

What is Rapport?

Rapport is a security software application that provides online transaction protection and protection from online identity theft for consumers. You can use Rapport to safeguard your web browser sessions that include fields where private or personal information is contained. Examples include:

- Online bank accounts
- Mutual fund accounts
- Online brokerage accounts
- Email (Hotmail, Yahoo! Mail, and Gmail)
- Social networking sites (Facebook, MySpace, Orkut, and LinkedIn)
- Insurance applications
- Personal medical information
- Online merchants (eBay, Amazon, Walmart.com, and Target.com)

Rapport is entirely transparent and does not require you to change the way you work or sign-in to these websites. It does not require any configuration or maintenance - you simply install and browse safely. Rapport further protects specific identities and sessions.

Why do I need Rapport?

Did you know that 2 million legitimate websites download malware to your PC? 15,000 newly infected web pages are identified each day and 79% of them are legitimate websites that have been hacked. Even well known websites such as Google and Yahoo have been reported to serve malware to users through ads. Even if you are very careful and only visit well-known websites, malware can silently find its way to your computer.

Did you know that a recent test of “best-of-breed” anti-virus vendors and Web browser anti-phishing filters revealed that more than half of active malware and phishing threats on the Internet go undetected? The average detection rate was 37 percent for malware and 42 percent for phishing.

Did you know that one in four personal computers in the US – or 59 million – is already infected with malware?

Did you know that recent malware can silently record keystrokes, capture screen images and steal confidential financial information from your computer?

Rapport's protection is based on a revolutionary technology that is entirely different from the technologies used by other desktop security solutions. Rapport protects your username, password, and other sensitive login information and prevents malware and fraudulent websites from stealing this information. Rapport also protects your online communication and prevents malware from tampering with your electronic transactions (for example, transferring money from your bank account to the attacker's bank account).

What is the user experience?

Download and installation is very simple. In a few mouse clicks, or less than 30 seconds, Rapport can be installed and running on your desktop. You do not need to register, you do not need to type anything or submit information and you do not need to restart your browser or reboot your computer.

When you browse to a website in Internet Explorer or Firefox, the Rapport icon appears next to the browser's address bar.

The icon is green when Rapport is protecting your communication with the website:



And the icon is grey when the communication is not protected:



Rapport comes preconfigured to protect certain websites who are working directly with Trusteer to give their valued customers the best protection possible.

Of course, you should have Rapport protect you on all websites where you login or where you can read or send sensitive information. You can add Rapport protection to any website with just two clicks. With Rapport, no pre determined settings are altered, no changes are implemented, and you encounter no interference with your online activity.

When Rapport identifies a security hazard, it usually neutralizes the threat without having to inform you. In a few cases where Rapport detects some level of risk, the program may require a confirmation (i.e. Yes/No) from you before neutralizing the threat.

Why do I need Rapport if I have other security solutions?

Conventional solutions, such as anti-virus software, anti-spyware software, personal firewalls and anti-phishing toolbars, rely on a list of known bad behaviors (a.k.a. signatures, heuristics, and black lists). These solutions are becoming less effective for financial fraud and identity theft, and targeted attacks that use new, sophisticated techniques that go undetected by conventional desktop security solutions. These attacks are considered the most dangerous, and have pose the biggest risk of causing you serious financial damage.

Rapport's protection is based on a revolutionary technology that is entirely different from the technologies used by conventional desktop security solutions. Rapport protects your username, password, and other sensitive login information and prevents malware and fraudulent websites from stealing this information. Rapport also protects your online communication and prevents malware from tampering with your transactions (for example, transferring money from your bank account to the attacker's bank account).

Do I still need anti-virus if I install rapport?

Yes. Rapport does not replace your antivirus and is not an antivirus solution. It works differently and prevents attacks that your antivirus solution cannot detect or remove, including malware. Antivirus and Rapport are two complementary security layers and Trusteer recommends using both for maximal protection.

Does Rapport store or send any information about me?

Rapport creates an encrypted signature of your credentials on your computer. This information cannot be used to retrieve your credentials and is used by Rapport to identify any unauthorized leakage of your credentials. Rapport sends **anonymous** reports about security events and internal errors to a central server. This information is used to improve the product and the policy. You can specifically instruct Rapport not to send out any information.

How is Rapport different from my top-notch internet security suite?

Rapport is very different from other Internet Security suites. An Internet Security suite consists of databases of malicious software and hostile websites which it uses to detect and remove threats from your computer. Internet Security suites' vendors constantly look for new malicious software and hostile websites in order to update their databases.

Rapport uses a completely different technology. It can tell when you are accessing your bank's website and can also tell when you are executing transactions, submitting login information, and reading sensitive bank statements. During that time, Rapport applies access control layers around your sensitive information and prevents malicious software and hostile websites from accessing or tampering with your sensitive information and transactions. An unauthorized access attempt, such as an attempt to read your password, or alter your transactions, is immediately blocked. **Rapport's access control policies are set by BankFIRST.** Banks that work with Trusteer build and maintain policies that define which information is sensitive and which operations on this information should be restricted. Unlike Internet Security Suites, Rapport does not need to maintain a database of malicious software and websites and can therefore block new threats and "under the radar" threats which Internet Security suites are not yet aware of.

BankFIRST and Trusteer work hard to keep Rapport effective against financial crimes that are currently targeting online bankers.

How exactly does Rapport protect me?

Rapport protects you against the following threats:

Keylogging

A Keylogger is a malicious software that resides unnoticed inside your computer. The keylogger records keystrokes (i.e. each time you type something on the keyboard) and then sends this information to the attacker. By grabbing your sign-in credentials and other sensitive information and sending them to the attacker, keyloggers enable the attacker to sign into your accounts. Rapport encrypts your keystrokes and prevents keyloggers from reading sensitive information.

Malicious Browser Add-ons

Browser add-ons (e.g. toolbars, BHOs, plug-ins) control everything that happens inside your browser. A malicious add-on is capable of reading sensitive information such as your sign-in credentials and passing them to the attacker. It can also generate transactions on your behalf, such as transferring money from your account to the attacker's account. Rapport prevents unauthorized browser add-ons from reading sensitive information and tampering with your transactions.

Malicious Programs

A malicious program can connect to your browser and control everything that happens inside your browser. Such a program is capable of reading sensitive information (such as your sign-in credentials) and passing them to the attacker. A malicious program can also generate transactions on your behalf, such as transferring money from your account to the attacker's account. Rapport prevents programs from connecting to the browser, reading sensitive information and tampering with your transactions while you are logged into protected websites.

Screen Shooting

This malware takes screen shots and sends them to the attacker. Screen shots can include your account details, balance, and even credentials, if the website uses keypads in the login page. Rapport prevents taking screen shots while you are connected to protected websites.

Session Hijacking

This malware steals your session parameters with a specific website and sends this information to the attacker. These session parameters can then be used by the attacker to take over your session with the website and to bypass the authentication process

that is required to log into the website. Rapport prevents access to session parameters while you are connected to protected websites.

Phishing

A phishing attack is when the attacker builds a website that looks exactly like a website you know and trust (for example www.bankfirst.com). The attacker then convinces you to visit this website (for example by sending you a fraudulent email). When you arrive at the fraudulent website you mistakenly believe that this is the real website. As soon as you try to sign-in to this fraudulent website, the attacker grabs your sign-in credentials and can now use them to access the genuine website on your behalf.

To protect you against phishing attacks Rapport learns the password (and sometimes even the username) you use with protected websites. Rapport then warns you each time you use the password or the username on a different website. Using this warning you can immediately understand that you are on the wrong website and prevent the password from being submitted.

Pharming or DNS Spoofing

A pharming or DNS spoofing attack is when the attacker causes your computer to go to fraudulent website each time you type a real website's address in the browser's address bar. The attack achieves this using various techniques such as infecting your desktop with malware or by compromising servers in your ISP's network. Once you arrive at the fraudulent website and try to sign in, the attacker grabs your sign-in credentials and can now sign into the genuine website on your behalf. To protect you against pharming attacks Rapport verifies the IP address and the SSL certificate of the website each time you connect to a protected website. If the verification fails, Rapport terminates the connection and establishes a new connection to the real website.

Which attacks does Rapport protect against?

Rapport protects you against the following attacks:

Phishing

A phishing attack is when the attacker builds a phony website (the phishing site) that looks exactly like a website you know and trust (for example your bank's website). The attacker then lures you to visit the phishing website (for example by sending you a fraudulent email). When you arrive at the phishing website you mistakenly believe that this is the real website. As soon as you try to sign into the phishing website, the attacker grabs your login credentials and can now use them to login to the real website, impersonate you and initiate fraudulent transactions.

Pharming

A pharming attack is when the attacker causes your computer to go to fraudulent website each time you type a real website's name in your web browser address bar. The attack accomplishes this using various techniques such as infecting your desktop with malware or by compromising servers in your ISP's network. Once you arrive at the fraudulent website and try to sign in, the attacker grabs your login credentials and can now use them to login to the real website, impersonate you and initiate fraudulent transactions.

Keyloggers

A Keylogger is malicious software that hides itself inside your computer. The keylogger records keystrokes (i.e. each time you type something on the keyboard) and then sends this information to the attacker. By grabbing your sign-in credentials and other sensitive information and sending them to an attacker, keyloggers enable an attacker to login to your accounts, impersonate you and initiate fraudulent transactions.

Man in the Middle

Man in the middle is an advanced variation of Phishing and Pharming attacks. In this particular attack you sign into the website and start working all the while entirely unaware that all the information exchanged between you and the website is passing to the

attacker. The attacker can view any private information and can alter your transactions. For example, if you request to transfer a certain amount of money to a specific payee, the attacker can change the payee's identity and have the money transferred to a different account.

Man in the Browser

"Man in the Browser" is malware that resides inside your browser in the form of an add-on (e.g. toolbar, BHO, browser plug-in). This malware controls everything that happens inside your browser. It is capable of reading sensitive information such as your sign-in credentials and passing them to the attacker. It can also generate transactions on your behalf, such as transferring money from your account to the attacker's account.

Screen Capturing

This term refers to malware that takes pictures of your computer screen and sends them to the attacker. Screen shots can include your account details, balance, and even credentials when the website uses keypads for login.

Session Hijacking

This term refers to malware that steals your session parameters with a specific website and sends this information to the attacker. These session parameters can then be used by the attacker to take over your session with the website and to bypass the authentication process that is required to log into the website.

Is Rapport hacker-proof?

Unfortunately, no security solution is hacker-proof. Rapport adds a very important and unique security layer that allows BankFIRST to better protect your sensitive information and promptly react to threats aimed directly at you. With Rapport, you are more secure and your bank has better mechanisms to protect your money. Security is a constant battle and Rapport, as your antivirus solution or any other security product you use, makes it harder for criminals to commit crime.

What is the difference between Rapport and SSL?

Rapport and SSL are complementary protection layers, performing different internet security duties. SSL protects the information flowing between you and the web site you are browsing, by encrypting the communication channel you use. SSL protects communication and runs on both your computer and the site you are browsing. Rapport prevents identity theft, which can be done regardless of the security of your communication channel (i.e. even if SSL is used). Rapport protects your sensitive personal information, and runs only on your computer.

Who is Trusteer?

Trusteer enables online businesses to establish a secure communication tunnel with their customers over the Internet that stretches from user's keyboard into the company's website. Trusteer's flagship product, Rapport, allows online banks, brokerages, retailers, and healthcare organizations to protect their customers from identity theft and financial fraud. Trusteer is a privately-held corporation founded by senior Internet security industry executives with specific expertise in enterprise and consumer desktop security. Trusteer is well-financed by U.S. Venture Partners. In 2008, Trusteer won the "Best of Web" award from the Online Banking Report and was covered by U.S. analyst firms Gartner and Frost & Sullivan.