WORLD SAVINGS®
Our strength is your security.℠

1901 Harrison Street – H07SE
Oakland, CA 94612

W3C Workshop on Transparency and Usability of
Web Authentication
March, 15-16 2006

Contributors

Kenneth L Wright II
Electronic Fraud Analyst
electronic Fraud Research
+1 510 446-4950
kwright567@worldsavings.com

FFIEC as a starting point

The Federal Financial Institutions Examination Council (FFIEC) released an interagency guidance stating, "Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks,"

This guidance pushes financial services to move towards fraud prevention by implementing stronger security, including multi-factor authentication into their authentication platforms. But the guidance offers no specifics on how to assess or mitigate the risks posed by single-factor authentication nor steps to monitor, track, and report fraud attacks.

Similar risks that financial institutions are faced with can be found throughout the eCommerce space across the web today. Many eCommerce sites lack the ability to properly conceal personal data, or inform end-user of the information not needed to navigate through the site. A common point of compromise will usually lie with the end-user being unawareness of fraud prevention practices. Multi-factor authentication platforms are designed to authenticate an end-user to site, but emphasis need to be address on the authentication of the site to the end-user. Many techniques and philosophies that are the bases for various multi factor authentication solutions are universal in the space of mutual authentication. Both multi and mutual authenticator rely on the en-user knowledge or recondition of a key phrase, biometric trait, or the ability to provide something they know.

The FFIEC guideline principles are the proper step to enforce similar tactics seen in the financial institutions authentication space to industries that are target point for data interception. End-users require standardization in addition to education to better assess the trustworthiness and identity of websites. By enforcing a standardized platform across different platforms such as online banking, eCommerce, and info update pages. It helps to instill an awareness of what is “Phishy” or and what is the “Norm”.

Growing Mutual Authentication Solutions

Since the release of the FFIEC report in 2001, there have been many technological innovations and legislative requirements introduced surrounding the protection of customer data. Also during this time, we have seen a rapid increase in the risk to the consumer through fraud schemes, such as identity theft, transaction fraud and phishing.

Multi-Factor Authentication is defined as an authentication protocol that requires two or more independent ways to establish the identity and privileges of a end-user. This contrasts with traditional password authentication, which requires only one factor, the knowledge of a password, in order to gain access to a system. Mutual Authentication is defined as the process of two principals proving their identities to each other.

During the research of multifactor authentication a review was made of various levels of products, services and/or solutions in this space. The most compelling solutions incorporated a global stance of front-end, in-session, and backend authentication and analysis.

Low Level

A visual design using a unique combination of visual indicators such as background color, font color, and/or a unique text message displayed to the end-user upon providing the site with their confidential information.

Mid Level

A visual design using a unique personalized graphic image and phrase displayed to the end-user upon providing the site with their confidential information. As well as authenticating the consumer to the site, by verifying the individual’s login credentials and device characteristics.

High Level
Incorporating a Mid Level platform by providing a visual design using a unique personalized graphic image and phrase displayed to the end-user upon providing the site with their confidential information. Combined with a mechanism to deliver an in session timer for a visual display of connectivity to the end user. Upon log out an email notification in addition to an on screen display providing the end-user a personalized transaction receipt.

Conclusion

Throughout my career in fraud operations and investigations, I've had the unique ability to have extensive interaction with the end-users perspective of being victimize. The event description that is common among most victims is "I didn't know, It told me to enter my info so I did." Why reinvent the wheel, using the fraud's tactics of misleading/ misinforming the end-user, can be used to empower and educate a user to combat fraud schemes. It is my stance that manipulating system structures by making browser enhancement, system configuration changes, and fraud detection program still doesn't address the end user's inability to detect fraud.

Member education is critical in terms of reducing account fraud and identity theft. Ecommerce sites currently offer consumers mounds of literature regarding return & refund policies, contact us information, and check-out procedures. But data sensitive sites are dropping the ball in the area of fraud awareness tips and techniques.

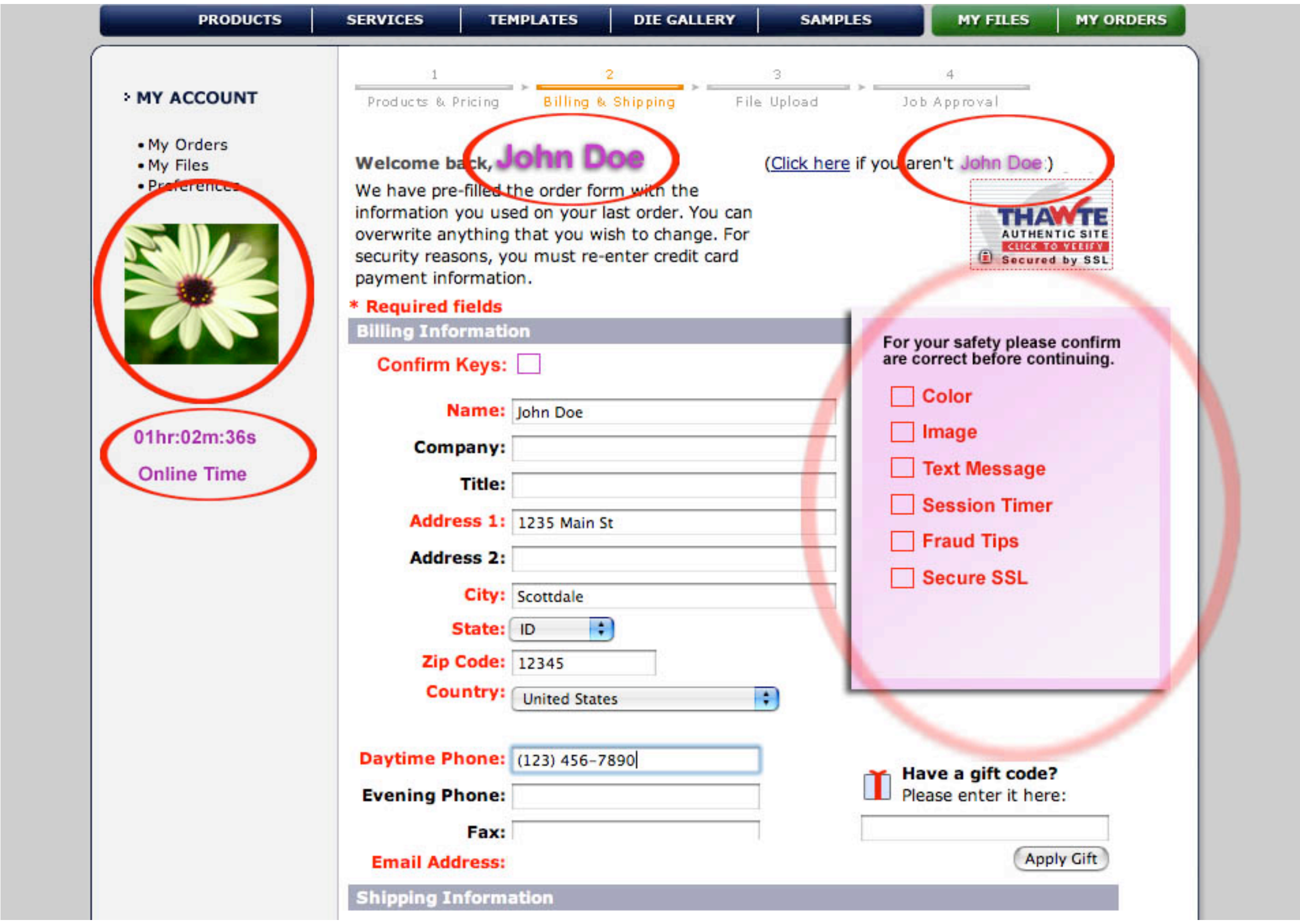
Incorporating a level of multifactor and/or mutual authentication with onscreen educational literature will instill fraud awareness to the end-user which will lower the pool of potential innocent victims.

By enforcement a universal format for the placement of fraud literature and providing end-users with personalized visual element can create a "reverse biometric authenticator" system. Biometric authentication is a method whereby an individual's identity is confirmed by examining a unique physiological trait or behavioral characteristic. The same process can be used to validate a site to the customer by providing the end-user with unique visual trait or behavioral characteristic that the site operates.

By training the end-user to validate a site using universal check and balances found in many financial institutions today. The End-user will learn to trust only sites that are created using these approved formats and avoid "Phishy" sites. In many fraud schemes today end-uses fail to provide end-user with step and techniques to investigate the site for themselves. Providing the end-user with key to authenticate a site can be as simple as a check list:

- ✓ Personalized greeting (correct spelling)
- ✓ Personalized color scheme
- ✓ History Data check
- ✓ Sensitive Data glossary

If widely accepted this method of personalized visual and behavioral indicators will heighten an end-user consciousness of safe data sharing procedures over internet channels. Placing complex but user friendly interaction barriers in the path of fraud attacks will lend a hand to weed out a growing population of opportunist fraudsters.



MY ACCOUNT

- My Orders
- My Files
- Preferences

01hr:02m:36s
Online Time

1 Products & Pricing → 2 Billing & Shipping → 3 File Upload → 4 Job Approval

Welcome back, John Doe (Click here if you aren't John Doe)

We have pre-filled the order form with the information you used on your last order. You can overwrite anything that you wish to change. For security reasons, you must re-enter credit card payment information.

* Required fields

Billing Information

Confirm Keys:	□
Name:	John Doe
Company:	
Title:	
Address 1:	1235 Main St
Address 2:	
City:	Scottdale
State:	ID
Zip Code:	12345
Country:	United States
Daytime Phone:	(123) 456-7890
Evening Phone:	
Fax:	
Email Address:	

For your safety please confirm are correct before continuing.

- □ Color
- □ Image
- □ Text Message
- □ Session Timer
- □ Fraud Tips
- □ Secure SSL

Have a gift code?
Please enter it here:

Shipping Information

klw