EASYSOLUTIONS

End-to-End Fraud Management

Stopping Cybercrime at the Customer Level

Summary Financial institutions are working hard to prevent fraud and keep their customers' money safe. But there is a wild card variable enabling fraud that institutions have no control over: end-user browsing behavior. Malware and phishing attacks resulting from poor user decisions have resulted in millions of dollars in losses, and courts are holding banks responsible. To reduce both liability and fraud, financial institutions must make it easy and convenient for customers to safely bank online while also obtaining insight into whether the users are doing what is necessary to keep themselves safe.

Detect Safe Browsing to Go (DSB2Go) from Easy Solutions is a secure personal web browser that creates a protected connection to transactional websites, defends against malware and other sophisticated threats, and gives financial institutions insight into whether end-users are taking the necessary measures to protect themselves when banking online. Delivered to end users in the form of a small, lightweight, and portable USB device, DSB2Go lets your customers perform transactions anywhere and from any machine while making sure those transactions are protected with the ironclad security you've come to expect from Easy Solutions.

TABLE OF CONTENTS

END USER BROWSING BEHAVIOR: THE ACHILLES HEEL OF FIGHTING FRAUD

1

As a financial institution, you've done what is necessary to comply with FFIEC regulations and keep users safe when making online transactions. You've implemented strong multi-factor authentication, transaction anomaly detection, and real-time monitoring of individual account behavior. You've synthesized all of these security measures into a layered protection plan meant to capture fraud at different points in the transaction process and counterbalance the weaknesses of any single control mechanism. You've blocked countless fraudulent IP addresses and applied out-of-band authentication to reduce money transfer fraud. But there is one link in the security chain that is completely outside the financial institutions' control: end-user browsing behavior.

It may seem incredible to those of us who work at financial institutions and online security firms, but many users don't know the first thing about keeping themselves safe when banking online. They make foolish decisions, like disabling anti-virus programs because they might slow the machine down a bit. They use internet cafes for online banking when traveling, or make transactions from public networks in places like airports and coffee shops. They click on phishing e-mails and links, sending credentials and passwords in response to emails when the institution has repeatedly said they would never ask for information in that way.

If this were just the client's problem, and they had to completely bear the brunt of their weak decision-making, banks could rest easier knowing that they did all they could to protect their customers' money. But the truth is that it's the financial institutions that are often on the hook for these bad customer decisions. Two recent court cases, both of which came down in favor of the customer and against the banks, illustrate that financial institutions are being held responsible for the money lost in online fraud incidents, even when a customer allowed malware to infect their machine, thereby enabling an attack.

> Experi-Metal v. Comerica

On the morning of January 22nd, 2009, an employee of the Michigan-based auto parts company Experi-Metal received a phishing e-mail that purported to be from Comerica Bank where the company held accounts. The employee entered his credentials into a false third-party imitation of the Comerica website, which enabled the criminals to make dozens of transfers over the next several hours to accounts located in Russia, Estonia, and China. All in all, $561,399 USD was lost, and the bank refused to cover the losses. This led to Experi-Metal suing Comerica, and the courts ruled in favor of the company, saying that the bank failed to prove it had accepted orders for the fraudulent transfers in good faith, even though the courts also said that the bank was found to have commercially reasonable security procedures in place, and that no bank employees acted dishonestly in accepting the fraudulent orders.

Comerica ended up settling out of court, deciding not to challenge the decision that left a bank responsible for a commercial customer allowing its computers to be hacked.

END USER BROWSING BEHAVIOR: THE ACHILLES HEEL OF FIGHTING FRAUD

1

> Patco Construction v. People's United Bank

In May 2009, a hacker gained access to the Maine-based Patco Construction company's online banking accounts, though it is unclear how, since a subsequent malware scan on the infected computer in question may have destroyed evidence detailing exactly how the fraud occurred; Patco alleges the use of a Zeus Trojan. In any event, the hackers obtained stolen credentials and challenge question answers, which granted them the ability to make almost $600,000 USD in fraudulent wire transfers. Less than half of this amount was recouped, and the bank refused to cover the loss, since the customer facilitated the downloading of the malware that caused the theft. Patco sued, and eventually the courts ruled in their favor, leading to a settlement that refunded Patco for all money lost, including legal fees. The courts ruled that although the bank had a reasonable security strategy in place, it failed to stop fraudulent transfers when they were happening, even though they were enabled by the customer and not the bank.

These rulings have sparked a seismic shift in fraud liability, in favor of the customer who loses money, even when the problem occurred on their end and the bank has commercially reasonable fraud prevention measures in place. And "commercially reasonable" doesn't just mean compliance to the letter of the law anymore; it requires the thorough implementation of security measures so that they work properly while also making customers aware of their availability. It is a high bar to clear, and completely the financial institution's responsibility.

Moreover, financial institutions have no real idea of what users may or may not be doing to keep themselves safe. When fraud occurs, and hundreds of thousands of dollars are stolen from an account, the customer's first instinct is to expect the bank to take responsibility for the fraud and pay back all of the money they lost. But what if the user, knowingly or not, permitted the malware to infect their own computer, and clicked on the malicious links and entered their credentials on a bogus website? In the Patco case, the bank couldn't prove this, and in the Experi-Metal case, the fact that the user volunteered the relevant information by falling for a phishing scam didn't matter: the onus was on the bank to take responsibility, and financial institutions still don't have a reliable way to guarantee that users do the right thing and keep themselves safe when banking online.

STOPPING FRAUD IN THE END-USER ENVIRONMENT: HOPE IS NOT A SOLUTION

2

Many solutions that end users could adopt to prevent online fraud are simply not feasible. The FBI and the American Banking Association propose that businesses and individuals use a dedicated machine only for banking and that won't even be used for e-mail, internet browsing, or anything else people generally do with a computer. Besides not being affordable or convenient for the majority of individuals, this protection strategy is also only as secure as the dedicated machine is. What if your teenage daughter or laziest employee is using Facebook on that computer when nobody is around? How can you safeguard that machine from unauthorized web browsing? One security expert advised banking customers to do the following to ensure security when performing transactions online, using a dedicated machine:

…set up a PC with Microsoft's Steady State, disable any Internet access except to the bank's online application and uninstall Outlook Express. I would make a completely locked down and hardened installation of Windows with all services disabled except for essentials. Assign a static IP address to the machine. I would use a software firewall and disable all ports except 80 and 443. Of course, anti-malware software would be essential [1].

Well, you can throw the convenience of online banking out the window. And really, how many online banking users could pull a security scenario like this off, even if they could dedicate a computer to solely online banking? The average customer expects security to be integrated with their normal online routines, presumes applications and devices will work with minimal to no setup or installation, and probably doesn't know where port 80 is located. Using a dedicated machine puts far too much burden on the end user, and we know from experience that this will translate into gaping security vulnerabilities that criminals will only be too happy to take advantage of.

A dedicated computer also complicates things if a user needs to travel and access their accounts on the road. Having more than one laptop – one just for banking, and the other for everything else – takes all the convenience out of using a portable computer. In addition to the hassle, users will be forced to use that banking laptop on insecure public networks that are only as safe as the people using them. And if their dedicated machine gets stolen, lost, or damaged, they must start all over again with a new machine. Considering all the security risks and extra equipment, a dedicated machine can actually make going to a physical branch seem like less of a headache than accessing an account online when traveling!

Your financial institution has also probably led educational campaigns so that users can be better informed on how to interact with online banking resources and avoid becoming a victim of electronic fraud. But it is impossible to reach everyone, and our own poll data from last year showed that more than a third of online banking users had no idea their financial institutions even conduct educational campaigns at all, with the number of unaware users actually increasing from the year before.[2] In addition, phishing messages have come a long way from that Nigerian guy asking you to help him collect an inheritance; even leading tech companies like Facebook and Apple have recently fallen for sophisticated and highly-targeted phishing attacks, and if the technologically-savvy workers at those companies can fall for well-crafted online scams, your institution's customers are probably even more vulnerable.

1 Worth Repeating: Use a Dedicated PC for Online Banking, March 13, 2010 http://itknowledgeexchange.techtarget.com/security-corner/worth-repeating-use-a-dedicated-pc-for-online-banking/

2 Research Report – Views of Latin American Consumers on Electronic Fraud 2012, http://www.easysol.net/newweb/Industry-News/Research-Report

STOPPING FRAUD IN THE END-USER ENVIRONMENT: HOPE IS NOT A SOLUTION

2

Finally, none of these jerry-rigged solutions provide the financial institution with any visibility into the end-user environment. Most of the time banks have no idea what users are doing when they access their accounts online. In both of the court cases above, users unknowingly clicked on malware that led to an attack and thousands of dollars in stolen funds, and the bank had no idea until after the money was already leaving the account. A solution to the problem of end-user malware infection must be implemented at the end-user level, making it easy and convenient for customers to safely bank online while also giving financial institutions insight into whether the users are doing what is necessary to keep themselves safe.

DETECT SAFE BROWSING TO GO (DSB2GO) FROM EASY SOLUTIONS:

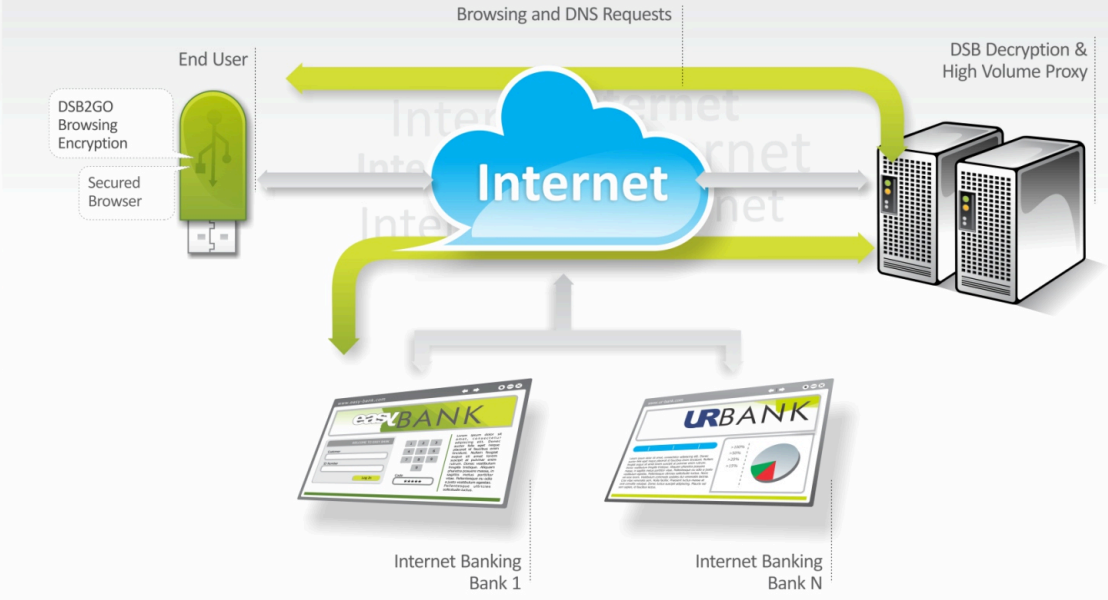
SECURE BROWSING ON ANY MACHINE, ANYWHERE

3

Introducing DSB2Go

Detect Safe Browsing to Go (DSB2Go) from Easy Solutions is a secure personal web browser that extends fraud prevention to the end user, creating a protected connection to transactional websites and defending against malware and sophisticated threats such as pharming, man-in-the-middle (MITM) and man-in-the-browser (MITB) attacks, where antivirus and spyware removal software are not effective.

Delivered to end users in the form of a small, lightweight, and portable USB device, DSB2Go is designed to prevent identity theft and electronic fraud while letting users continue to make transactions online the same way they always have. Using DSB2Go's online management portal, financial institutions can supervise the devices given to their customers, and make sure that users are doing their part to keep transactions secure.

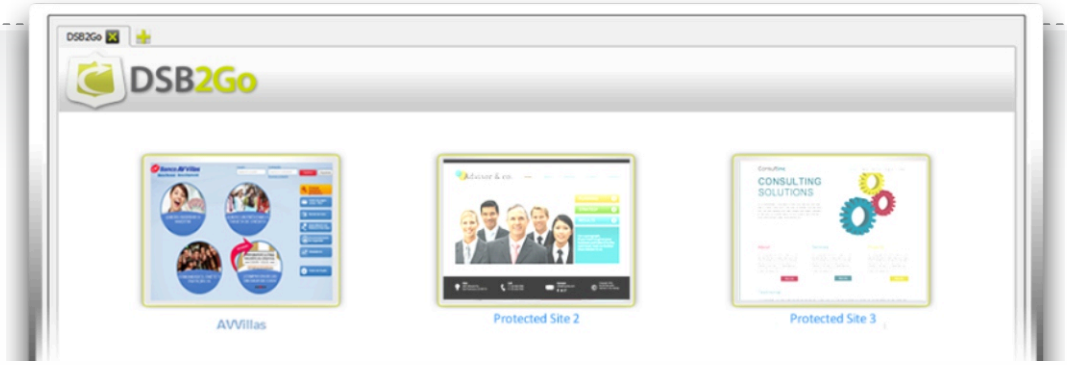


DETECT SAFE BROWSING TO GO (DSB2GO) FROM EASY SOLUTIONS:

3

SECURE BROWSING ON ANY MACHINE, ANYWHERE

The DSB2Go device works by creating a protected channel between the user's computer and Easy Solutions' secure servers, ensuring that the critical aspects of the transaction are happening at the server level and not on the machine, making those transactions impervious to any malware that might be on the computer. Essentially, DSB2Go turns any internet-connected computer into a dedicated machine for online banking, regardless of whether the machine is infected.



The protection of DSB2Go begins as soon as the user inserts the device into the USB port of their computer. There is no software or installation; DSB2Go's browser opens automatically when the device is connected. The computer doesn't even have to be restarted; no further end-user action is necessary for the secure online banking to begin. The browser itself is similar to almost any common browser your user population is already familiar with, the homepage contains the protected site or sites that your institution wishes to provide, and they are the only pages that users will be able to access through the browser. Using the concept of a unique session, the browser doesn't save any previous browsing history or information, keeping sensitive data safe even when a USB device or the computer it is connected to is lost or stolen.

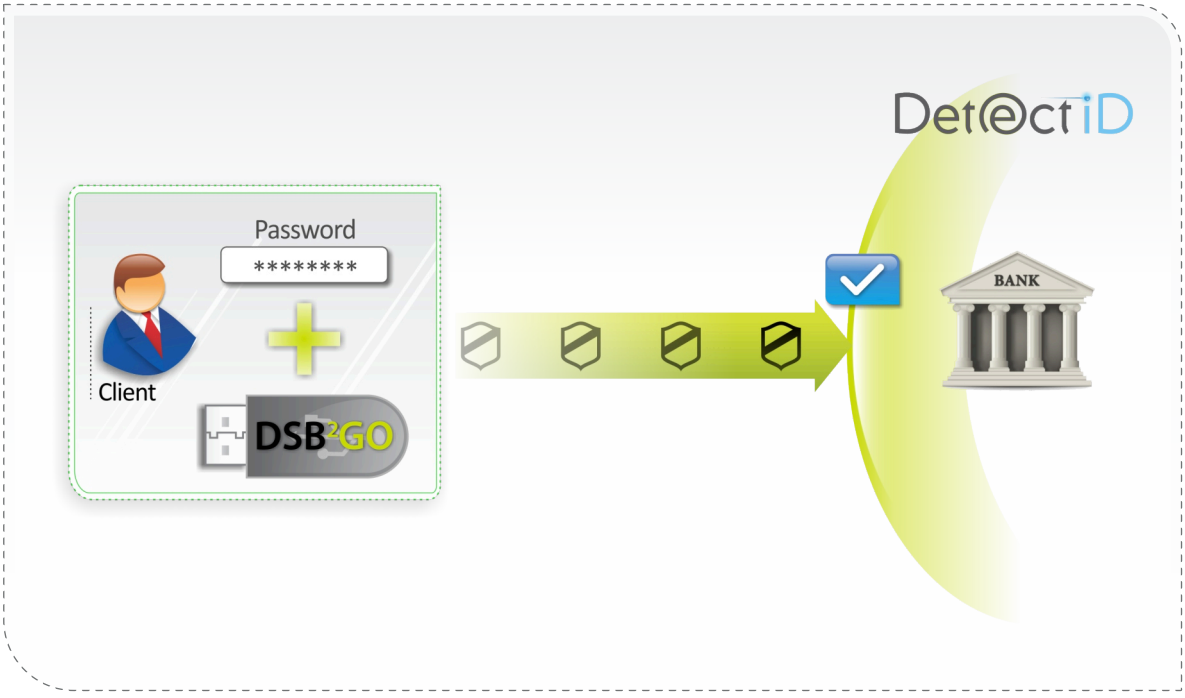
This is true end-to-end fraud management, giving institutions the final missing piece to fully solve the electronic fraud puzzle. DSB2Go simply asks users to connect a USB device and bank online the same way they would through a browser that is similar to Internet Explorer, Mozilla Firefox or Google Chrome. No anti-virus software to install, no firewalls, no dedicated machines; the user literally just has to plug in a USB device into any computer and they can bank safely. DSB2Go also eliminates the wild card of user behavior in contributing to online fraud; since transactions can only take place on the secure browser, and the browser only allows navigation to the bank's legitimate website, users can't be redirected to a fraudulent site, can't click on malicious links or attachments, and can't type their credentials somewhere where a keylogger can capture them. DSB2Go literally protects users from themselves by only allowing connections with transaction sites specifically chosen by a financial institution and blocking all others. In addition, DSB2Go restores the convenience of users being able to perform online transactions from anywhere and any machine without compromising on security.

DETECT SAFE BROWSING TO GO (DSB2GO) FROM EASY SOLUTIONS:

3

SECURE BROWSING ON ANY MACHINE, ANYWHERE

DSB2Go offers simple administration for financial institutions as well. Through an online management portal, financial institutions can supervise the parameters of the USB devices that end users will employ to access protected sites, sorting users into different groups with separate rules for streamlined organization and reference. The portal also provides visibility into end-user browsing habits, since the institution will have access to auditing and detailed reports that show when the devices are being used, and whether protected sites are being accessed with the device or not. Finally, financial institutions have a way of guaranteeing security when their customers bank online, and protecting themselves against liability for irresponsible user actions. With visibility into the end user's online environment, institutions have much more insight into whether their customers are enabling attacks by downloading malware or making transactions from unsafe locations. By offering a truly protected channel for users to access your institution's online banking platform, there will be fewer attacks to investigate, and your institution will be in compliance with FFIEC regulations that stipulate the use of solutions that protect customer information and prevent identity theft.

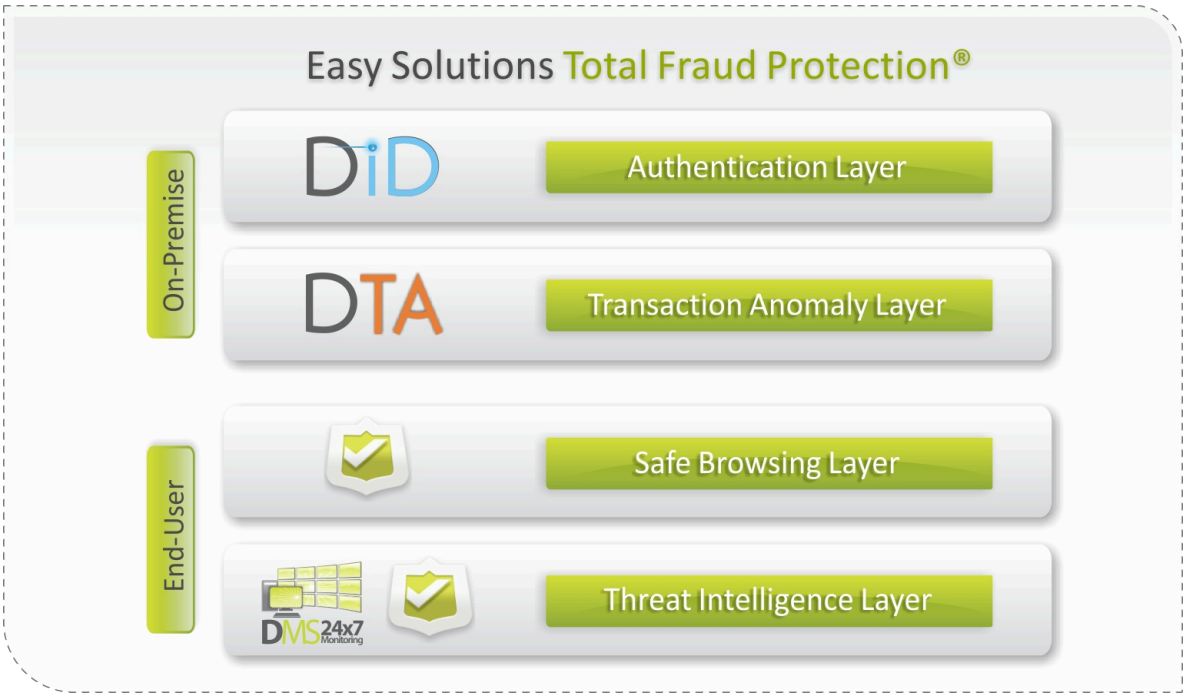


DETECT SAFE BROWSING TO GO (DSB2GO) FROM EASY SOLUTIONS:

SECURE BROWSING ON ANY MACHINE, ANYWHERE

3

When combined with DetectID, Easy Solutions' multi-factor authentication solution, the DSB2Go device turns into a second authentication factor to verify the user. DetectID uses proprietary, multi-factor and multi-channel technology to provide a wide array of user authentication types to suit your institution's security needs and desires, including authentication using devices, tokens, security images, challenge questions, one-time passwords, and virtual or physical grid cards. Under this combined fraud protection plan, any transaction attempted without using the DSB2Go protected browser can be denied or trigger additional authentication schemes so that only the genuine user is able to make transactions.



By creating a protected channel to your online banking platform through DSB2Go, and securing your devices and authentication procedures with DetectID, your financial institution and its customers can begin employing the Easy Solutions Total Fraud Protection Strategy: A multi-layered approach which proposes that there is no one single silver bullet solution for all electronic fraud problems, but rather a variety of solutions that seek to systematically thwart fraud across different transactional channels and at any stage of a fraud incident. This cutting-edge, holistic strategy includes different products offering services related to phishing prevention, multi-factor authentication, and the detection of anomalous transactions. Start preventing fraudulent transactions perpetrated against your customers' accounts today with DSB2Go and DetectID.

For more information about DSB2Go please visit ***www.easysol.net*** or write us at ***sales@easysol.net.***

ABOUT EASY SOLUTIONS

4

Easy Solutions is the only security vendor focused on the comprehensive detection and prevention of electronic fraud across all devices, channels and clouds. Our products range from anti-phishing and secure browsing to multifactor authentication and transaction anomaly detection, offering a one-stop shop for multiple fraud prevention services.

The online activities of 32 million customers of 120 leading financial services companies, security firms, retailers, airlines and other entities in the United States and abroad are protected by Easy Solutions fraud prevention systems. Easy Solutions is attractive to companies that want a one-stop shop for most fraud-related prevention services.

Easy Solutions is a proud member of such key security industry organizations as the Anti-Phishing Working Group (APWG), the American Bankers Association (ABA) and the Florida Bankers Association (FBA).

EASYSOLUTIONS

Headquarters:
1401 Sawgrass Corporate Parkway, Sunrise, FL 33323
– Tel. +1-866-5244782
Latin America:
Cra. 13A No. 98 – 21 Of. 401 Bogotá, Colombia
– Tel. +57 1- 7425570
info@easysol.net
www.easysol.net