

TRUSTEER, INC.'S RAPPORT FAQ

How does my computer get infected by malware or other malicious software?

- It is possible that computers can be infected via many methods including:
 - A malicious individual intentionally installed a Trojan or other malicious software
 - A user of the computer was tricked into installing the software believing that they were installing some piece of "necessary" software
 - The computer was already infected with a different piece of malware (often known as a "dropper") and that other piece of malware installed the software or Trojan
 - If the computer's patches were out of date the computer could have been exploited either by visiting a malicious website, or by being attacked by a malicious or infected computer

How can I protect myself from fraudulent attacks on my computer?

1. Install Trustee, Inc.'s Rapport browser protection software. Rapport helps you secure your browser from malware attacks and fraudulent websites. Rapport's innovative technology picks up where conventional security software fails.
2. Update your PC's Malware protection software frequently. Strengthen your online security by keeping your protection software, such as anti-virus software, and your web browser version updated.

What is Trustee's Rapport?

- Rapport is a security software application that provides online identity theft and online transaction protection. You can use Rapport to help protect your web browser sessions with any website that contains private or confidential information. Examples include:
 - Online bank accounts
 - Investment accounts
 - Email
 - Online merchants such as eBay or Amazon

Rapport is entirely transparent and does not require you to change the way you sign into online applications or how they work. It does not require any configuration or maintenance; you simply install and browse safely.

Why do I need Trustee's 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 behavior (a.k.a signatures, heuristics, and black lists) and fraudsters. While they are important, Rapport adds an additional layer of security that protects you internet session.

Rapport's protection is based on new technology that is different from the technologies used by current desktop security solutions. Rapport helps protect your username, password, and other sensitive login information and prevents malware and fraudulent websites from stealing this information. Rapport also helps protect your online communication and prevents malware from tampering with your transactions, (e.g., transferring money from your account to the attackers account).

How is Trustee's Rapport different from my top-notch Internet Security suite?

- Rapport is different from Internet Security suites. Internet Security suites consist of databases of malicious software and hostile websites which they use to detect and remove threats from your computer. They constantly look for new malicious software and

hostile websites in order to update their databases. In contrast, Rapport applies access control layers around your sensitive information and helps prevent malicious software and hostile websites from accessing or tampering with your non-public information and transactions. Unauthorized access attempts, such as attempts to read your password, or alter your transactions, are immediately blocked.

Do I still need my anti-virus if I install Trusteer's Rapport?

- Yes. Rapport does not replace your anti-virus and is not an anti-virus solution. It works differently and prevents attacks that your anti-virus solution cannot detect or remove. Anti-virus and Rapport are two complementary security layers and we recommend using both for maximum protection.

Which attacks does Trusteer's Rapport help protect against?

- Phishing – this is when the attacker builds a phony website (the phishing site) that looks exactly like a website you know and trust. The attacker then lures you to visit the phishing website via tactics like sending you a fraudulent email. As soon as you try to sign into the phishing website, the attacker grabs your login credentials and can then use them to log into the real website, impersonate you and initiate fraudulent transactions.
- Pharming – happens when the attacker causes your computer to go to a fraudulent website each time you type a real website's name in your web browser 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 log into the real website, impersonate you and initiate fraudulent transactions.
- Keyloggers – this is a 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 login 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 – this 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" – this 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.
- Session 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.

Does the download take a long time?

- It is very simple to download Trusteer's Rapport protection software. A few mouse clicks and Rapport can be installed and running on your desktop in approximately 30-seconds. 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. With Rapport, no pre-determined settings are altered, no changes are implemented, and you encounter no interference with your online activity.

How do I know Trusteer's Rapport software is monitoring the website?

- After you have successfully downloaded the Rapport software, you will see a green Rapport arrow at the far right of the address bar when you go to Amegy Bank's website. The green of the arrow tells you that the website is protected with Trusteer's Rapport software.
- You can easily add Rapport protection to other websites you visit. Simply follow the steps outlined below:
 - Go to the website you would like to protect
 - You will notice the Rapport arrow at the far right of the address bar is gray
 - Left click on the gray Rapport arrow
 - A dialog box appears – left click on the large orange arrow that says 'Protect this Website'
 - The Rapport arrow is now green, which lets you know it is now protected
 - Trusteer's Rapport will automatically monitor your future visits to that site.
 - *This may vary based on your Internet Browser

Which operating systems and browsers are supported by Trusteer, Inc. for the Rapport protection software?

- Trusteer, Inc. currently supports Windows XP, Windows Vista, and Windows 7 running Internet Explorer 6, 7, 8 or Firefox 2 or 3. The list of operating systems and browsers is subject to change without notice.
- Trusteer's Rapport software is not available for Macintosh computers at this time.

Is Trusteer's Rapport hacker-proof and does it make my computer hacker-proof?

- Unfortunately, no security can protect against all risks. Rapport adds a very important security layer that better protects your sensitive information, your accounts and promptly reacts to threats aimed directly at you. However, security is a constant and changing battle. Rapport, your anti-virus solution, and any other security product you use, make it harder for criminals to commit crime.

Who is Trusteer?

- Trusteer, Inc. is a privately held corporation founded by senior internet security executives with specific expertise and consumer desktop security. 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. Additional information can be found by visiting Trusteer, Inc. at <http://www.trusteer.com/company>.
- Amegy Bank of Texas has contracted with Trusteer, Inc. to allow its clients to download its Rapport security solution. Trusteer's Rapport product helps protect clients who install the service from identity theft and financial fraud when conducting business online.

Trusteer's Rapport software is a product of Trusteer, Inc., made available for free to customers of Amegy Bank of Texas. Amegy Bank of Texas and Zions Bancorporation are not affiliated with Trusteer, Inc., and they do not provide, warranty, or guarantee the content, service or operation of Trusteer Rapport. By downloading and installing Trusteer's Rapport, you agree with Trusteer, Inc. to the terms and conditions of the Trusteer's Rapport end user agreement. Any problems, concerns or questions regarding Trusteer Rapport should be directed to Trusteer, Inc. at support@trusteer.com.