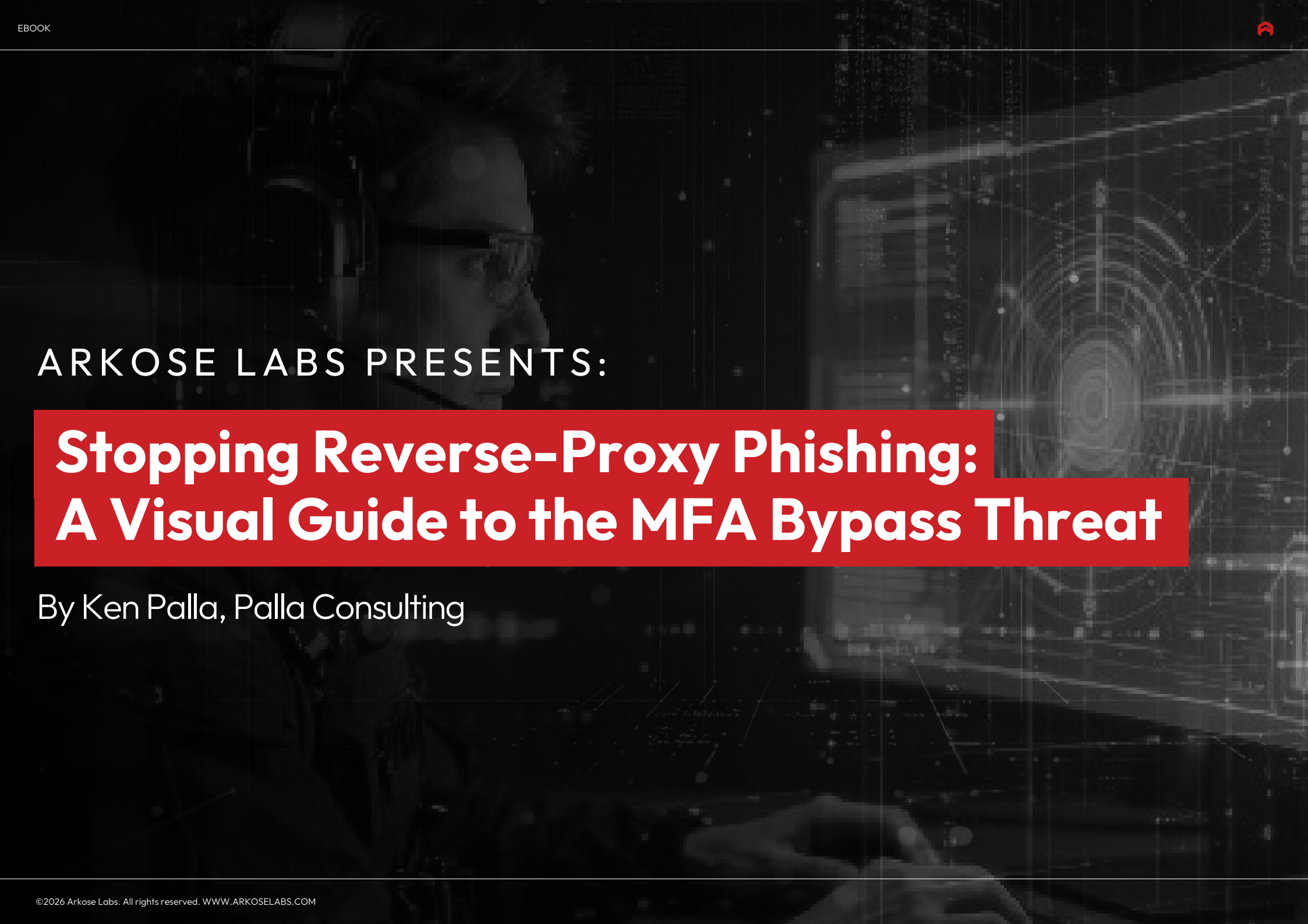


ARKOSE LABS PRESENTS:

Stopping Reverse-Proxy Phishing: A Visual Guide to the MFA Bypass Threat

By Ken Palla, Palla Consulting

Phishing Has Never Been More Dangerous

By the Numbers[1]

3.4 BILLION
Phishing emails sent every single day

31%
Of all attacks target financial services

1 MILLION
Phishing attacks in Q1 2025 alone

The Barrier to Entry Has Dropped to Zero

With phishing kits and GenAI, anyone can become a phisher. Technical skills? No longer required. Just $50 and you're in business.

$

Before GenAI

- Required technical expertise
- Time-consuming and expensive
- Limited scale

$$$

After GenAI

- $50 for phishing kit subscription
- 30 minutes to launch campaign
- Unlimited scale with automation

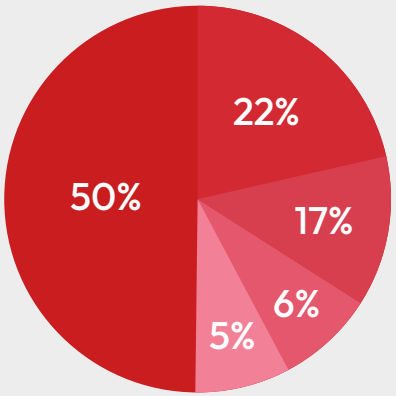
[1] https://apwg.org/trendsreports

Why Phishing Still Works

Our Brain Works Against Us [2]

We have two thinking modes—and phishers exploit the faster one.
System 1: Fast, emotional, react first
System 2: Slow, logical, think it through.

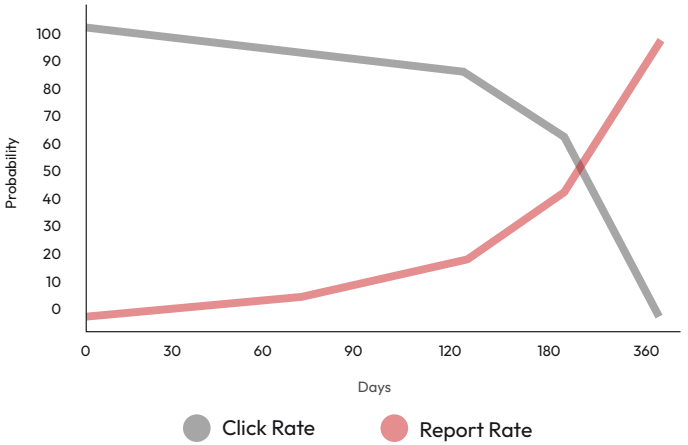
Phishing works because it triggers System 1—we react before we think.



Why We Click

- Mimicry
- Don't Remember
- Rushing
- Curiosity
- Fear of Consequences

Training Wears Off Quickly [3]



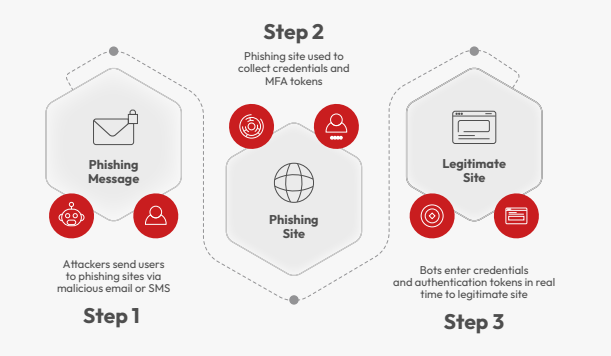
3.5% click rate after training-9.5% after 60 days -Keeps rising after 2 months

We need technology that doesn't rely on perfect human judgment.

[2] https://www.beauceronsecurity.com/blog/new-research-shows-why-employees-click-on-phishing-e-mails
[3] https://www.beauceronsecurity.com/blog/new-research-shows-why-employees-click-on-phishing-e-mails

How Phishing Works

The Attack Flow



STEP 1: Phishing Message Email or SMS with urgent message and link

STEP 2: Phishing Site Fake login page collects credentials and MFA tokens

STEP 3: Target Site Attacker uses stolen credentials to access real account

The Email Looks Legitimate

Malwarebytes provided a sample email involving PayPal.[4]

The "From" address? Easily spoofed with special software

The design? Cloned with GenAI in minutes

The urgency? Carefully crafted to trigger System 1 thinking

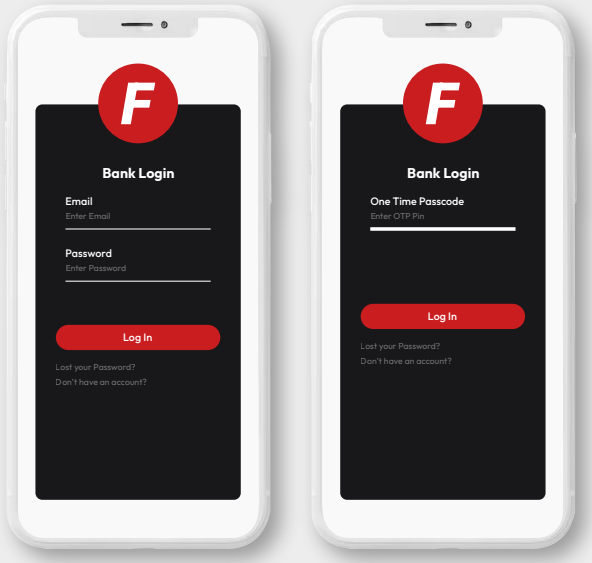
None

From: service@paypal.com

Subject: Set up your account profile

"New Profile Charge: We have detected a new payment Profile with a charge of $910.45 USD at Kraken.com..."

The Login Page Is Identical



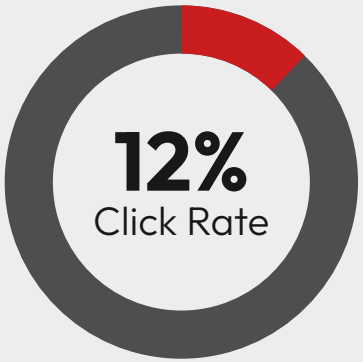
Because it's using **reverse proxy technology,** the phishing site looks exactly like the real thing—because it **IS** the real thing, just intercepted.

[4] https://www.malwarebytes.com/blog/news/2025/09/paypal-users-targeted-in-account-profile-scam

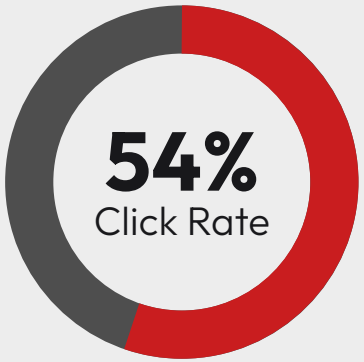
AI Makes It Worse

AI-Targeted Phishing Is Devastating[5]

Traditional phishing:



AI-generated spear phishing:



AI creates perfectly targeted, personalized emails at unlimited scale.

What AI Enables

- Perfect emails in any language
- 10,000+ personalized emails instantly
- Clone websites in seconds
- Entire campaigns run autonomously

Real Impact

"BMO is now blocking 150,000-200,000 phishing emails per month. We're convinced criminals are using AI."

— Lawrence Zelvin, BMO Financial Group[6]

[5] https://www.malwarebytes.com/blog/news/2025/01/ai-supported-spear-phishing-fools-more-than-50-of-targets
[6] https://www.reuters.com/investigates/special-report/ai-chatbots-cyber/

Why Your MFA Isn't Working

	Traditional Phishing	Reverse Proxy Phishing
Method	Static fake website	Real-time interception via a proxy
Target	Credentials	Credentials, MFA, session tokens
Bypass MFA	Rarely possible	Designed to bypass MFA
User Experience	Static fake site separate from legitimate site	Appears identical to the legitimate site as the proxy fetches the legitimate site's content in real time
Detection Difficulty	Easier to detect	Very difficult to detect as the legitimate site is involved

Here's What Happens

1. You enter your password → Captured by proxy
2. You enter your OTP code → Captured in real-time
3. Proxy forwards to real site → Login succeeds
4. You see your real account → Everything looks normal
5. Attacker has your session cookie → They're now logged in as you

What Gets Compromised

- Username and password
- One-time passcode (captured live)
- Session cookie (ongoing access)
- All your device fingerprinting passes through normally

The attacker looks exactly like you to the bank's security systems.

What Actually Stops Reverse Proxy Phishing: Real-Time Detection

Arkose Titan is a unified fraud prevention platform that stops automated attacks and human-driven fraud across your entire digital environment. By combining real-time risk assessment with economic deterrence, Arkose Titan makes attacks too expensive and time-consuming for fraudsters to sustain.

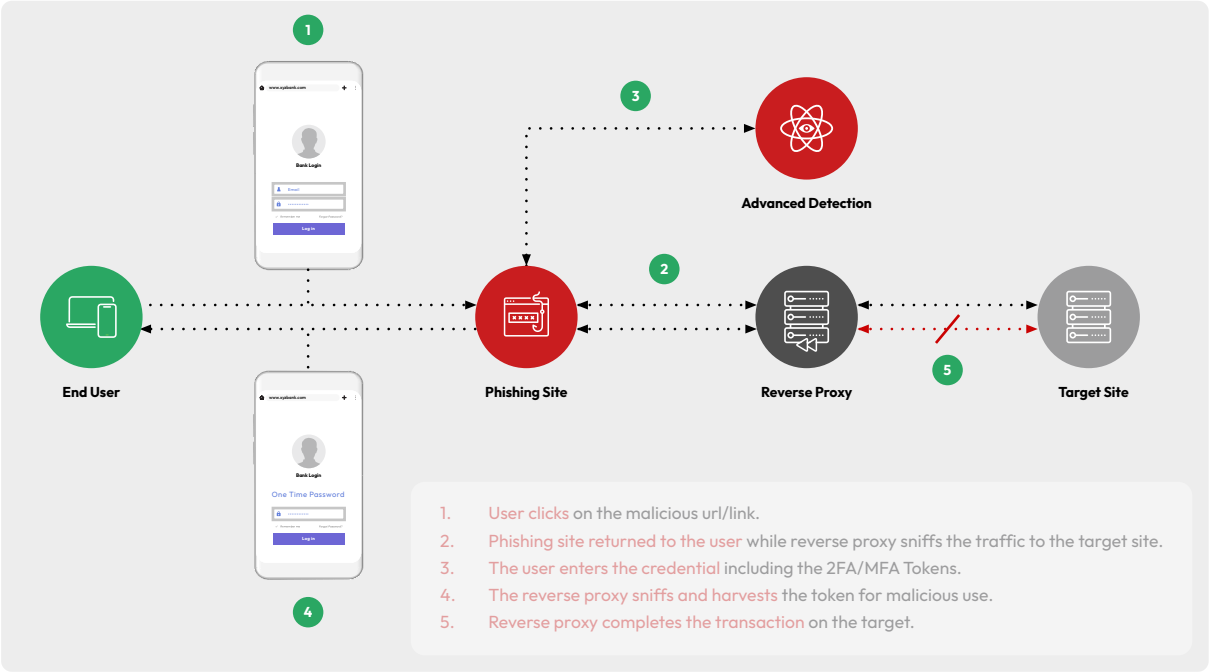
Arkose Phishing Protection, a key component of Arkose Titan, offers behavioral detection and cryptographic verification that identifies reverse-proxy phishing attempts in real time.

Token verification - Legitimate sites have cryptographic tokens that reverse proxies can't replicate

225+ risk signals - Analyzes device, traffic patterns and behavior across the session

Real-time response - Blocks suspicious attempts immediately or captures for analysis

Continuous learning - Global intelligence network shares new attack patterns across all customers



Take Action Today

Three Steps You Can Take This Week

1. Evaluate Real-Time Phishing Protection
Traditional blacklists can't keep up with modern reverse proxy attacks. You need behavioral detection, cryptographic verification and real-time response capabilities that identify attacks in seconds.

2. Audit Your Current MFA
Are you still relying on SMS or email codes? These are vulnerable to reverse-proxy interception. Consider your upgrade path to phishing-resistant authentication.

3. Review Your Email Security
Check your DMARC status and browser protections to add defense-in-depth layers that complement real-time detection.

Want the Complete Picture? This e-book is focused on the reverse proxy phishing threat and real-time detection solutions. For comprehensive recommendations on phishing-resistant MFA options, email security controls, device fingerprinting and building a complete defense strategy, read Ken Palla's full technical whitepaper.

Contact & Resources

Scan to read the full technical whitepaper

Get the Full Whitepaper

Author: Ken Palla, Palla Consulting

Since 2005, Ken has been in Online Security. He was a Director at MUFG Union Bank, retiring in early 2019. He helped shape the initial responses to the U.S. 2005 and 2011 FFIEC Regulatory Guidance to improve online security for US Banks. He is an early adopter and has selected and implemented a number of online security products. In 2019, he received the Legends of Fraud Award at the 3rd annual FraudCON conference in Israel. He is currently consulting to banks and to online security vendors.

Special thanks to:

- Ryan Powell, CIBC
- Mitch Davies, Arkose Labs Senior Data Scientist
- Arkose Labs Cyber Threat Intelligence Research (ACTIR) team

Talk to an Expert

Arkose Labs is the leading proactive fraud deterrence provider purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. © 2026 Arkose Labs.