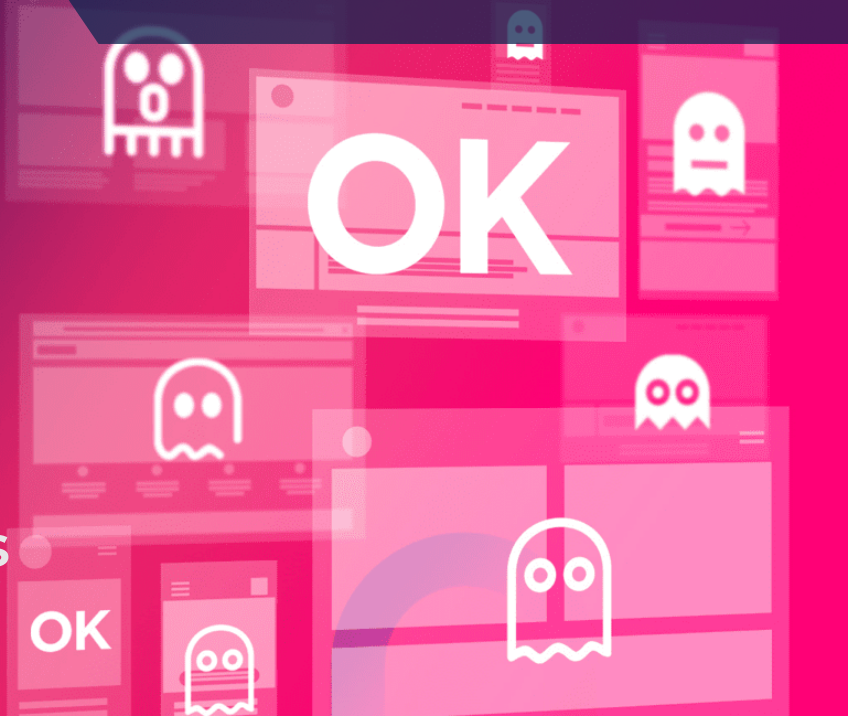
MEMCYCO
Authenticity goes both ways



Preventing frauds against your customers using sites pretending to be you

Fraud against customers in your industry occurs every day. Many of these frauds start by the criminal using sites that impersonate your brand.

The natural trajectory of your business is to become more digital. Today, most of the products offered in your industry as well as the communication with your customers are done online.

This opens the door for cyber-criminals to trick your customers and carry out frauds against them. Every year hundreds of thousands of customers complain about frauds, and organizations such as yours are paying tens of millions as remediation to them.

Some countries have actually passed regulations making organizations legally responsible for such remediation. Often, customers who are subject to fraud do not even know it until the damage is already done.

Organizations have no visibility and hear about these attacks from affected customers. MEMCYCO provides a solution that can help you and your customers to be protected from Frauds that use websites impersonating you.

Impact on Revenue

Loss of consumer trust can impact revenue by up to 20% per year [1]

Trust is Priceless

"73% of consumers would reconsider using a company if it failed to keep their data safe. Yet only 51% would switch companies if they were charged a higher price than competitors for a similar product" [2]

Stolen Identities

Brand impersonation represents 50% of cybercrime

MEMCYCO
Authenticity goes both ways

What Is Proof of Source Authenticity (PoSA™)?

While the market has invested tremendous effort into end-user authentication, the natural next step is a fully comprehensive solution which covers every point of impact between the user and the organization.

PoSA™ is the world's first solution that provides strong and secure proof of website and communication authenticity. It consists of two parts: An advanced detection, alerting and protection system, and a digital watermark.

Detection & alerting

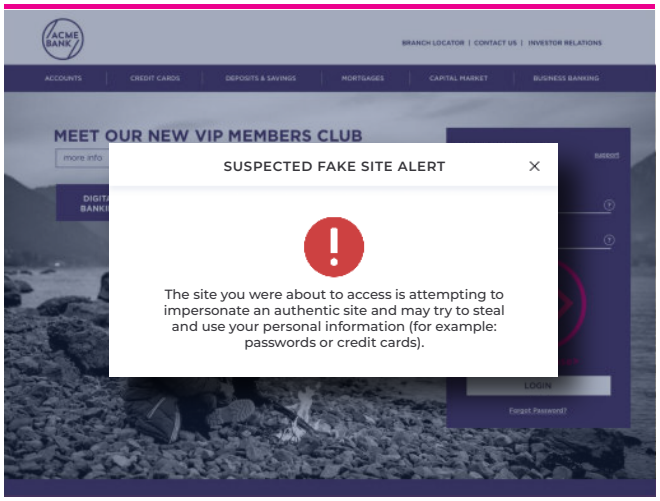
PoSA provides security teams with full visibility into attacks using fake or unauthorized sites, in real time, before any damage is caused. This enables organizations to take action immediately while protecting their users from falling into fraudulent traps

Main Features:

- Real time impostor site attack detection from day zero
- Details of all exposed end users
- Reverse engineering detection
- Impostor profiling
- Unknown workstation / environment detection
- Multiple credential attempt detection
- Password brute force detection
- Low reputation referral detection following fake site visit

Red alerts to end users

PoSA also provides a Red alert to end users when they attempt to navigate to a cloned or spoofed site, in order to prevent them from falling into the attacker's trap



MEMCYCO
Authenticity goes both ways

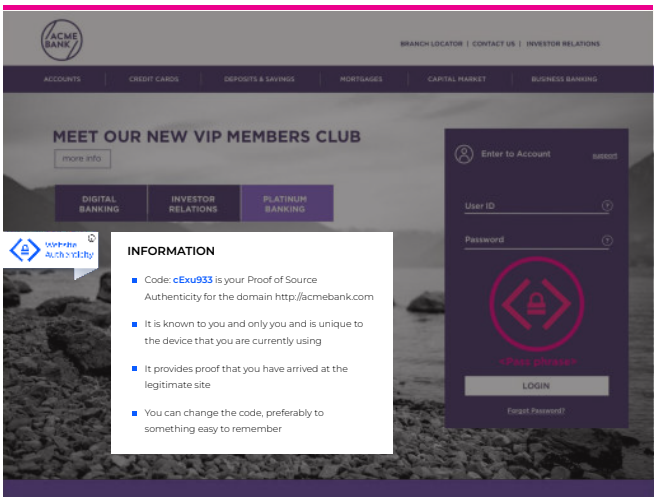
The Digital Watermark

A brand can increase their end-user trust by implementing PoSA™'s digital watermark. It provides instant Proof of Authenticity to end-users, proving to them that the website they visit and communications they receive are truly genuine. The watermark can also be applied to your authorized partners' websites, helping you tackle unauthorized 3rd parties.

The watermark contains a code and animation that are randomly generated and can be customized at will by the end-user, meaning they are un-forgeable. Crucially, the end-user does not need to register or install anything to see the watermark.
PoSA™ also respects and protects user privacy. The watermark is generated on device and remains there.

See the real end-user experience of a site supported by PoSA™

Click here



Installation & deployment

One line of code installation on website, no user registration or installation required.

Key Benefits

- Know when brand impersonation attacks are planned and executed on your customers
- Protects users from falling into brand impersonation traps
- Real-Time detection before damage is done
- Leverage attack scope visibility to prioritize response and remediate customer experience impact
- Increase revenue as a result of increased trust
- Reduce user education efforts
- Know identities of all attacked users
- Requires minimal effort to install, deploy and maintain
- Increase trust by positive visual confirmation of authenticity
- Reduce user education efforts