# Trusteer Rapport
## Maximum Security You Can Bank On

Trusteer
an IBM Company

### The Internet: Convenient for your business, and for cybercriminals

The internet offers massive advantages, conveniences and opportunities. But with such access, various security risks are unearthed. Taking this into consideration, the bank took exhaustive steps to protect the information transmitted and processed when online banking. For example, the bank safeguards confidential data sent over the internet so that it is not retrieved or modified by unauthorized parties.

### Where is the weak link on security?

Despite these safeguards, there is one area in which the bank cannot directly protect customers from certain risks. The bank cannot directly protect customers from themselves and the way in which they use their computers. Your computer and the applications you use can expose you to potential risks.

### Antivirus: A False Sense of Security

There's something that the antivirus industry doesn't want you to know: their products aren't that effective at stopping sophisticated viruses. Studies show that **antivirus software detects only about 25% of the most popular malware** currently being emailed to people[1]. That's because the virus creators move too quickly. By the time antivirus products are able to block new viruses, it is often too late. The bad guys have already managed to tap out a business's bank account.

### Signature detection doesn't work

To identify new viruses (also known as "malware"), antivirus solutions calculate a special signature for each incoming file, and compare it to a dictionary of known virus signatures. Antivirus cannot defend against malware unless a file sample has already been obtained and signature created.

The problem is that malware authors are also very, very clever. They are able to create millions of files, each with a unique signature every month. The same malware can be masked in many different files, each with its own signature that is unknown to antivirus.

Antivirus solutions take days, sometime even weeks, to detect new financial malware signatures and remove them. However, fraud occurs hours after a new malware file with an unknown signature is released. So by the time the antivirus provider eventually cleans the computer of the malware, it may already be too late to prevent fraud from occurring.

1 KrebsOnSecurity; A Closer Look: Email-Based Malware Attacks, June 21, 2012

## The Trusteer Rapport Approach

Trusteer's innovative technology picks up where conventional security software fails. From the moment it is installed, Trusteer Rapport protects your device and mitigates financial malware infections. As long as you keep Trusteer Rapport running on your computer, it will also prevent future attempts to infect your computer. Trusteer also communicates with the bank, allowing our security team to take immediate action against changes in the threat landscape.

Trusteer Rapport doesn't look for file signatures. Trusteer Rapport doesn't bother to examine what the file is, but rather what the file does. Trusteer Rapport detects the malware installation process and breaks it – keeping the computer clean. Even if malware managed to install on the device, Trusteer Rapport detects and blocks any attempt by the malware to compromise the browser and your online banking session. By stopping the malware's bad behavior, Trusteer Rapport is able to provide protection above and beyond what is possible with antivirus. This is why the bank has chosen to partner with Trusteer to offer our customers the best protection against financial fraud.

## Extra layer of protection

Trusteer Rapport is optimized to stop financial malware and preventing financial fraud. But that doesn't mean you should discard your antivirus solutions entirely. Many other viruses exist. They will slow down your computer or interfere with your work, but they will not attempt to steal money from you. Your antivirus solutions should be used to protect you from these types of viruses.

### How Trusteer Rapport protects:

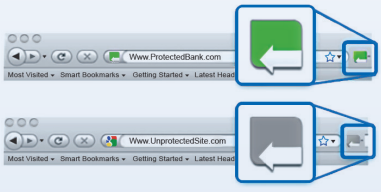
- Removes existing financial malware from the computer immediately
- Prevents future malware infections
- Protects credentials and personal information from key-logging and screen capturing attempts
- Stops phishing attacks from stealing credentials and data
- Notifies the bank of threat activity to further drive fraud prevention

### Benefits to your customer:

- Easy to install: Installation takes only a few seconds, no need to restart your computer or configure program
- Compact: Trusteer Rapport is a small piece of software that won't slow down the computer or interfere with other applications
- Automatic: Nothing for you to do, as updates are done in the background
- Effective: In a recent study, Trusteer Rapport stopped 100% of all financial malware testers used to try and infect a protected machine
- Proven: Trusteer Rapport was developed by the online security experts at Trusteer and currently protects over 30 million users worldwide
- Free: For customers of the bank Trusteer Rapport has been provided at no cost

### How you know it's working:

- Once installed, a green Trusteer Rapport icon will be displayed near (or in) the browser's address bar when you are viewing a website that is protected by Trusteer Rapport
- If the site is unprotected, a grey icon will display instead




**Trusteer, an IBM Company**
545 Boylston Street, 5th Floor | Boston, MA 02116
Tel: +1 (617) 606-7755 | Toll free: +1 (866) 496-6139 | E-mail: info@trusteer.com | www.trusteer.com

*new threats,* ***new thinking***