

## *Finding a Balance between Security and Convenience*

Security is top of mind in most businesses today and particularly so in the financial services industry. Striving for a balance between security, safety, cost and convenience is, and will continue to be, an ongoing challenge. Keeping up with security measures and technologies is a constant game of cat and mouse. Ensuring your financial institution is as unattractive as possible to fraudsters and preventing the mistakes of well-intentioned staff, while also looking at ways to ensure security measures are in place and kept current, requires continual diligence.

While members are looking for some assurance that their money and information are safe, employees seek security measures that are easy to implement and monitor day to day. However, both members and employees alike require that these security systems are intuitive, effective, and easy to use.

It is advisable to begin by leveraging the existing security features already available within your applications. Consider a vault that is constructed with the most sophisticated locking mechanisms available, but that is left hanging open. That is the case with applications that have elaborate features to block unauthorized access, but that allow a four-digit, numeric-only personal identification number (PIN).

Another area to focus your efforts is social engineering, which is a collection of techniques used to manipulate people into performing actions or divulging confidential information. Some common methods include "phishing" and "pharming," the act of enticing people with emails or links to fraudulent or counterfeit sites and capturing their credentials for later use. "Attack vectors," the general term used for different ways criminals compromise systems using malware (malicious software), including spyware, trojan horses, keystroke loggers, denial of service and brute force attacks, are also very common. Without question, one of the greatest tools for addressing social engineering is in the realm of public education - both internal and external - recognizing the tremendous influence that education can play in creating "social change."

How can your credit union educate members about social engineering? The first step is to develop educational programs that are tailored to your credit union and membership. It is extremely important that online security measures be heavily marketed to members. For example, multi-factor authentication solutions provide tools to combat against online fraud and provide the ability to deter phishing, pharming, key logging and brute force attacks, as well as provide real-time monitoring of Internet traffic and member activities. Educating members about security precautions when online or when using checks and card products can help reduce or even prevent an increase in fraudulent activity. What can your credit union do to prevent social engineering attacks? Install an incident reporting and tracking program that will help you discover and address specific vulnerabilities. Policies, standards, guidelines, and so on cover a wide range of areas, but the important thing is to develop them internally with growth and accountability in mind. Topics that should be covered include information sensitivity, password protection, ethics, acceptable use, email, database credentials, Extranet usage, VPN security, and server security.

On the technical side, continue to install spam filters and update software patches, at a bare minimum. Making cryptography standard for email and Web access, not allowing passwords to be saved in browsers, and changing to an internal messaging program are a good first step.

No security solution today is bullet proof; the best solutions make it harder for the fraudsters to infiltrate your financial institution and target your members. As victims of car theft have learned, the goal is to deploy security to make yourself the least attractive target to the thieves. With credit union security, the goal is similar; make your members the least attractive target possible. As your members' trusted financial advisor, your job is to balance security with member-acceptance, reliability, performance and adaptability.



**Niles Bay**  
Vice President

**Niles Bay** is Vice President of Product Development for Harland Financial Solutions. With over 21 years of software development experience, 14 within the financial institutions industries, he has led development efforts for the credit union core systems group of Harland Financial Solutions for four years. Previously he held technical and executive positions at Intel, Electronic Data Systems, and Metavante. Harland Financial Solutions supplies software and services to thousands of financial institutions of all sizes, offering its solutions in both an in-house and service bureau environment. The company is a leader in core systems, item processing, enterprise content management, branch automation, customer relationship management, business intelligence, origination and document solutions, risk management, compliance training, financial accounting, open documents, mortgage solutions, electronic funds transfer (EFT), self service solutions and performance advisory services.

**HARLAND**  
FINANCIAL SOLUTIONS

 **UltraData**

**Contact Info:** [www.harlandfinancialsolutions.com](http://www.harlandfinancialsolutions.com)