Combatting Today’s Financial and E-Commerce Threats

Overview

» Cybercriminals focus on finance and e-commerce providers and their users.

» Users are the weakest link. Social engineering tactics steal company and personal data.

» Traditional security cannot keep up with the volume, variety and velocity of today’s threats.

» With our unique approach, Webroot® keeps users safe anywhere and on any device.

» Webroot delivers advanced online fraud prevention for PCs and mobile devices.

» Webroot offers lightweight, powerful and interoperable solutions for banks looking to protect themselves and their customers from banking malware and internet attacks.

Introduction

The impact of today’s organized cybercrime is felt across the financial and e-commerce sectors the world over. As more people access financial services and accounts from personal devices, service providers and their users have become the primary targets for online fraud. Gartner research shows that more than 50% of online attacks are aimed at users of financial and e-commerce services. That research confims that people continue to be the weakest link in the security chain, and predicts that distributed denial of service (DDoS) and criminal social engineering scams, such as spear phishing, have reached new levels of prevalence and deviousness. Every day, newer and more inventive scams trick people into handing over their financial and personal information, while the security industry fails to provide effective solutions to these problems.

Big Data and the Webroot® Intelligence Network (WIN)

At more than 60 million unique variants per year, the volume, variety, and velocity of malware flooding the internet and the numerous ways in which we connect to it is staggering. The only way to keep up is to leave traditional methods behind and analyze huge data sets in real time in the cloud, then use this data to not only detect, but predict and prevent attacks.

Big data lets us discover malware as soon as it tries to infect a user, and then protect all other users against such attacks without the hassle of time-consuming signature updates. The Webroot Intelligence Network (Figure 1) integrates billions of pieces of information from multiple sources — including data from customers, test laboratories, and intelligence shared between security vendors — to create a massive malware detection net. Unique URL and IP data feeds from strategic partners further enrich our malware intelligence. Each time an endpoint is added anywhere in the world, Webroot SecureAnywhere® protection becomes more powerful and effective.

50% of online attacks target banks and e-commerce users

Gartner Research, 2013
Solutions for Financial Institutions

Financial institutions are attacked from three different angles: online and mobile banking, unsecured employee devices, and network assaults.

Banks need solutions that provide coverage across all three threat vectors. Webroot offers a portfolio of products that protect bank customers, employees, and networks.

**Advanced Online Fraud Prevention > Protecting Customers in Real-time**

Customer devices constitute a major point of weakness for a banking institution, and cybercriminals aim to compromise them. Research shows that even customers with security software installed are at risk of fraud and identity theft. The volume and sophistication of modern malware is often too complex for traditional antivirus solutions to provide adequate protection. Banks need a balanced solution that protects their customers without impacting user experience.

Our advanced online fraud prevention utilizes SecureAnywhere™ technology for PCs and mobile devices to provide a safe online and mobile banking experience. Using the industry’s smallest and fastest client technology, Webroot offers identity protection, secure browsing, anti-phishing, and credential management, even if a customer’s PC or mobile device is infected.

**Webroot SecureAnywhere® AntiVirus > Online Banking for PC and Mobile**

Banks and their customers are attractive targets for fraudsters looking to compromise customers’ devices and capture personal information. The challenge for bankers is the lack of visibility and control over customers’ computers. In addition, traditional antivirus is failing to adequately protect customers against the volume and range of threats that now exist.

Banks need to balance solutions that protect their customers but don’t negatively impact online experience. Small, lightweight, powerful and interoperable Webroot solutions are the perfect fit for banks looking to protect themselves and their customers from banking malware and internet attack.

Webroot SecureAnywhere® AntiVirus detects, removes and protects against malware on the PC in real time. Additionally, the Identity Shield secures browsing, anti-phishing and the credential protection module helps protect online banking sessions, even if the customer PC is infected.

**Features**

- Downloads and installs in seconds
- Ultra-fast scan times, first scan <2 mins, subsequent scans ~ 20 Secs
- Small footprint on the device, won’t impact PC performance
- All users are instantly protected, no configuration required and no need to download signature updates, set it and forget it
- Specializes in detecting and removing early zero day malware and targeted attacks
- Cleans infections quickly and thoroughly
- Integrated secure browsing and real-time anti-phishing
- Will work along existing security solution
- Supports multiple devices (PC, Android™ and iOS® smartphones and tablets)
- Supports multiple languages
- 24/7 online customer support provided by Webroot
Providing Webroot SecureAnywhere® AntiVirus free to banking customers or promoting this security solution has proven to be a successful strategy for progressive banks. A dramatic reduction in fraud can occur in a few weeks after the launch of the antivirus. Vulnerable users, those most prone to downloading malware, are typically early adopters. (Figure 3)

Webroot SecureAnywhere AntiVirus will run without conflict with other antivirus software since 64% of computers are infected with malware even with another antivirus installed, and 20% of computers are infected every week with malware that is missed by the users’ existing antivirus security.

**Web Access Intelligence > Online Banking Visibility**

Paired with Webroot SecureAnywhere AntiVirus, Web Access Intelligence (WAI) provides another powerful layer of defense. When Webroot SecureAnywhere AntiVirus is installed on the customers’ computer, WAI will deliver the following information:

» Who is logging in to online banking
» Which device they are using
» Whether Webroot is installed
» The security status of the device
» Whether antivirus protection is on the device and up to date
» Whether the device is infected, and what it is infected with

This intelligence allows the bank to block or restrict online banking access, or offer the customer Webroot SecureAnywhere AntiVirus to address issues and improve the security on their computer. (Figure 2)

**Mobile Security SDK Protection > Mobile Banking**

Securing mobile banking presents new challenges – less authentication, data sharing, using public Wi-Fi, downloading of third party apps, and device and data loss. Ensuring the mobile banking experience is protected without affecting the user experience is an attainable goal.

The Webroot® Mobile Security SDK is designed to embed security within a mobile banking app. No customer intervention is required. Silent, running in the background and without impacting the customer’s device, the Mobile Security SDK delivers real-time threat intelligence to the bank for instant analysis, interrogation, and action.
Additionally, the SDK includes a powerful, yet flexible, risk scoring mechanism to simplify the decision making process when assessing risks on a mobile device. Banks have the option of weighting risk scores or using the simple traffic light red-yellow-green risk assessment. Integration of the SDK into the mobile banking app is quick and easy, and can be implemented within weeks.

The Mobile Security SDK creates a unique device ID for each customer device as secondary authentication. Additional information reported includes: rooted/jailbroken status, applications running, presence of a keyboard running, if the device is running in an emulator, geo location, network information, and much more, all to assess the status of the mobile device. (Figure 4)

Mobile banking is a critical account access method for active, profitable customers. Embedding the power of mobile security into the mobile banking app provides the information banks need to manage risk.

Summary

For banking and e-commerce providers, maintaining the trust and confidence of customers and employees is critical, so providing the best possible security is paramount. Over 30 financial institutions worldwide utilize Webroot solutions to improve their online and mobile banking security, protect their customers, and gain access to critical security intelligence to mitigate fraud losses. Our cloud security solutions are designed to address the challenges of banking and e-commerce providers everywhere, ensuring that your customers, employees, and networks are secure.