— TENTATIVE AND PRELIMINARY DRAFT —
FOR DISCUSSION PURPOSES ONLY

Phishing & Identity Exposure Assessment

February 2026

redw
Advisors & CPAs

AlmostEncrypted Technologies

Phishing & Identity Exposure Assessment

Table of Contents

AlmostEncrypted Technologies
Phishing & Identity Exposure Assessment

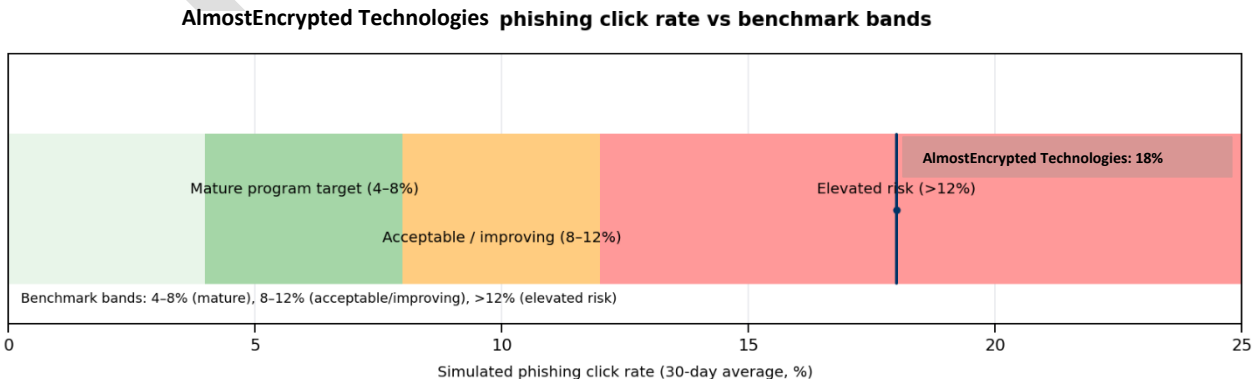
Executive Summary

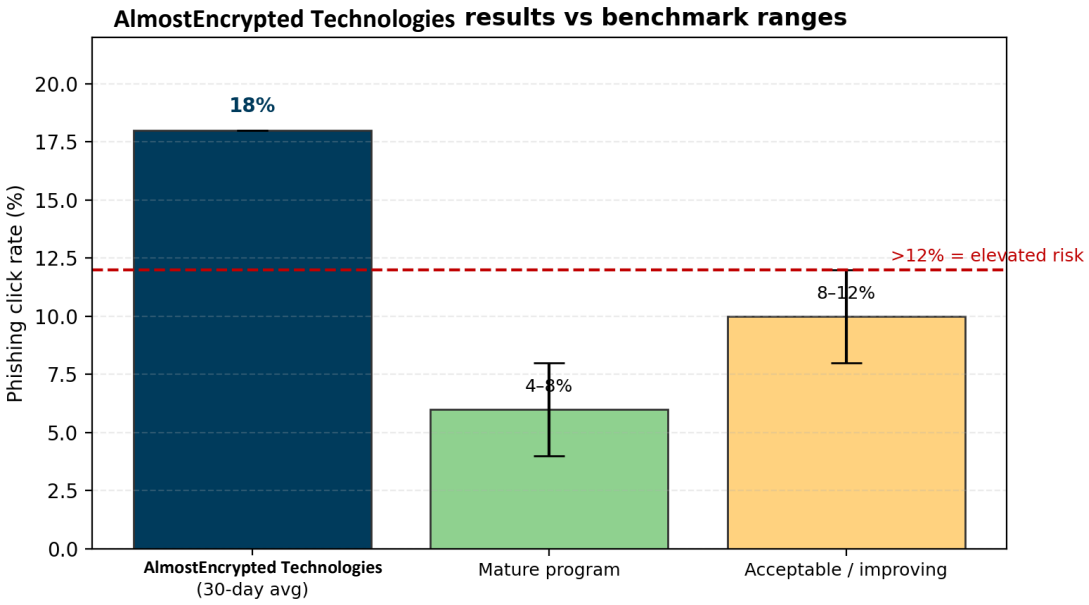
Over a 30-day assessment period, AlmostEncrypted Technologies participated in a simulated phishing and identity exposure assessment to establish a baseline view of employee vulnerability and exposure to email-based social-engineering as well as credential-based cyber risk, two of the leading drivers of financial fraud and operational disruption across the financial services sector.

The assessment covered 257 @almostencryptedtech.com staff and service account email addresses, with each email address receiving one simulated phishing email per week over a four-week period. The program leveraged 134 distinct campaign templates modeled on real-world attack vectors including shipping and notifications, current events, financial lures, and business email compromise (BEC) to measure realistic user exposure. A dark web scan of AlmostEncrypted Technologies email accounts was also performed to identify potential external credential exposure.

The assessment identified measurable, organization-wide human and identity exposure that exceeds industry benchmarks for similarly sized financial services and mortgage organizations. Specifically:

- A 30-day simulated phishing click rate of 18%, exceeding the industry benchmark threshold (>12%) associated with increased exposure to wire fraud and business email compromise.
- Post-click training completion of 31%, indicating a gap between user failure events and corrective learning.
- 24% of corporate email accounts associated with known credential breaches were identified, increasing the likelihood of account takeover, credential replay, and business email compromise.



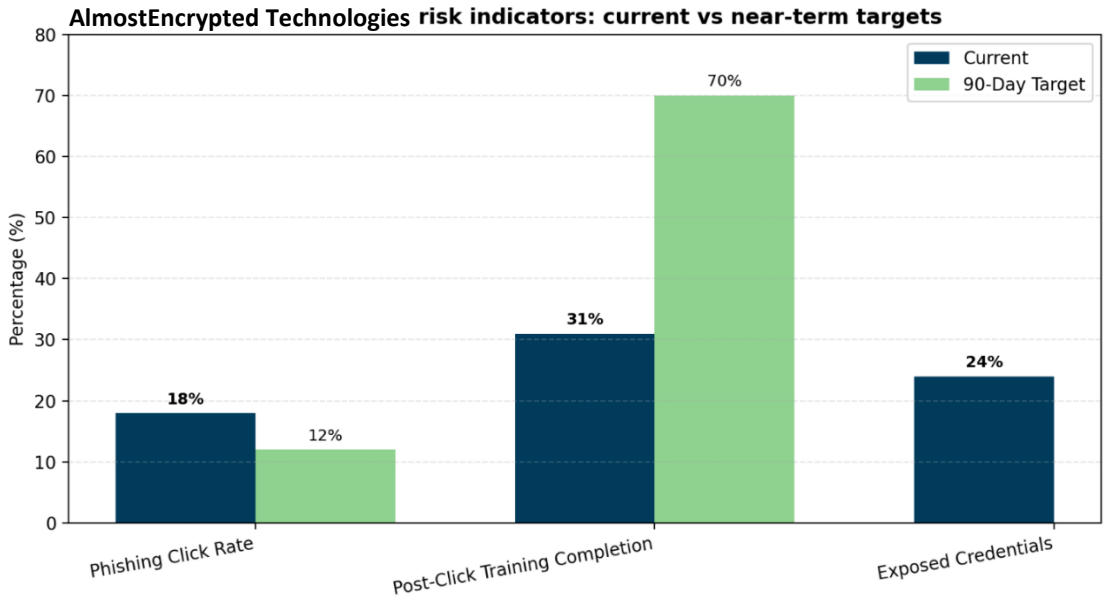


AlmostEncrypted Technologies' exposure is broad-based rather than concentrated. Most users who clicked phishing simulations did so only once, suggesting that risk is systemic and behavioral and not limited to a small number of high-risk individuals. The phishing templates most likely to succeed echoed real business processes such as internal document requests, invoicing, and third-party notifications which are consistent with current attacker behavior.

AlmostEncrypted Technologies' results are not unique and align across industry trends suggesting that social engineering and credential misuse remain dominant entry points for cyber incidents. Importantly, the findings represent a baseline, not a steady state. Experience across similar organizations demonstrates that measurable, sustained reduction in risk is achievable through focused management actions rather than technology changes alone.

Implementing a 30/60/90-day program prioritizes risk containment, behavioral correction, and executive visibility, with emphasis on:

- Reducing successful phishing interactions over time
- Closing the learning loop after user failure
- Improving early detection and response via phishing reporting
- Containing identity risk tied to exposed credentials
- Establishing trend-based reporting for leadership oversight



With disciplined execution and management accountability, phishing and identity-driven risk can be materially reduced into an acceptable range over the following quarters. This approach positions AlmostEncrypted Technolgies' cybersecurity awareness as a governable business risk, aligned with financial, operational, and reputational resilience objectives.

Key Risk Signals

For a benchmark financial services / mortgage company of ~260 employees running 4 phishing simulations in 30 days the target average click rate across the 30-day period*:

4%–8% (mature program)

8%–12% (acceptable / improving)

>12% (elevated risk for mortgage / wire-fraud exposure)

If this is a new or recently restarted program, an initial 30-day average of 8%–12% is common, but the trend should be sharply downward by campaign 3–4 (3-4 months).

The metrics below provide an overview of AlmostEncrypted Technologies' phishing and security awareness effectiveness for the assessment period. These results reflect user response rates, learning engagement, and program execution.

- Active employees in scope: 257
- Simulated phishing click rate (30 days): 18% (~48 employees)
- Post-click training completion: 31% (~14 completed; ~32 did not)
- Repeat clickers: only 5 employees clicked two separate campaigns; all other clicks were one-time events

* https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report

- Templates closely aligned with real business processes (e.g., DocuSign, Microsoft invoices, HR requests) consistently outperformed generic phishing lures in generating clicks.
- Corporate email credentials found in known breaches (darkweb monitoring): 24% (~64 AlmostEncrypted Technologies email accounts)

Systemic Context (Why This Is Not Unique)

Verizon's Data Breach Investigations Report (DBIR)[†] consistently shows that human behavior (social engineering) and credential misuse remain dominant pathways into organizations across industries. AlmostEncrypted Technologies' results align with these broader patterns: phishing succeeds quickly, and exposed credentials increase the likelihood of account takeover and downstream fraud.

Program Objectives

Cybersecurity awareness program objectives are designed to reduce the risk of material financial and operational impact by strengthening human defenses across high-risk business activities. Program benefits include:

- Reducing the likelihood of successful social engineering by improving employee recognition and behavior.
- Increasing early detection via high reporting rates and rapid response workflows.
- Containing identity risk by reducing the presence and usability of exposed corporate credentials.
- Improving resilience for high-velocity financial workflows typical of residential sales and mortgage origination (e.g., wire changes, invoice/payment updates, closing document requests).

Target Milestones (No Silver Bullet – Directional Improvement)

The following target milestones establish management-accountable benchmarks for tracking progress and sustaining measurable reductions in phishing risk.

Phishing click rate (simulations)

- Current: 18%
- 0–90 days target: ≤ 12%
- 3–6 months target: 8–10%
- 6–12 months target: 5–7% sustained

Training completion after failure (post-click)

- Current: 31%

[†] https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

- 0–90 days target: ≥ 70%
- 3–6 months target: ≥ 85%
- 6–12 months target: ≥ 90% sustained

Phishing reporting rate (once Report Phish is deployed)

- Current: Not yet measurable (no button deployed)
- 0–90 days target: Overall: 10–15% | Report-after-click: 8–12%
- 3–6 months target: Overall: 20–25% | Report-after-click: 12–15%
- 6–12 months target: Overall: 25–35% | Report-after-click: 15–20%

Darkweb Credential Password Reset

- Continue to monitor darkweb for exposure
- Reset passwords on a recurring frequency or as identified on darkweb
- Initiate policy prohibiting employees from using AlmostEncrypted Technologies' credentials outside of the work environment

Key Recommendations

Based on the results of AlmostEncrypted Technlogies' phishing simulations, the following recommendations are intended to address identified gaps, reinforce user behavior, and reduce the likelihood of successful phishing attacks.

- Assign simulations and training that exhibits real business processes to improve relevance and retention.
- Deploy phishing reporting and make reporting a primary success metric (in addition to click reduction).
- Close the learning loop by increasing post-click training completion and reducing repeat-click behavior.
- Treat exposed corporate credentials as a containment priority: reset, verify MFA, and monitor for suspicious sign-ins.
- Verify and continuously validate MFA and privileged access controls within Google Workspace.

* * * * *

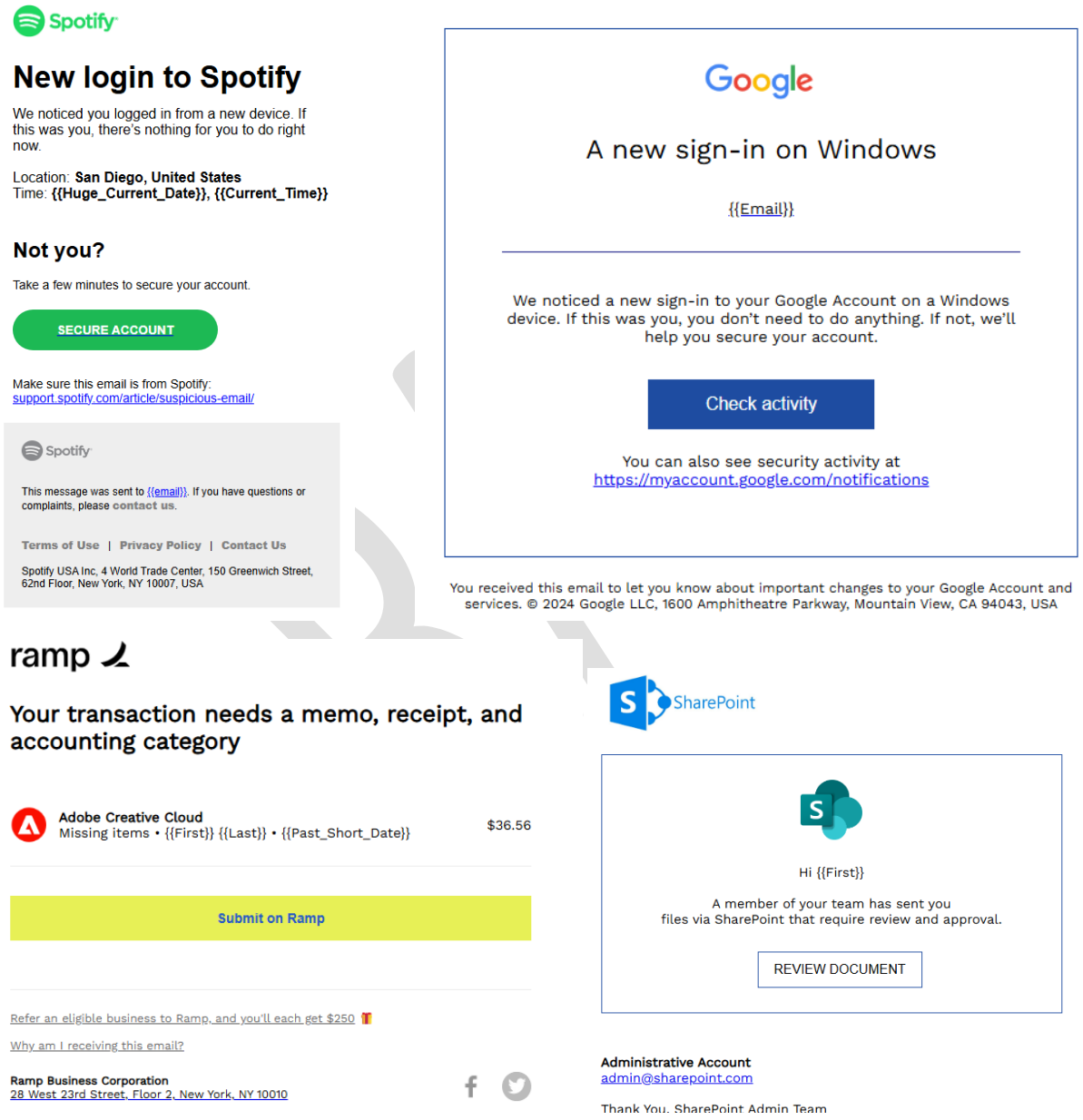
We received excellent cooperation and assistance from AlmostEncrypted Technologies in preparation for and during this assessment. We sincerely appreciate the courtesy extended to our personnel.

REDW LLC

Albuquerque, New Mexico
March 19, 2026

References

Example Phishing Templates – 134 different templates were utilized during the 4-week campaign including real-world attack vectors; Notification / Shipping, Current Events, Financial, and Business Email Compromise (BEC). Below is a small representation of templates that were clicked.



Hi {{First}},

It looks like you added an email address as an account alias. For security purposes the account number is encrypted.

- **Email Added:** {{Email}}

- **Account Number:** ********6475

NOTE: If you're not already logged in to this account, you will need to log in using an email address that has already been verified.

If you added this email address as an alias, use this link to verify:
https://account.com/Verify?aliasname={{Email}}&aliastype=Email&otc=*Df83UI!IuYxbTXf!!k1eGZB5g54wg5w4g54wty5Crl08oYHslrYC*!uOTHlzkOUAG!lrj7TEFwH2!D*6xNImA%24&mn={{Email}}&cxt=ALS

If you didn't make this request, use this link to cancel:
https://account.com/Remove?aliasname={{Email}}&aliastype=Email&otc=*Df83UI!IuYxbTXfvf54wtg54g5we6i8WXucVCrl08oYHslrYC*!uOTHlzkOUAG!lrj7TEFwH2!D*6xNImA%24&mn={{Email}}&cxt=ALS

Thanks,
The {{Company_Name}} security team

Microsoft

Sign in to view your Microsoft 365 Enterprise Premium invoice

Your Microsoft 365 Enterprise Premium invoice is now available in the Microsoft 365 admin center. Sign in to view it.

View your invoice >

If you've already paid, disregard this email.

If you're set up to pay by credit card, no action is required—we'll charge your card within 24 hours of the invoice date.

To review changes made to this subscription, go to the subscription history in the Microsoft 365 admin center.

Additional resources

- Learn more about your invoice
- Learn how to navigate your invoices
- Change the way you receive invoices
- Change your payment method
- Change your billing address

Account information

Organization name: {{Company}}
Domain: {{email}}
Subscription name: Microsoft 365 Enterprise Premium
Subscription expiration date: {{Future_Date}}

Did you find this email helpful YesNo

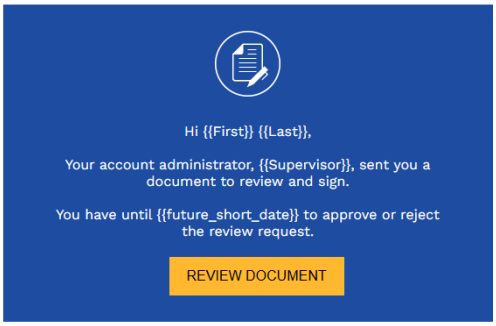
View or update your billing notification preferences.

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

DocuSign



Administrative Account
{{supervisor_email}}

Please see the DocuSign 2023 Updated Contract Terms.pdf

Thank You, Docusign Admin Team

Request a package hold to a FedEx location near you.

FedEx

Now that you're enrolled in FedEx Delivery Manager®, you can track your package and even make delivery changes on the go.

Package Details

Order Date: {{Current_Date}}
Name: {{First_Name}} {{Last_Name}}
Merchant: Cisco Tehcnologies
Delivery Date: {{Future_Date}}
Delivery Address: {{Office_Location}}

Track Package

This email has been sent to {{email}}. All future FedEx email communications will be sent to this address. You can unsubscribe or update your email profile at any time. To ensure this email is delivered to your inbox, please add fedex@{{action_url}} to your address book.

© 2024 FedEx, Attn: Review our privacy policy. All rights reserved.

AI-Powered Polymorphic Phishing - REDW utilized real-world attack vectors throughout the 30 day campaign to emulate the phishing emails generated now with AI technology. Below is an excerpt from KnowBe4 identifying this trend.

AI-Powered Polymorphic Phishing Is Changing The Threat Landscape For Good.

Our Threat Research team has observed polymorphic phishing campaigns being sent at a much larger scale than ever before. In 2024, at least one polymorphic feature was present in 76.4% of all phishing attacks and in 57.49% of commodity attacks (white noise phishing).

Polymorphic phishing campaigns consist of a series of almost identical emails which only differ by a small detail. These slightly altered attacks can be difficult to detect by systems that look out for 'known bad' (blocklisting of known fraudulent addresses and payloads), such as Microsoft's native security and secure email gateways (SEGs). Similarly, they can also be hard to remediate from inboxes across an organization using traditional email security technologies.