



Cernious CamoKey™ Use Case

Real-Time Protection Against Real-Time Credentials Theft

Business Problem

Consumers are increasingly targeted by cyber criminals for their login credentials (e.g. usernames and passwords) required by businesses for online transactions.

One tactic employed by such cyber criminals is to first penetrate unprotected PCs with key loggers – programs that record every keystroke on a keyboard, and then quietly send the logs to remote sites to parse for usernames and passwords. Advanced, real-time Optical Character Recognition (OCR) technologies render typical virtual keyboards useless.

Symantec's research indicates the proliferation and growth of such tactics: of the top 50 malicious programs infecting PCs, 65% target confidential information; with *88% of those malicious programs containing keystroke-logging capabilities* – an increase of 16% in just one year (*source: Government Internet Security Threat Report, Symantec 2007*).

Whereas consumers must do more to protect their PCs, businesses are at the greatest aggregate financial risk when their customers' login credentials are stolen: these cyber criminals use the stolen credentials to login to the businesses and conduct fraud.

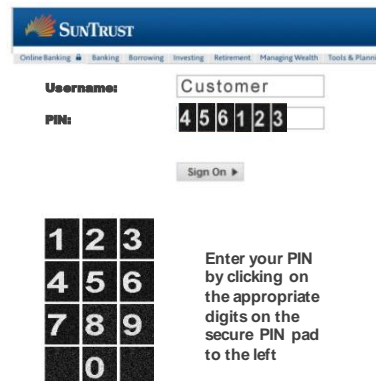
According to a 2007 study by Forrester, the cost per data record stolen ranges from \$90 to \$305. With total records stolen estimated to be 30k to 188k per breach, the costs to the business can be anywhere from \$2M to \$22M!

Cernious Solution

With Cernious' CamoKey™ virtual keyboard and PIN pad, the end users' entries and the keys themselves become invisible to advanced key-loggers.

Prior to entering in login credentials, the site presents the user with Cernious' CamoKey™ on-screen keyboard.

Animated images of text and numbers are readable by the end user, but not by automated OCR programs and key loggers – meaning the end user's login credentials are safe even before they are encrypted for transfer over the Internet.



Illustrative mock-up

Key Advantages

- **Real-time protection from credentials theft** conducted by malicious programs residing on un-secure PCs and endpoints – with no client hardware or software required!
- **Extends reach of enterprise data protection measures** to circumvent threats residing on PCs operating outside managed security environments
- **White-label SaaS solution** enabling unprecedented scale for brands built on delivering trusted services
- **Dynamic security delivery model** enabling real-time adjustments to stay ahead of evolving security threats

Contact Cernious for additional information or to schedule a demo

Tim Brown
Tim@Cernious.com
(801) 673 – 3322
www.Cernious.com