Status Quo Anti-Phishing is Ineffective

Some websites attempt to combat phishing by placing a static picture on the login page. The picture is intended to assure the user that they are on the real website and not a phishing site. This approach is ineffective because the picture never changes so users tend to ignore it. Furthermore, a static image is easy to spoof.

Dynamic, Mutual Authentication is the Solution

Confident ImageShield™ is an image-based, user authentication technology that generates one-time passwords. It can be used as a dynamic, mutual authentication solution to fight phishing. It displays different images every time and requires the user to actively authenticate by correctly identifying which images fit their previously-chosen, secret categories.

How it Works:

1. The first time a user registers with your website, they will go through an enrollment process. The user will select a few authentication categories they can easily remember – such as bicycles, flowers and cars.

2. To log in to your website, the user enters their username and a Confident ImageShield is displayed.

3. The user authenticates by identifying which images on the Confident ImageShield fit their secret authentication categories. The Confident ImageShield generates a one-time password that is added to the user’s login credentials.

4. Only after successfully authenticating using the ImageShield, the password field becomes enabled and the user can enter their text password.

One-Time Passwords

The pictures that appear on the Confident ImageShield are different every time, but the user will always look for their same categories. Each picture is randomly paired with a different alphanumeric character. In this way, Confident ImageShield generates a unique, one-time password every time. Yet, the user only needs to remember their few categories.

By creating one-time passwords, Confident ImageShield provides strong authentication that is secure against dictionary attacks, keyloggers and the security breaches associated with weak passwords, stolen credentials and password re-use.

Current Anti-Phishing Vs. Confident ImageShield™

- Single image is the same every time and tends to be ignored over time
- Static image can be readily spoofed
- Not interactive
- No opportunities for password strengthening
- Multiple images,
- Images change each time but the user’s categories always remain the same
- Interactive to engage the user in the security process
- Adds one-time passwords to the login credentials

GET STARTED TODAY!

Web demo: www.confidenttechnologies.com/demos
Visit www.confidenttechnologies.com/trial to start a FREE trial
Why it’s More Secure

The specific pictures on the Confident ImageShield, their location on the display, and the alphanumeric characters associated with each image are different every time. In this way, the user must actively engage with the authentication process to identify which images fit their secret categories. This makes the user an active participant in strong security practices and prevents the user from ever entering their password on a spoofed website where the Confident ImageShield does not appear.

Administration Options

- Control the size and shape of the ImageShield and number of images displayed. Example in-line and grid options:

  ![Image Shield Options](image)

- Determine the number of categories users must remember
- Dictate whether or not users must identify images in order
- Display or hide letters overlaid on the images
- Choose clickable version or require users to type letters
- Fully customizable look and feel to match your website
- Integrates easily with existing user management, authentication, and access control systems
- Built-in alerts that complement your security monitoring or risk management systems
- Manage configuration settings from an internal admin console
- View security performance metrics

Deployment Options

Confident ImageShield for anti-phishing can be deployed as:

1. Software as a Service (SaaS)
2. An appliance installed in your data center

Confident ImageShield can also be licensed as a white label component for OEM enterprise solutions to enhance security and usability for your users.

Full SDKs Available in:

- ASP.NET version 2.0 and up
- PHP version 5 and up
- Java Standard edition 5 and up
- Python 2.7 and up
- IOS version 4 and Android 2 for mobile

Full RESTful web service support for other platforms.

Contact Confident Technologies

Visit: [www.ConfidentTechnologies.com](http://www.ConfidentTechnologies.com)  Call: 858-345-5640  Email: Sales@ConfidentTechnologies.com

GET STARTED TODAY!  Web demo: [www.confidenttechnologies.com/demos](http://www.confidenttechnologies.com/demos)  Visit [www.confidenttechnologies.com/trial](http://www.confidenttechnologies.com/trial) to start a FREE trial