



Cybercriminals first started to use malware in force back in 2005 to obtain authentication details from consumers. The initial methods used were simple: spam email distributed the malware, the malware recognised target businesses' URLs being accessed, pop-up messages then asked the consumer to re-enter their authentication details, or the keystrokes on accessing the business were recorded. These were then transmitted to the cybercriminal network to access the service and steal funds and perform identity fraud.

The current world is now seeing cybercriminals deploy upwards of 25,000 new pieces of malware on the internet every day, using ever-increasing ways to access and use the internet as their distribution channel. They are able to infect more than an estimated 50,000 PCs daily, continually exploiting vulnerabilities in even the most current and up-to-date PCs. With this scale and variety of attack, the security software industry is struggling to keep up.

Performing transactions on the internet is now part of everyday life for financial companies and their customers. Every day billions of pounds flow around the world as money for everything from corporate takeovers to gas bills is moved from one location to another. Today more than 500 million people log on to 2,000 online banks daily. These are now services that many people take for granted, allowing bills to be paid and money to be transferred while sitting in their living room. Internet banking is now a core element of a business' customer offering and profit generation; and consumers in our fast-paced world are increasingly reliant on its use and flexibility.

## Banking Fraud is a Serious Threat to Customer Confidence

Bank and eCommerce businesses are fully aware that cybercrime and consequential fraud losses are a serious threat to their services and profitability:

***"In the UK more than 21.5 million people now bank online. Most fraud on online bank accounts involves a customer being duped into giving away their user passwords and security information via a phishing scam, or by their PC being infected with spyware designed to steal the information. UK banks in 2008 saw internet banking fraud losses increase 132% to £52.5m, due to increasing use of malware" (source: APACS)***

In most countries the bank is liable for fraud losses, unless the customer has been unduly negligent. This is, however, difficult to prove and taking a more restrictive approach in a bid to reduce these threats, many banks have recently introduced stronger customer authentication to prevent fraud losses and improve consumer confidence, i.e. using chip and pin, risk engine and automated phone call solutions. These solutions can offer some protection in the short term. However, the cybercriminals have already reacted by using Man-in-the-browser attacks to obtain credentials and perform automated transactions using the customer's PC. This increases the sense of nervousness to the consumer; they are totally unaware of the fraud occurring and are more often than not unable to find out how the fraud occurred.

## Endpoint Protection is Key

Banks have been aware for some time that the quality of security on a customer's PC is key to effective fraud defences.

As a consequence, banks have maintained a consumer education strategy to advise the consumer on how to ensure their PC protection is up to date and patched. Often though this has fallen on deaf ears, due to a combination of the consumer not understanding what they need to do and having the comfort that, if they suffer fraud, the bank will usually compensate them. Government education programmes, despite significant funds to support delivery, have faced similar challenges and results in getting their message across to consumers.

In many instances the customer is totally unaware that their PC and personal information has been compromised.

Online Banking Fraud		Vectors Of Attack		
	Vector	Basic Methodology	User Awareness	Examples of Banking Trojans Deploying This Vector
Phishing Attacks		User typically receives an authentic looking email, or follows a 'convenient' link from another web site which takes the user to a fake but authentic looking web site where they unwittingly disclose their credentials.	May arouse suspicion	Not dependent on malware but can be triggered by it
Keystroke Loggers		Keystrokes are recorded as they are entered. These are correlated to the currently active web page and forwarded to the criminal's data center on demand.	Totally Unaware	ZEUS/WSNPoem, MBR/Torpig/Sinawal, Goldun, Silent Banker
Screen Grabbers		Screen contents, including keystrokes entered and all data displayed are harvested and forwarded to the criminal's data center on demand.	Totally Unaware	ZEUS/WSNPoem, MBR/Torpig/Sinawal, Goldun, Silent Banker
Clipboard Stealers		Whenever data is copied by the user with CTRL + C or Print Screen the contents are harvested and forwarded to the criminal's datacenter on demand.	Totally Unaware	
Internet Cache Riffing		Data stored in the Internet Browser cache or in the form stored input cache are harvested and forward to criminal's data center on demand.	Totally Unaware	ZEUS/WSNPoem
Man-in-the-Browser		Browser Add-ons, Helper Objects, Scripts and Injected code are used to harvest data entered or displayed by the browser and forwarded to criminal's data center on demand.	Totally Unaware	ZEUS/WSNPoem, MBR/Torpig/Sinawal
DNS Poisoning	<a href="http://www.TheBank.com">Http://www.TheBank.com</a>  <a href="http://www.CrimeInc.com">Http://www.CrimeInc.com</a>	The mechanisms for translating a web site URL to the appropriate IP address of the web site are modified to connect the user with the criminal's data center pretending to be the bank or intended site the user wanted to visit.	May arouse suspicion	DNS Changer, Trojan Bancos



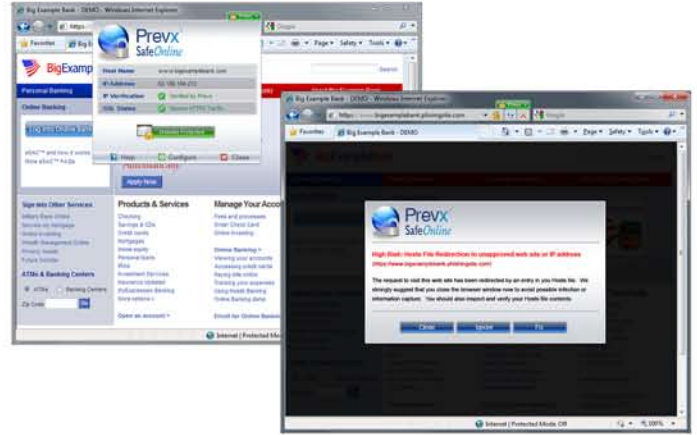
**Prevx**<sup>®</sup>  
SafeOnline

# Fighting Cybercrime

**Prevx SafeOnline provides class-leading protection against banking Trojans, phishing and other web centric attacks even if a PC is infected by malicious software.**

Prevx SafeOnline operates as a powerful incremental layer of defense, which independently hardens the operating system and internet browser environment to prevent new or undetected malware from being able to read, access, or relay user and session credentials, keystrokes, and screen contents. It also prevents Form Injection, Phishing, DNS Poisoning, Proxy and other attempts to re-direct the user to fraudulent websites.

Prevx SafeOnline incorporates an innovative and highly flexible Graphical User Interface (GUI), which is barely noticeable unless a threat exists that necessitates user action. When such a threat occurs, for example, if the user is attempting to enter their banking logon details in to a phishing website, then the GUI presents the user with a clear view of the threat and guides them to safety with simple clear options.



In addition to the powerful protection features of Prevx SafeOnline it can also provide a powerful security intelligence capability via the management console, which receives real-time feeds of new phishing and malicious URLs, domains and poisoned DNS servers from a wide variety of partner feeds which supplement powerful heuristics in offering class-leading protection.

## Layered Protection is Essential for Maximum Protection

**As an incremental layer, Prevx SafeOnline also includes real-time malware detection, incorporated from the acclaimed Prevx 3.0 anti-malware product. It is a very user-friendly and effective solution in response to current and future malware. It has a simple user interface and ultra fast silent scanning, which is able to detect even advanced rootkits. It has real-time access to Prevx's instantly updated infection database to ensure that scans are run against the latest threat information.**

Combining both products will significantly boost overall protection. Unlike Prevx SafeOnline, and similar products in this category, when a threat is identified by the anti-malware product it is totally neutralized and removed from the system. The anti-malware product may also be optionally invoked before or during a banking logon session. Unless the scan finds malicious software that represents a serious threat then the customer experience is completely unaffected.

Usability is a key focus of Prevx products and Prevx SafeOnline is no different. Minimal user interaction is required to complete the rapid installation and configuration of Prevx SafeOnline, which can be completed in less than a minute. Also, it has a small user footprint on a web browser, which provides the assurance of website security while not interfering with the user experience.

Prevx provides a comprehensive layered 'defense in depth' approach and, used in combination, Prevx SafeOnline will protect the Internet banking session from new or unidentified Trojans while the anti-malware module ensures the removal of kernel level threats. The Prevx solution is always shipped as a full product including all modules and takes the form of an 830kbyte download. The Prevx solution provides both financial institutions and consumers with the confidence that they have effective, layered and class-leading security protection.

Prevx SafeOnline was independently tested by Immunity Inc, the world leaders in security and vulnerability testing, to test how effective it was at combating today's industrial grade banking Trojans like: ZEUS/WSNPOem, MBR/Torpig/Sinowal, Goldun, Silent Banker, plus Immunity's highly renowned 'CANVAS' exploit engine. The test results reported that Prevx SafeOnline was successful in preventing modern Trojans and credential stealers from targeting Immunity's usernames, passwords, and other information when installed.

Online Banking Fraud		How Prevx SafeOnline Protects		
	Vector	Protected	Method of Protection	Benefits
Phishing Attacks		✓	Prevx SafeOnline prevents unintentional exposure of banking credentials to any web site that has not been explicitly approved, and verified in advance by the user.	Whenever a user attempts to enter protected banking or credit card credentials into a web site that has not been pre-approved, the web site address is added to the suspicious list.
Keystroke Loggers		✓	Prevx SafeOnline builds a 'private tunnel' directly between the keyboard input and the Internet Browser which cannot be viewed by other processes.	Defeats keystroke loggers and malicious processes harnessing benign applications to read keystroke input.
Screen Grabbers		✓	Prevx SafeOnline hides the screen contents and display buffer from any process not essential to the web session.	Defeats screen grabbers and malicious processes harnessing benign applications to read screen contents.
Clipboard Stealers		✓	Prevx SafeOnline hides the clipboard contents from any process not essential to the web session.	Defeats Clipboard stealers and malicious processes harnessing benign applications to copy the clipboard contents.
Internet Cache Rifting		✓	Prevx SafeOnline protects the internet and web forms cache from any process not essential to the web session.	Defeats Internet Cache Rifting malware by preventing access to the internet and web forms cache.
Man-in-the-Browser		✓	Prevx SafeOnline intrusion and extrusion engines protect the Browser process and memory from plug-in and injected code trying to assert control over the browser process and session contents.	Defeats pre-existing and new zero-day malware attacks on the Browser process.
DNS Poisoning	<a href="http://www.TheBank.com">http://www.TheBank.com</a>  <a href="http://www.CrimeInc.com">http://www.CrimeInc.com</a>	✓	Prevx SafeOnline detects Hosts file, Proxy and poisoned DNS attacks and centrally verifies ultimate DNS resolution against 'proven' DNS Services.	Defeats local DNS contamination attempts instantly and catches external DNS poisoning with centralized verification and provides immediate protection to subsequent users.