ARKOSE LABS

How AiTM Reverse Proxy Phishing Attacks Sidestep MFA Security

An attacker sets up an AiTM (Adversary-in-the-Middle) phishing site and reverse proxy server, then sends a phishing email.

Your Favorite Company

Dear Customer,

I hope this message finds you well. We are reaching out to you from Your Favorite Company because our monitoring systems have detected some unusual activity on your account that we believe could be unauthorized.

Immediate Action Required

To ensure the security of our account, we urgently need you to confirm your identity at our official website at yourfavoritecompanyy.com. Thank you for your immediate attention to this matter!

—Customer Security Team

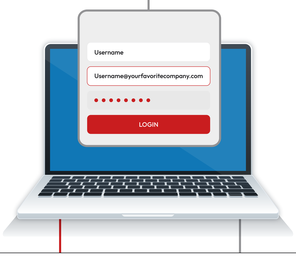
Does the end consumer detect the phishing attempt?

YES

The consumer ignores or reports the phishing email.

NO

The consumer clicks the link in the email and enters their credentials into the phishing site.



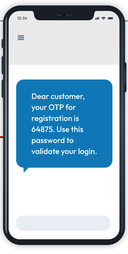
Does the company use AiTM phishing detection software?

YES

A warning message alerts the consumer to the scam.

NO

The reverse proxy server captures the consumer's credentials, forwarding them to the legitimate company site. The company uses MFA and sends an OTP to the consumer.



The consumer enters the OTP into the phishing site.

Your Favorite Company Login

One-time Passcode

Enter OTP

LOGIN

Lost your password?
Don't have an account?

MFA

The reverse proxy server forwards the MFA token to the legitimate website. The attacker logs into the consumer's account.

ATTACK FAILS

ATTACK SUCCEEDS

The attacker can now drain the account, apply for loans, harvest personal information or carry out other damaging activities.

Attackers are bypassing MFA — and standard defenses aren't enough. Arkose Titan detects, alerts and blocks dangerous AiTM reverse proxy phishing campaigns before they can succeed.

LEARN MORE >

The world's leading organizations, including two of the top three banks and the largest tech enterprises, trust Arkose Labs to fight online fraud and keep users safe in digital transactions. Our patented AI-powered platform detects, traps, and neutralizes bots and bad actors before they can make an impact, without sacrificing the experience of genuine users, and tracks and shares real time, global threat intelligence with our customers. No one else is more proven at scale, provides more proactive support for internal security teams, or outperforms Arkose Labs in sabotaging attackers' ROI. Our verified customer reviews on G2 reflect the value we add reducing the volume, internal cost, and impact of bot attacks and online fraud. Based in San Mateo, CA, Arkose Labs operates worldwide with offices in Asia, Australia, Central America, EMEA and South America.