

IronKey Protects Commercial Online Banks and Customers from Malware, Fraud and Invalid Fund Transfers



“ In the past six months, financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid banking credentials belonging to small- and medium-sized business. ”

2009 NACHA and FBI Guidance to Financial Institutions

Safeguarding Commercial Online Banking Customers from Next-Generation Malware

A major shift in the tactics of global cyber criminals is putting commercial banking customers at significant risk. A rapidly rising number of attacks using a new generation of malicious software (“malware”) has cost corporate banking up to \$1,000,000 per incident. Once this malware infects a computer that is used to access commercial online banking services, the attackers can effectively take over the corporate financial accounts in real time by hijacking active banking sessions. They can then issue commands for funds transfers to offshore accounts, where the money is rarely recovered.

It is far more lucrative for cyber criminals to make numerous \$9,000 transfers from a single corporate bank account than to try to hijack thousands of consumer-based accounts and make small money transfers.

Risks Posed by Next-Generation Malware

This commercial online banking malware comprises a number of new families of Trojans that use live authenticated sessions to defeat traditional security defenses, including multi-factor authentication that banks have employed to protect consumers against phishing fraud. They are not only capable of stealing corporate authentication credentials, but they can also perform fraudulent transactions from a victim’s own computer.

The IronKey Solution—Isolating the Banking Environment from Online and PC-based Threat Vectors

In response to this threat, IronKey has developed an easy-to-use and cost-effective solution for banks, which also implements recently updated NACHA guidance. Combined with best practices—such as initiating payments under dual control, and out-of-band transaction payment confirmation—the IronKey™ Enterprise Online Banking Solution protects commercial banking customers from next-generation malware. The solution also is designed for easy deployment to corporate banking customers—it requires no installation of software on most customers’ computers, and an online service manages the devices and provides security updates.

The IronKey Enterprise Services Online Banking Solution includes:

Easy-to-Use IronKey Multifunction USB Flash Drive Security Device—includes an onboard virtualized operating system and Web browser that is protected against malware on the host PC.

The device is easy-to-use. Corporate banking customers simply plug it into their Windows computer and enter their device password when the IronKey login screen appears. Once the IronKey flash device is successfully unlocked, its virtualized operating system automatically runs, and the secure portable Web browser launches and goes directly to the issuing bank’s website.



Two-Factor Authentication with Onboard RSA SecurID—

Eliminates the need to issue a second two-factor authentication device. The IronKey device includes onboard RSA SecurID One-Time Password technology, so that a single USB token serves both as a secure banking platform, as well as a strong authentication device.

Onboard Anti-Malware Scanning—Implements one of the key best practices recommended by NACHA and the FBI, which calls for corporate banking customers to ensure that all anti-virus and security software is robust and up-to-date. Developed in partnership with McAfee, the IronKey anti-malware solution receives regular updates, and ensures that users' computers are scanned for known malware whenever they initiate an online banking session.

Secure Virtualized Environment Protects Against Malware—

The secure virtual machine player on the IronKey runs a hardened Linux-based operating system that is completely isolated from any malware on the PC host. From inside the secure operating environment, the user launches a locked-down Web browser, which goes directly to the bank's website and cannot be used to access other websites.

Optional Security Services—Include transparent PKI authentication and anti-pharming via trusted DNS.



The IronKey Multifunction Security Device

Is a unique integration of custom silicon, security firmware, security software, and online security services. It provides a unique set of security features and benefits, including:

- Password protection and hardware encryption keep the device secure if lost or stolen. FIPS 140-2 Level 3 security validation is the highest available on the commercial market
- All IronKey applications are digitally signed and verified on the IronKey device using an RSA 2048-bit key before they can be installed and run on the IronKey device
- Password self-recovery allows banking customers to retrieve their device password via email and challenge questions, reducing Help Desk calls
- Onboard RSA SecurID interoperates with your existing authentication infrastructure and saves you money
- Onboard PKI with digital certificates functionality allows you to extend the capabilities for non-replayable authentication and digital signing of transactions
- Security and software updates over the Internet ensure that your customers have the latest anti-malware signatures and IronKey security updates
- Auto-timeout logs users out of the device so that malware cannot use it to spoof connections during off-hours and weekends
- Remote kill and lock-out of lost and stolen devices allow financial institutions to remotely deactivate devices in the field
- Ability to limit IronKey device usage to specific IP Address range(s)—e.g., a customer's corporate network
- Rugged and waterproof design ensures device longevity



www.ironkey.com
sales@ironkey.com

5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA

Toll-Free 866 645 9847
T 650 492 4055
F 650 967 4650