MEMCYCO

Solution Brief

Customer ATO & Fraud Protection

Detect website impersonation attacks in real-time, stop ATO and other scams, protect customers, and get complete attack visibility.

SITE IMPERSONATION ATO
IT ONLY TAKES A FEW SECONDS

1. Customer receives fake comms they think is from you
2. They click a rogue link to a fake version of your site
3. In seconds, they've shared their credentials with scammers

SCAM EVOLVES INTO FULL-SCALE ATO
And it might not stop there. Ransomware attacks can also start with site impersonation. Yet such attacks may never be traced back to website impersonation as a technique-of-origin

All the while, business and customer are unaware and unprotected. You may never know a website impersonation incident even took place.

MEMCYCO PUTS A SWIFT END TO THAT

Memcyco's agentless solution protects you and customers up front, with full visibility of the attack source, timing and the customers attacked.

MEMCYCO'S SECRET SAUCE

Memcyco's breakthrough capabilities give you the upper hand against some of the most devastating cyber threats, like ATO and ransomware attacks, that are increasingly perpetrated using website impersonation.

WHAT IF YOU HAD

- **A tamper-proof sensor** in your site code, raising the alarm when customers click links to websites impersonating yours.
- **Or the ability to ID user devices** as 'trusted' or 'untrusted' allowing or denying access accordingly.

ONLY MEMCYCO

- **Shields both business** *AND* CUSTOMER
- **Detects fake-site clicks** IN REAL TIME
- **Offers attack details** OF ATTACKER & VICTIMS
- **Enriches risk engine** WITH ATTACK FORENSICS
- **Brings breakthrough** MITIGATING TECHNIQUES
- **Proves site authenticity** TO CUSTOMERS

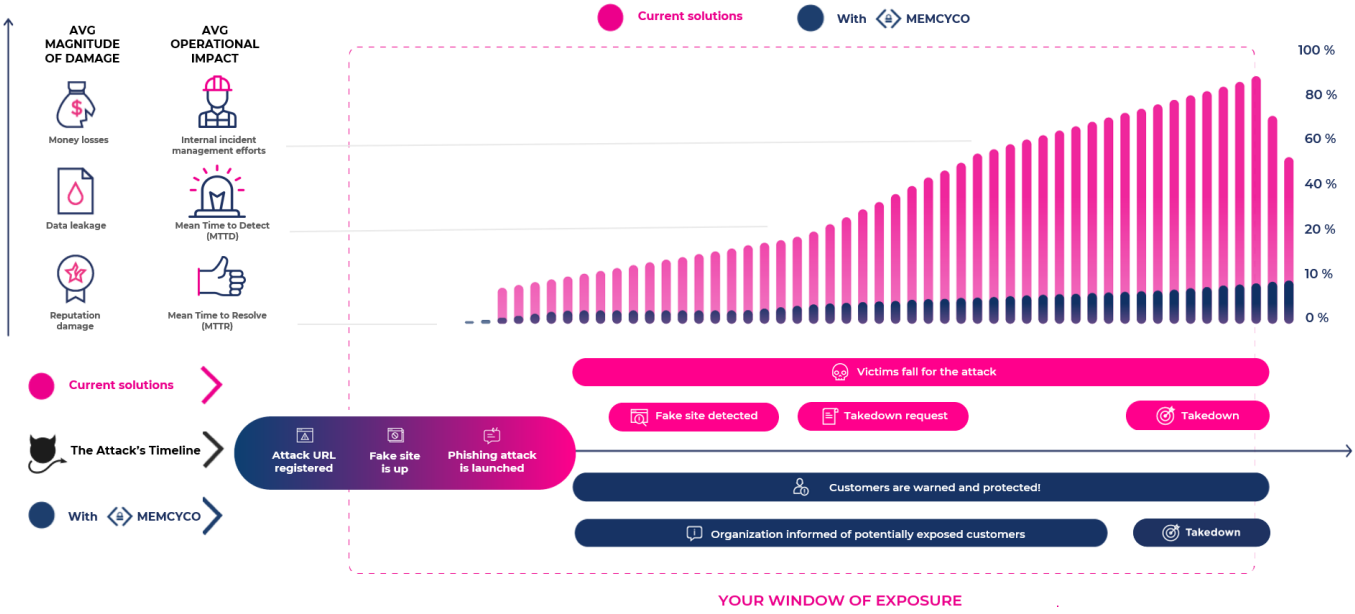
CLOSING THE 'WINDOW OF EXPOSURE' (WoE)

PHASE I

Phase 1 of your 'window of exposure' is the time from when an impersonating site goes live, to when it finally gets taken down. Historically, no effective solve for this has been offered and WoE is still widely accepted as an inevitable risk.

Fact 1: No other solution on the market offers active protection to you **and** your customers during the 'window of exposure'.

Fact 2: Memcyco is also the only solution that stops stolen data from being weaponized against you later by yet more bad actors.



PHASE II

After phase I, when the attacker already harvested user data, a second phase starts, during which that data is used to attack the company. In many cases the data isn't used immediately but rather sold on to yet more fraudsters hatching further attacks against your site. This is when the real damage is done, and attacks can persist over time.

BUSINESS VALUE

Fewer attacks
AND LESS HARMFUL

Fewer financial losses
FOR YOU & CUSTOMERS

Tons of money saved
ON INCIDENT MANAGEMENT

Regulatory resilience
CURRENT AND FUTURE

Stronger retention
AND ENGAGEMENT

Reduced risk
OF PR MELTDOWNS

MEMCYCO'S PLATFORM

UNDER THE HOOD

Detect

- Detect fake sites
- Identify scam victims and attackers
- Provide full-scope attack detail

Protect

- Notify customers with real-time Red Alerts
- Grant access to hacked users when using trusted devices
- Deceive attackers with real user credentials replaced with useless 'dummy credentials'
- Feed risk engine with previously unobtainable data

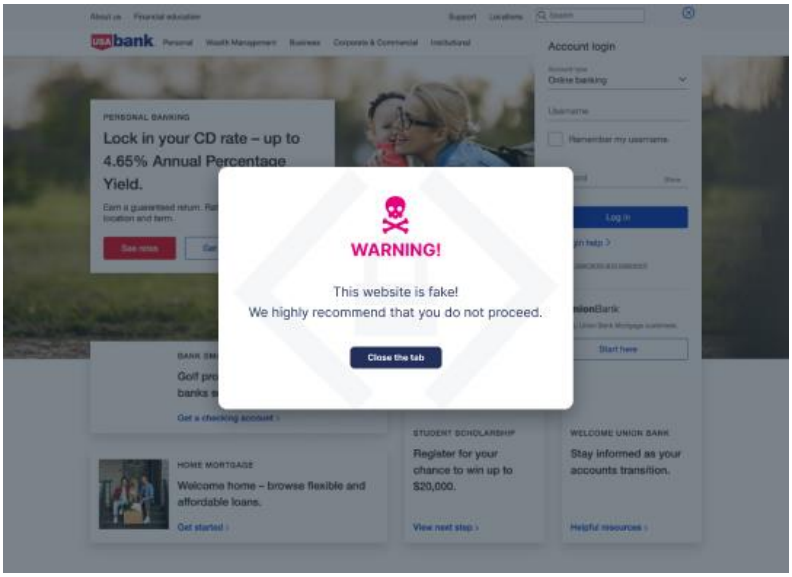
Respond

- Block attackers who access genuine site with decoy data
- Bombard fake sites with trackable 'dummy credentials', even if real user credentials were never stolen
- Take down fake sites

NO OTHER SOLUTION DOES THIS

Besides flagging attacks to you, Red Alerts pop up automatically on customer devices the moment they navigate to a site that impersonates yours. Memcyco is the only solution that does this. And it's 100% agentless.

Fact 3: Memcyco is also the only solution that delivers exact data on every user who fell victim to the attack.



ONE FINAL TRICK

What if you could replace real customer credentials, harvested by attackers, with artificial, trackable credentials? Memcyco does exactly that. Not only are these 'dummy credentials' useless; if attackers use them for ATO attempts, they risk revealing device data like geolocation, and other data that may be used to inform digital forensic investigation.