MEMCYCO

Digital Impersonation, Phishing and ATO Protection

Capability Maturity Scorecard

MEMCYCO

About this Scorecard

Security leaders know that airtight security requires a unified posture spanning people, process and technology. What's less obvious is how to adapt that posture in the face of modern phishing, ATO and digital impersonation threats that are now amplified by one-click website cloning kits and social engineering campaigns perfected with the help of AI.

This scorecard will help you benchmark your capability maturity for a modern context. It will also reveal whether your defenses are truly pre-emptive, predictive, and proactive, or just marketed that way.

Who should complete this?

CISOs, Heads of Fraud, and security leaders should use the scorecard to:

- **Pressure-test vendor claims:** Does your solution deliver on the 3 Ps with capabilities that are truly pre-emptive, predictive, and proactive?
- **Flag strategic gaps:** are there issues that deserve executive attention? seen but not reported by people on the ground
- **Align cross-functional teams:** are communication silos and bottlenecks creating excessive exposure to risk?

Instructions

Completing the scorecard should take just 10 – 15 minutes:

- **For each section,** select one answer that reflects your organization's most consistent state.
- **Even if more than one applies,** choose what's true most of the time. Each answer has an attributed score.
- **Finally, tally up your total** to see how you stack up and what you need to do to achieve full phishing, ATO and digital impersonation protection capability maturity.

MEMCYCO

Organizational Readiness: People and Process

How prepared are your customers to avoid brand impersonation scams, and how calibrated are your processes to respond to threats?

This section scores the maturity of your customer-facing education and internal fraud governance – two pillars that determine whether you can proactively prevent phishing-driven attacks before they escalate.

Select only one answer that represents the highest level of action you take in each area

A To what degree do you equip your customers to avoid scams?

☐ **1 point** – We provide basic fraud warnings across customer touchpoints.

☐ **2 points** – We proactively educate customers with alert and phishing examples.

☐ **3 points** – We run targeted fraud awareness campaigns with contextual in-app guidance.

☐ **4 points** – We deliver real-time messaging based on behavior, but not user-specific.

☐ **5 points** – We personalize alerts and risk cues based on live user and session risk data.

B How fast can your fraud governance processes detect and respond to threats?

☐ **1 point –** We have informal fraud response processes, but no standardized workflows.

☐ **2 points –** We respond manually to fraud feeds or alerts without formal prioritization.

☐ **3 points –** We use predefined workflows to mitigate phishing-driven ATO.

☐ **4 points –** We run semi-automated decisioning but don't alert customers in real time.

☐ **5 points** – We use full automation with real-time fraud prevention measures and customer alerts.

MEMCYCO

Technology Readiness: Being Truly Pre-emptive, Predictive, and Proactive

Does your phishing, ATO and digital impersonation protection solution live up to vendor claims of being pre-emptive, predictive, and proactive?

This section challenges whether your technical defenses stack up versus the marketing claims. For each question stack provide analyst definitions of what truly qualifies as pre-emptive, predictive and proactive security.

Analyst benchmark:

Pre-emptive security

"Proactively deflecting and defending against cyber threats by identifying and mitigating likely attack vectors and related vulnerabilities and exposures before they can be exploited." [1]

Select only one answer that represents the highest level of action you take

C Pre-emptive – Can you detect and deflect

☐ **1 point** – No, rely on external feeds to identify phishing domains but only after they go live.

☐ **2 points** – Our solution monitors domain registrations to detect suspicious activity before phishing pages go live, but doesn't intervene.

☐ **3 points** – Our solution detects early-stage user interaction with phishing sites (e.g., clicked links), but doesn't intervene.

☐ **4 points** – Our solution provides real-time browser-based alerts or redirects to prevent customers exposing credentials.

☐ **5 points** – Our solution automatically takes down phishing pages or blocks user engagement in real time.

[1] ***Gartner®**, Emerging Tech: Top Challenges in Preemptive Cyber Defense, Lawrence Pingree, Isy Bangurah, Luis Castillo, Walker Black, 22 October 2024*

Analyst benchmark:

Predictive security

"Leveraging telemetry data, artificial intelligence (AI), and machine learning to detect threats early and provide actionable insights that improve incident response" [2]

Select only one answer that represents the highest level of action you take

D Predictive – To what degree can you predict which accounts will be targeted for ATO?

☐ **1 point** – No. We use general risk scoring or historical trends to make loose predictions.

☐ **2 points** – No. use basic threat feeds and trend analysis for scenario forecasting.

☐ **3 points** – We monitor phishing infrastructure and campaign activity to flag users at heightened risk of targeting.

☐ **4 points** – We detect early signs of credential compromise tied to specific users or login attempts.

☐ **5 points** – We analyze attacker behavior and infrastructure in real time to accurately predict which accounts will be targeted.

Analyst benchmark:

Proactive security

"A strategic approach to controlling security posture and reducing breaches through strong visibility, prioritization, and countermeasures." [3]

E Proactive – Can you see threats as they're emerging and deploy countermeasures before impact?

☐ **1 point** – No, we rely on post-incident alerts and/or post-mortem forensic investigations.

☐ **2 points** – No, our solution flags suspicious behavior or anomalies but doesn't counter.

☐ **3 points** – Our solution renders stolen credentials useless during active attempts.

☐ **4 points** – Our solution uses decoys and false signals to deceive attackers and protect legitimate users and accounts.

☐ **5 points** – We use real-time measures, proactively blocking untrusted devices to stop fraud progression, and prevent ATO.

[2] *Gartner®, Emerging Tech: Top Use Cases in Preemptive Cyber Defense, Lawrence Pingree, Carl Manion, 13 August 2024.*
[3] *Forrester®, My Prediction For The 2024 RSA Conference: Proactive Security Will Dominate Use Cases, Erik Nost, May 1 2024*

MEMCYCO

Scoring Breakdown: What Your Score Means

0–6 points → Minimal protection:
Your defenses are mostly reactive and you're mostly relying on luck, not layered protection. Urgent investment is needed in both process and tooling to avoid damaging breaches.

7–12 points → Partial maturity:
You've got tools and workflows in place, but attackers will likely move faster than you can respond. Time-to-intervention is still too slow.

13–18 points → Solid foundation:
You've invested in the right areas but still lack real-time visibility and pre-emptive defenses. Improvement could significantly reduce costs.

19–25 Points → Full maturity:
You're ahead of the curve. Aim to evolve further by operationalizing agility across people, process, and tech to stay resilient at scale.

Are you buying protection or promises?

You've got your score. Now ask yourself, do your defenses live up to the promises your vendors sold you?

1. Did you buy a solution that claims to be predictive, but only analyzes historical data?
2. Are your defenses pre-emptive in theory, but reactive in practice?
3. Do you hear "proactive" a lot, but still wait for alerts after damage?

If you answered 'yes' to any of these three questions, it's time for a Memcyco demo.

From 'detection' to 'disruption'

Reassess your vendor claims through the lens of operational impact. Does your solution expose and treat the root cause of ATO fraud, or just the symptoms?

Benchmark internal and vendor-led defenses against a framework of predictive, pre-emptive, and proactive intervention.

For enterprises identifying gaps, the priority is to shift from detection to disruption before user exposure. Memcyco's agentless solution enables that shift, operationalizing real-time response to digital impersonation, phishing and customer ATO attacks at scale.

About Memcyco

ACHIEVE >10X ROI FROM THE 1st YEAR

Proactive, real-time protection against phishing, ATO, and digital impersonation

Memcyco predicts ATO, phishing and digital impersonation attacks, protecting companies and their customers from digital fraud. Memcyco is the only solution that provides real-time victim identification, pre-emptive ATO prevention, and credential deception technology, offering unmatched visibility into evolving threats.

SOLUTION OVERVIEW

Memcyco gives us pre-emptive foresight of ATOs in the making with real-time visibility into phishing attacks and brand scams before they hit our customers. Even if customers fall for scams, Memcyco dismantles card data and credential theft attempts at the moment of impact.

– Oren K, CEO
Mid-Market Organization (1,000-5,000 emp.)

The only solution that

- ✓ Identifies individual victims in real time
- ✓ Predicts & preempts ATO incidents
- ✓ Swaps real data with decoy data
- ✓ Proactively deceives threat actors
- ✓ Mitigates Man-in-the-Middle attacks

2025 GLOBAL AWARDS GOLD WINNER CYBERSECURITY

GLOBAL RECOGNITION AWARD 2024

The Cyber150 List 2024

Reveal attacks in granular detail, like never before

Memcyco delivers unprecedented real-time attack visibility of attacks, attackers, individual victims, fake sites, compromised user credentials and card data, suspicious devices, at-risk users, and other attack identifiers.