MEMCYCO
Authenticity goes both ways

Preventing impostor attacks on your customers

Impostor attacks and counterfeit scams occur every day and consumers fear they will be next.

Your customers' fear is well justified, as cyberattacks such as these are exponentially rising. No vertical or industry is immune from these attacks. After hearing about an attack, consumers become hesitant about interacting with any business in the affected industry.

This results in:

> Lower conversion rates for emails, text messages, online ads, and websites

> Broad erosion of trust in a brand

Often, customers subject to scams do not even know it until the damage is already done. Brands have no visibility and hear about these attacks from affected customers.

This results in:

> Frustration and loss of customers' confidence

> Loss of business from complaining customers and even worse, from those who don't

> Negative Impact on brand reputation

> High compensation and recovery costs

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

OK

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.
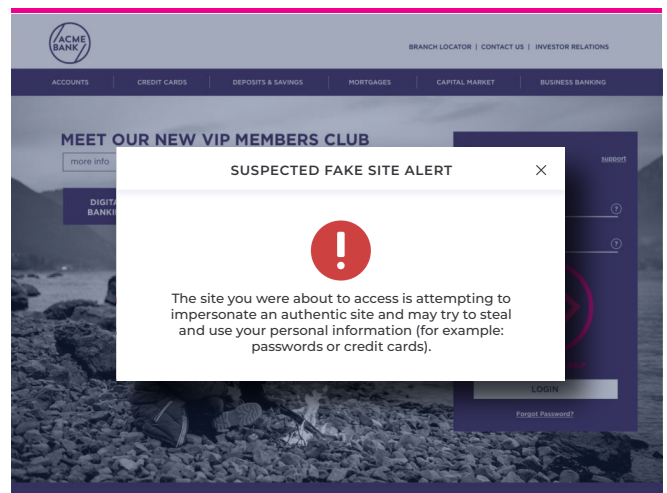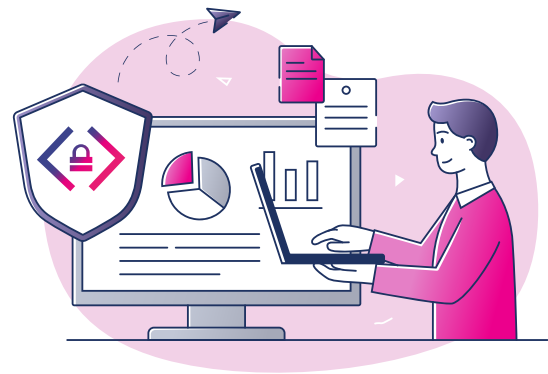

Main Features:

- › 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

ACME BANK

BRANCH LOCATOR | CONTACT US | INVESTOR RELATIONS

ACCOUNTS | CREDIT CARDS | DEPOSITS & SAVINGS | MORTGAGES | CAPITAL MARKET | BUSINESS BANKING

MEET OUR NEW VIP MEMBERS CLUB

more info

DIGITAL
BANKING

support

SUSPECTED FAKE SITE ALERT   ✕

!

The site you were about to access is attempting to impersonate an authentic site and may try to steal and use your personal information (for example: passwords or credit cards).

LOGIN

Forgot Password?

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
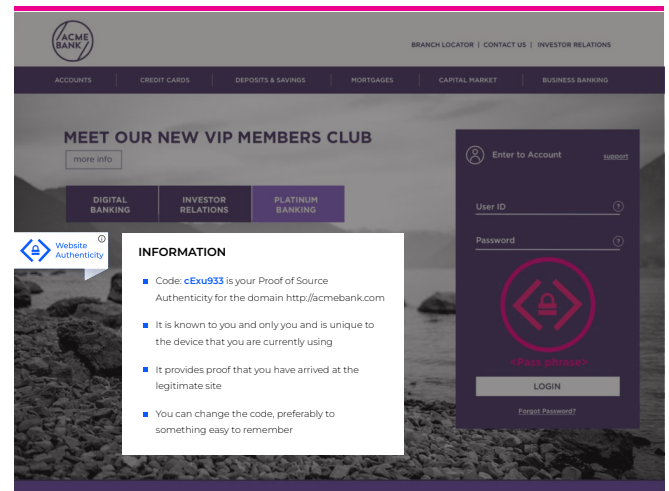
Installation & deployment

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

> Improve online campaign conversions

> Know identities of all attacked users for easier communication

> Increase trust by implementing positive visual confirmation

> Reduce user education efforts

> Prevent unauthorized affiliates

> Increase sales, reduce costs