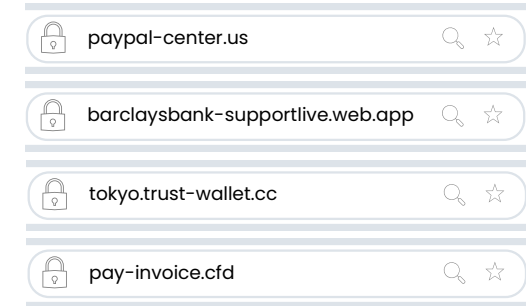
Money moves constantly through a small business: invoices are paid, suppliers receive transfers, employees make purchases, customers request refunds, and banking platforms are accessed throughout

Cybercriminals exploit these familiar financial processes because they create opportunities to intercept payments, capture financial information, or redirect transactions. Crucially, an attack doesn't always look like financial fraud. A convincing supplier request, an overdue invoice, or a routine payment notification can provide the context needed to make an unusual request appear legitimate.

For attackers, the opportunity lies in understanding how businesses normally move money and finding the right moment to insert themselves into that process.

17%

Of the human-readable threats reference a financial activity

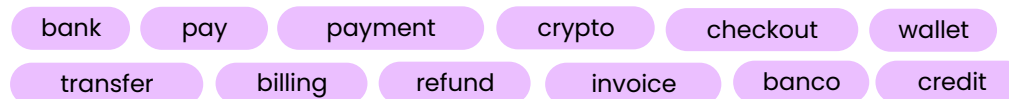


*Examples observed in threats blocked for SMB subscribers during Aug-26

Top money-related brands observed

	Coinbase	Crypto Assets		Apple	Digital Payments
	Barclays	Business Banking		Paypal	Online Payments
	Robinhood	Investments		Binance	Crypto Trading
	Amazon	Online Purchases		Bank of America	Business Banking

Most common money-related words





02 Money

Real Threats. Familiar financial moments.

These are real examples of threats that the protection service stopped. They imitate everyday financial interactions, from payments and banking to invoices and official services, using familiar contexts to make malicious requests feel legitimate.

Attackers don't just target money. They imitate the moments when businesses expect money, documents, and financial information to move.

Blocked threats

Get an Invoice

INVOICE

Heston Chamber of Commerce

Invoice No: 100-1000000

Invoice Date: January 1, 2025

Due Date: January 1, 2025

Amount Due: \$100.00

Service Subscription

Sub2API

Subscription to API Conversion Platform

Get Started

Subscription to API

Secure Password

Pay Me Now

Bank Login

Georgia Pacific Bank

Welcome

Please confirm you are not a Robot by verifying the auto-generated code below. This will enable you have access to Georgia Pacific Bank Online banking channels.

Enter code

Verify code

Payment Information Update

xfinity

Please update your payment information:

Name on card

Full name on card

Card number

XXXX XXXX

Expiration date

MM/YY

Security code

Address

APT, SUITE

State

City

Zip code

Pay Taxes

IRS Secure Document Portal

Initializing secure connection to retrieve your tax documents.

Establishing encrypted connection

Verifying your identity and credentials

Accessing secure tax document vault

Preparing your personalized tax statement

Billing Information

AT&T Wireless

FIRST NAME

LAST NAME

BILLING INFORMATION

BILLING ADDRESS

ZIP CODE

DATE OF BIRTH

CITY

STATE

EN / SN

CARD NUMBER

CVV

EXP DATE

PHONE NUMBER

AT&T PHONE PIN

Credit Card Payment

Card Number

5218531125183872

Expiration Date

03/30

Security Code (CVV)

378

Submit

Payroll Management

BOOKS & TAXES INC.

Payroll Portal - Secure Client Sign-In

Email Address

Password

Sign In

Payment Security Alert

Alert

A payment of \$289.00 USD was attempted using your Apple Pay ID from an unrecognized device.

Device: Desktop (Windows, Chrome)

IP Address: 186.121.144.101

Location: Santana, Boyaca, Colombia

If this isn't you, please report to Customer Support.

Tap to call Support: +1888-530-7545

Payment form

Online payment

\$50.00

Appointment Deposit

Notes

Add any details or notes about your purchase here.

Payment Method

Apple Pay

Google Pay

Credit or Debit Card

ACH Bank Transfer

Account Holder Name

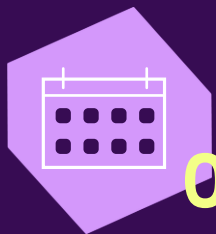
Account Type

Business Account

Personal Account

Routing Number

Account Number



03 ROUTINE

Attackers hide inside the working day

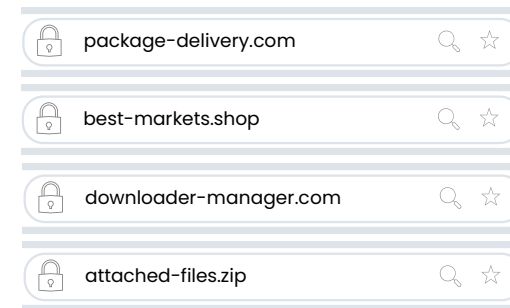
Many cyberattacks begin with something completely ordinary: tracking a delivery, opening a shared document, downloading a file, joining a meeting, reviewing a CV, or trying a new online tool.

These activities matter because they provide attackers with ready-made contexts in which interaction is expected. A document is supposed to be opened. A delivery link is supposed to be clicked. A meeting invitation is supposed to lead somewhere. Instead of asking users to do something obviously unusual, attackers increasingly position malicious activity inside behaviors employees already perform.

As businesses adopt more cloud services, digital workflows and online tools, the number of these everyday interactions continues to expand.

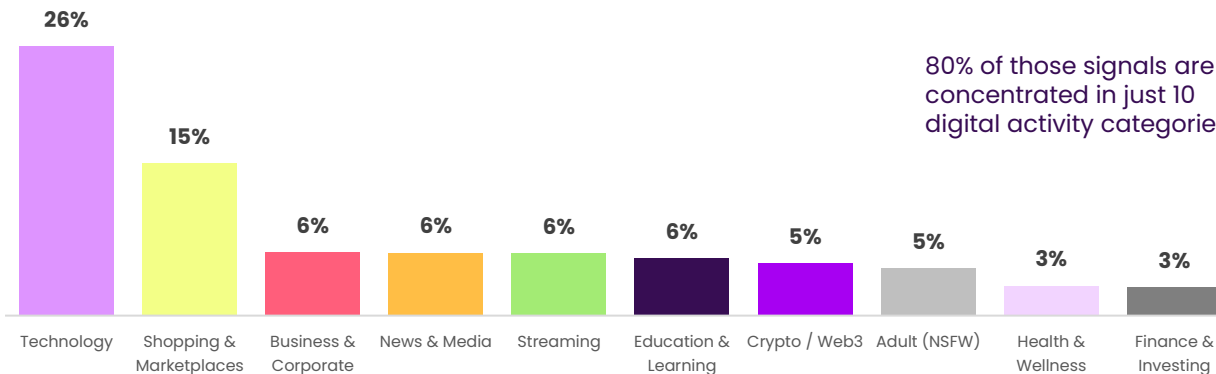
Over **60%**

of blocked domains were linked to an identifiable digital activity or market

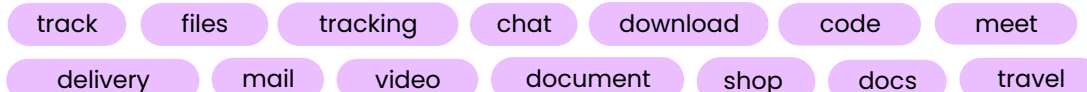


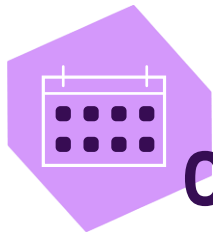
*Examples observed in threats blocked for SMB subscribers during Aug-26.

Top 10 Digital Activities Exploited by Cybercriminals



Most common routine-related words



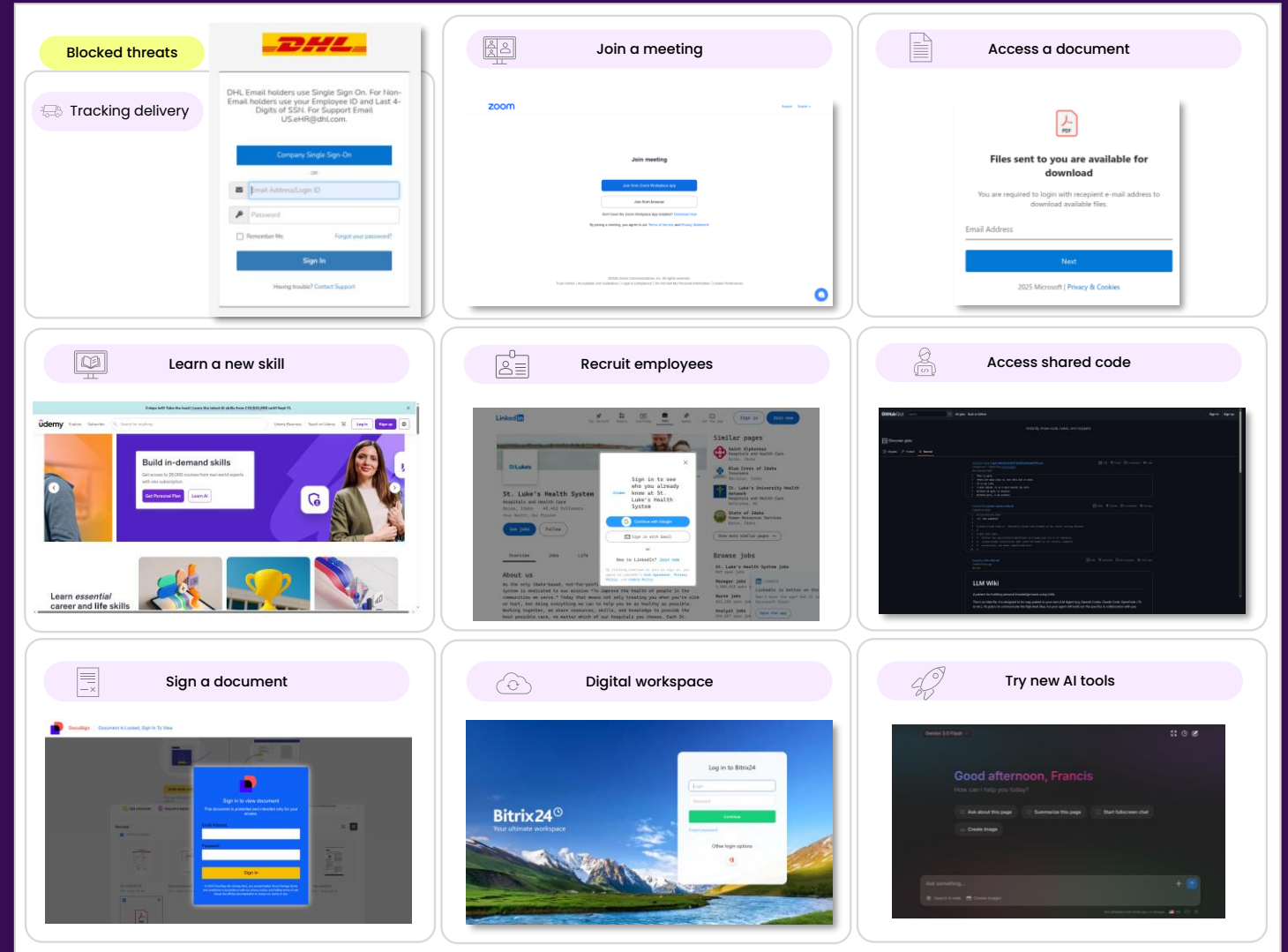


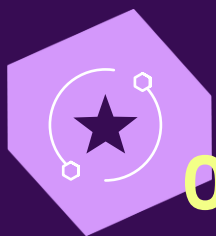
03 ROUTINE

Threats blend into the working day

A delivery to track. A call to join. A document to download. A business platform to access. These are ordinary digital tasks employees move through every day, and that familiarity gives attackers a natural place to hide.

Across services and activities, the same principle applies: the closer a threat resembles a normal part of the workday, the less reason there is to question it.





04 TRUST

Familiarity lowers the barrier

Successful deception rarely starts from zero. Attackers borrow credibility from organizations people already know: technology providers, banks, delivery companies, retailers, government services, and other familiar brands.

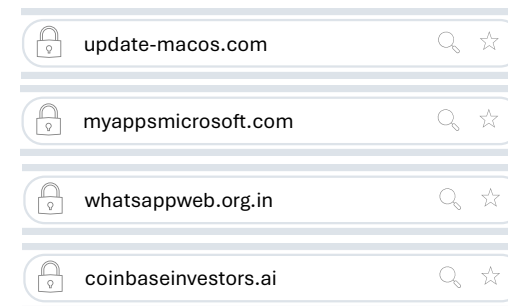
The imitation can extend well beyond a logo. Domain names may contain recognizable words, pages reproduce familiar layouts, and messages use language associated with security, support, or account management. Each element helps make an unfamiliar destination feel more legitimate.

For SMBs, where employees regularly interact with dozens of external platforms and providers, identifying these subtle differences can be particularly difficult. The attacker does not need to create trust from scratch; they only need to borrow enough of it to make the next step seem reasonable.



1 in 3

market-linked threats
uses a recognizable
brand to generate trust



*Access-related threats blocked for SMB subscribers during Aug-26

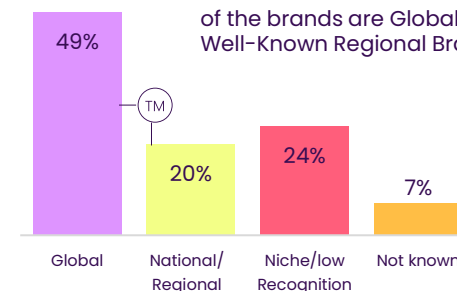
The familiar contexts behind brand references

Online Market for the **Top 20** Most Exploited Brands

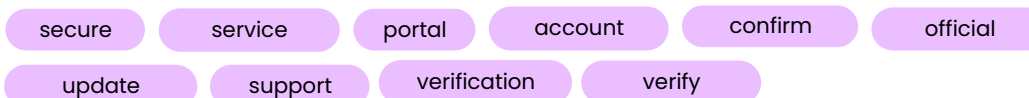
Technology	8	
Finance	4	
Crypto/Web3	3	
Social	3	
Streaming	1	
Shopping	1	

7 in 10

of the brands are Global or Well-Known Regional Brands



Most common trust-related words





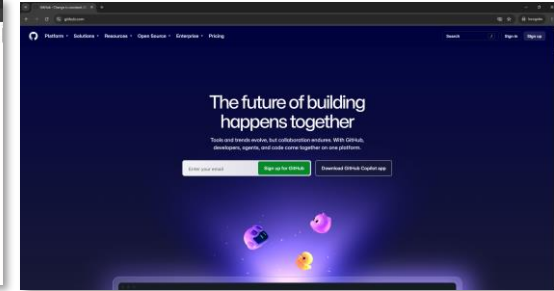
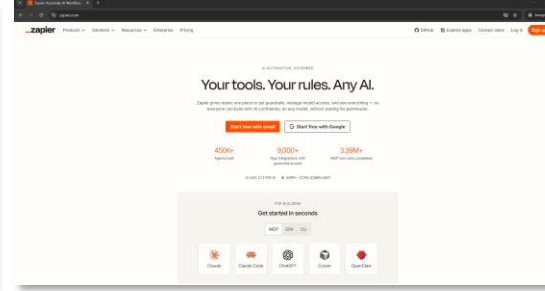
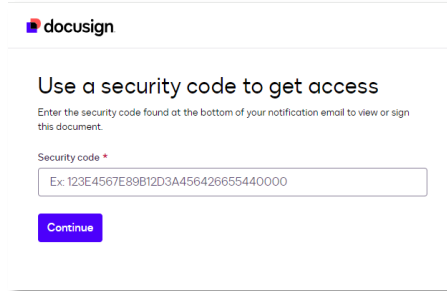
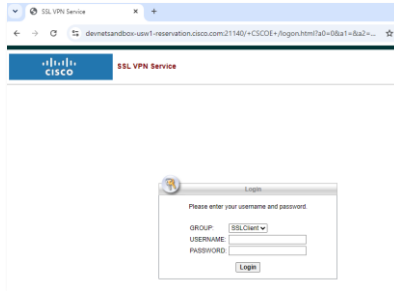
04 TRUST

The difference can be almost invisible

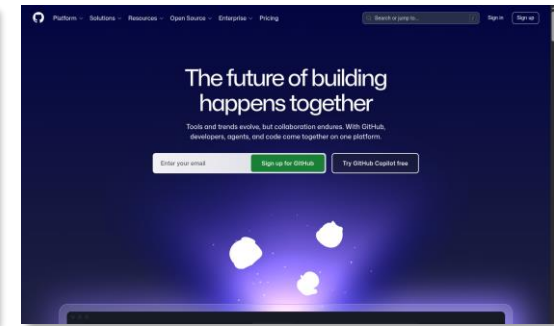
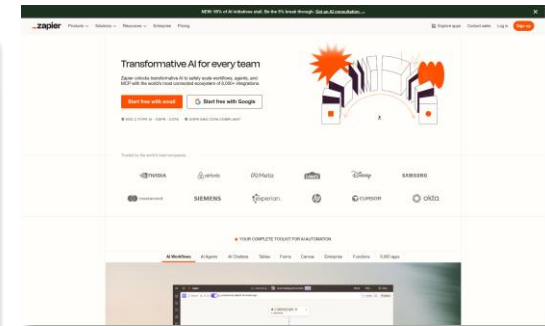
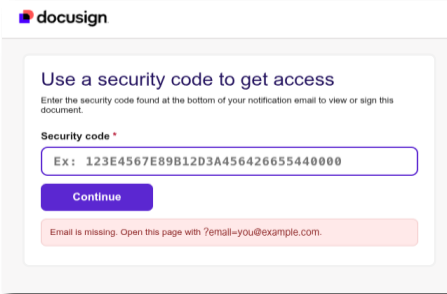
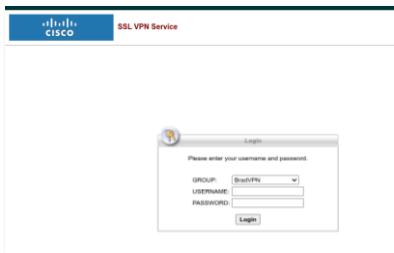
Attackers don't always create obviously fake experiences. They can reproduce the look, language, and functionality of trusted business services with remarkable accuracy. Side by side, the malicious and legitimate pages may appear virtually identical. From VPN access and developer platforms to automation tools and document-sharing services.

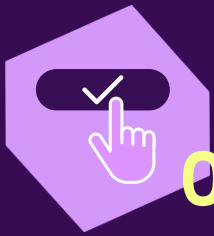
The challenge for employees is no longer simply recognizing a suspicious-looking website. It is identifying when something familiar is being presented from the wrong place.

Legitimate pages



Scam pages





05 ACTION

Every attack eventually asks for something

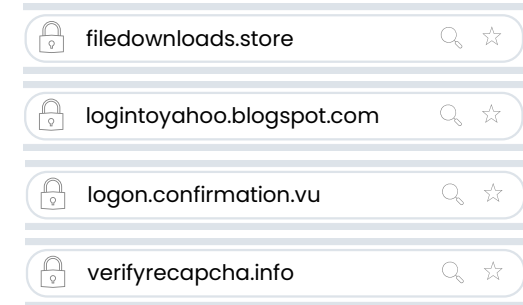
A convincing domain, a familiar brand, or a believable story has limited value until it persuades someone to act. That action may be as simple as signing in, opening a document, downloading a file, approving a request, making a payment, or granting permission.

This is the point where exposure can lead to compromise. Importantly, the requested action often feels entirely consistent with what came before it. Employees are not necessarily ignoring an obvious warning; they may simply be completing what seems like a normal task.

Understanding these actions provides a different view of the threat landscape. Rather than focusing only on what a malicious site is, it reveals what the attacker ultimately needs the user to do.

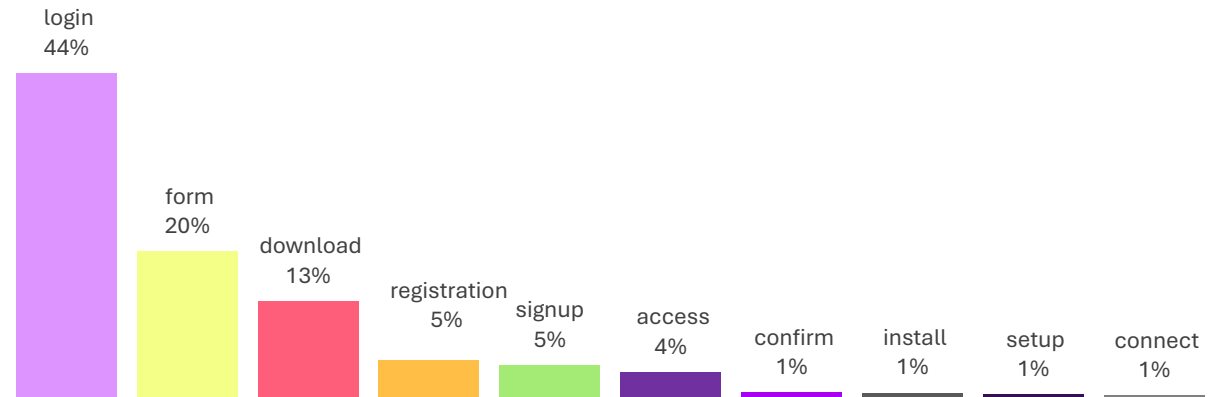
Over **15%**

of visible threat URLs contained language prompting a direct user action



*Examples observed in threats blocked for SMB subscribers during Aug-26.

Most common action signals





05 ACTION

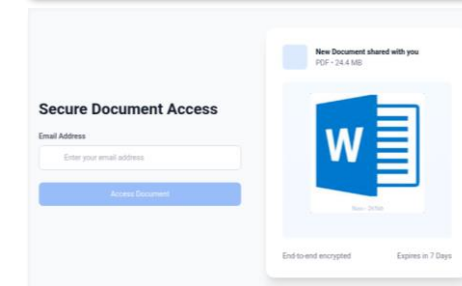
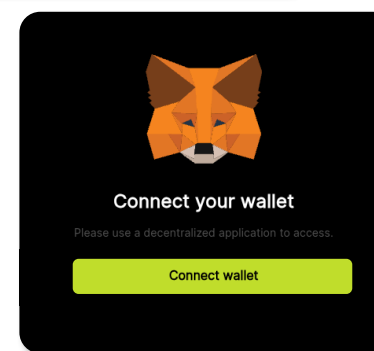
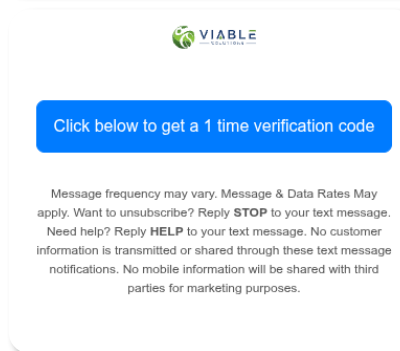
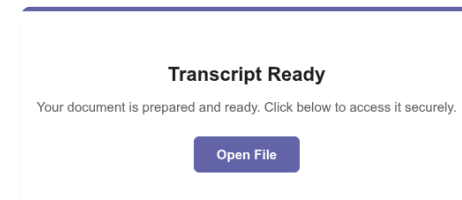
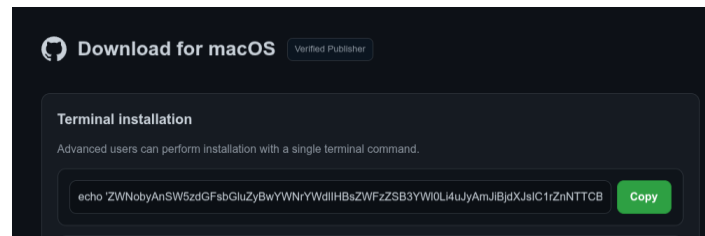
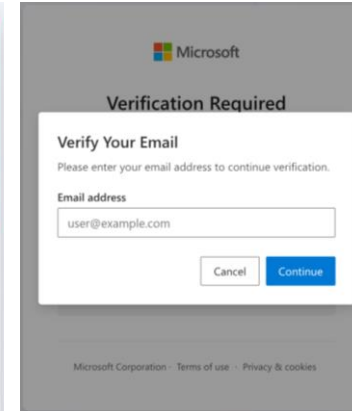
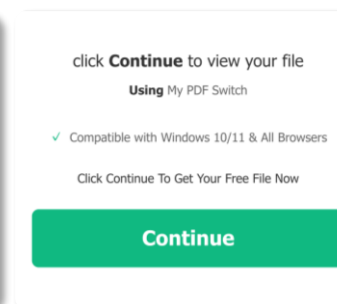
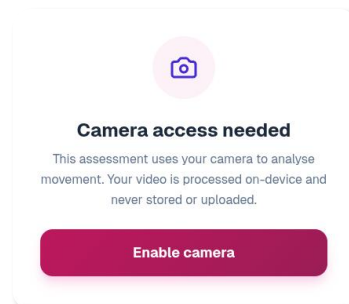
The deception only works if someone acts

Across very different threats, the final objective is remarkably similar: persuade the user to take one more step. Grant camera access. Enter a verification code. Open a document. Download a file. Update software. Connect an account.

The prompts may look helpful, necessary, or routine, but each is designed to turn a convincing experience into a user action.

The danger is often hidden behind a perfectly ordinary instruction: click, open, download, connect, or allow.

Blocked threats



Different opportunities.
Different disguises.

**One common challenge:
expecting every employee
to recognize the threat
before they act.**



ALLOT SOLUTION

Protection Without More Complexity

The patterns uncovered in this report share one important characteristic: many become visible at the network level. Malicious domains, deceptive destinations, suspicious infrastructure, and connections to known threats can often be identified before users have to decide whether something looks legitimate.

For small businesses, that matters. Effective cybersecurity cannot depend entirely on every employee recognizing every threat, or on every SMB having the resources to manage enterprise-grade security tools.

Network-based protection adds a security layer to something every connected business already uses: its connection.

Protection becomes less dependent on individual vigilance and easier to deliver consistently across the business.



CLOSURE

Main conclusions

Exposure is Normal

Within six months, threat exposure becomes more common than non-exposure among protected SMBs. Cyber exposure isn't limited to a small group of unusually vulnerable businesses.

Attackers Exploit Normal SMB Behavior

Accounts, payments, digital routines, familiar brands, and everyday actions create opportunities precisely because they are part of how businesses normally operate.

Protection Should Be Just as Embedded

If threats increasingly hide inside legitimate-looking interactions, protection cannot depend entirely on employees identifying what is fake. For SMBs, security works best when it is built into the way they connect.

The opportunity isn't to ask small businesses to become cybersecurity experts. It's to make being connected inherently safer.

About the analysis

This report combines anonymized protection telemetry from SMB customers with Cyber Threat Intelligence analysis conducted by the Allot Threat Intelligence Lab.

We used protection data to measure threat exposure, frequency, diversity, and novelty, and analyzed malicious domains, URLs, and captured threat pages to better understand how threats are presented to users.

For the lexical analysis, we identified human-readable threat domains: malicious domains or subdomains containing recognizable words, brands, services, or activities that can provide additional context about the threat. In Q2 2026, 69% of threats stopped for SMB customers met this definition.

We analyzed these signals across five dimensions: Access, Money, Routine, Trust, and Action, using combinations of keywords, brand references, digital activity categories, and, where available, captured threat pages. A single threat may contain signals relevant to more than one dimension; the five dimensions should therefore be understood as overlapping lenses into attacker opportunity, rather than mutually exclusive threat categories or attack stages.

How to read the findings

Percentages throughout the report use the analytical population relevant to each finding, for example, human-readable threats, market-linked threats or visible URLs. The analysis base is indicated alongside each KPI where relevant.

Brand references indicate that we identified a recognizable brand in the analyzed threat data. A brand reference does not by itself establish

impersonation or attacker intent. Where available, captured threat pages and additional threat intelligence provide further context and validation.

Examples shown throughout the report are real threats Allot protection service observed and blocked. They are included to illustrate how the patterns identified in the data can appear to users and should not be interpreted as representing the prevalence of a particular campaign or technique.

External References.

Case Study: Adversary-in-the-Middle (AiTM) phishing, p.11.

Independent research from Microsoft Threat Intelligence and SEKOIA.IO supports the technical explanation of AiTM phishing, documenting techniques in which attacker-controlled infrastructure proxies legitimate authentication flows and captures session information, potentially enabling account access despite non-phishing-resistant MFA.

www.microsoft.com/en-us/security/blog/2026/05/04/breaking-the-code-multi-stage-code-of-conduct-phishing-campaign-leads-to-aitm-token-compromise/

<https://www.sekoia.com/blog/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit>

About Allot

Allot (NASDAQ & TASE: ALLT) makes networks safer, smarter and more valuable. We make it our mission to help telcos and enterprises gain deep network insight, defend against evolving cyber threats, and unlock new value for their customers. At the core of Allot's solutions is Deep Network Intelligence, powered by advanced AI/ML technologies, enabling unmatched app-aware visibility, even when traffic is encrypted. The same intelligence that drives precise traffic control and Quality of Experience (QoE) optimization enables real-time protection against DDoS and cyber threats, and the market's only comprehensive network-native platform that turns security into revenue-generating services. Through these services, we enable telecom providers to offer accessible and affordable cybersecurity protection services to their consumer and small business customers who do not have the resources or expertise to protect themselves otherwise. Leveraging 30 years of advanced telecom and enterprise network expertise, Allot partners with more than 500 communication service providers, including many of the world's top 10 telcos, and over 1,000 enterprises. Recognized by top analysts and trusted globally, Allot is at the forefront of secure, intelligent network experiences.

