HomeTrust Bank

Business Connect Online Security Best Practices

For protection against cyber-crimes and account high jacking

Businesses of all sizes are being targeted for cyber-crime on almost a daily basis. Financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. Organized crime groups are believed to be responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.

If You Become a Victim...

In the event you become a victim of fraud, there are a number of immediate steps that should be taken to help protect your financial interests:

Immediately cease all activity from computer systems that may be compromised. Unplug the Ethernet or cable modem connections to isolate the system from remote access.

Immediately contact your financial institution so that the following actions may be taken to contain the incident:

- Disable online access to accounts
- Change online banking passwords
- Open new accounts as appropriate
- Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.

File a police report with the local police department and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies and banks. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

Contact your local FBI field office, https://www.fbi.gov/contact-us/field-offices or file a complaint online at www.IC3.gov.

Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.

Realize that if personal online banking has been conducted from the affected business computer system, there is the potential for identity theft. Review recommendations provided on the Federal Trade Commission's Identity Theft website.

Consider having the network and computer system reviewed by a qualified computer forensic/information security professional.

HomeTrust Bank

How you can protect yourself…

The FBI and other federal government agencies have provided the following recommendations for businesses:

Computer System Security

In order to protect the security of your accounts, HomeTrust Bank will never contact you to ask for your electronic banking credentials (e.g., login ID and password). We will never request sensitive information from you via email (e.g., Social Security number, account number, login ID or password). Never respond to requests for such information, whether solicited by email, phone, postal letter, or in person.

- All online banking activities should be conducted on a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
- Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information.
- Do not open file attachments or click on web links in suspicious e-mails as that could expose the system to malicious code that could hijack your computer.
- Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as a DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- Create a strong password with at least 10 characters that includes a combination of mixed case letters, numbers and special characters.
- Prohibit the use of "shared" usernames and passwords for online banking systems.
- Use a different password for each website that is accessed.
- Change the password a few times each year.
- Never share username and password information for online services with third-party providers.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Ensure virus protection and security software are updated regularly.
- Ensure computers are patched regularly, particularly operating system and key applications, with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
- Consider installing spyware detection programs. HomeTrust Bank offers Trusteer Rapport to our customers at no cost to them. More information is available at https://www.hometrustbanking.com/business/trusteer_rapport.php
- Clear the browser cache before starting an online banking session in order to eliminate copies of web pages that have been stored. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
- Use a secure session (**https** not http) in the browser for all online banking.
- Avoid using an automatic login feature that saves usernames and passwords for online banking.
- Never leave a computer unattended while using any online banking or investing service.
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign

on information leaving the customer vulnerable to possible fraud.
- Business Connect customers should perform a related risk assessment and controls evaluation periodically

NOTE:
Business Connect customers are not covered by the consumer protections of Electronic Funds Transfer Act, which limits consumer liability from unauthorized electronic transfers.

Account Controls
- Reconcile your banking transactions on a daily basis.
- Use dual control for ACH and wire transfers. Approval of transactions should be done by a different employee than the initiating employee, to provide proper dual control.
- For added security with wire transfers, we strongly encourage customers to use separate computers for the wire submittal and wire approval functions.
- Make use of check cashing limits and automated payment filters.

Liability
- Familiarize yourself with your online banking user agreement and with your liability for fraud under the agreement and the Uniform Commercial Code as adopted in your jurisdiction.

Communication
Stay in touch with other businesses to share information regarding suspected fraud activity. Immediately escalate any suspicious transactions to your financial institution, particularly ACH or wire transfer activity. There is a limited recovery window for these transactions and immediate escalation may prevent further loss.

Contact Us
If you notice suspicious account activity or experience customer information security related events, please contact us.

Customer service representatives are available Monday through Friday, 8:00 a.m. until 7:00 p.m. and Saturday from 9 a.m. to 3 p.m. (EST).

Phone: 855.202.0020

Email: BusinessOnline@hometrustbanking.com

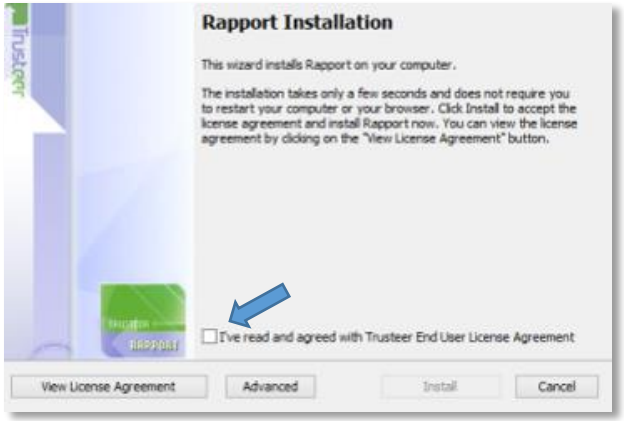
Quick Guide to Downloading and Installing Trusteer Rapport

1. Download

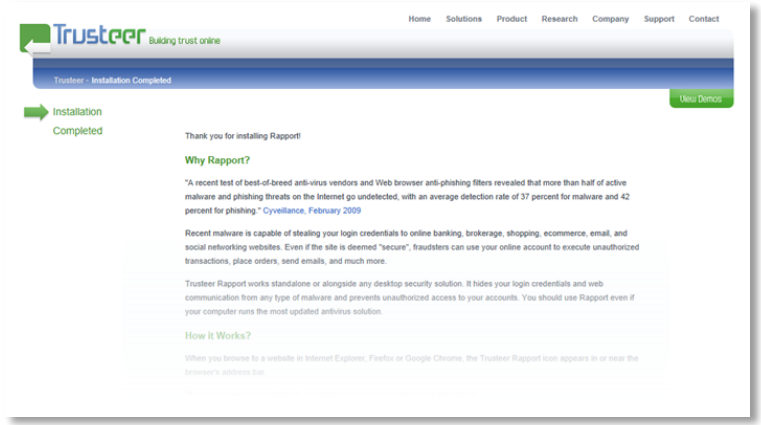
When you log in for the first time on an unregistered computer, you will see a pop-up with a download link. Click the Download Now button:

2. Install

Accept the Trusteer Rapport End User License Agreement. Follow the prompts to install Trusteer Rapport.



After successful installation, you will see a confirmation page like this:



For more information about Trusteer Rapport and how it works, visit www.hometrustbanking.com/business/trusteer_rapport.php

Quick Guide to Downloading and Installing Trusteer Rapport

(Step 2 Continued)

You may close the confirmation page and you should see the Business Connect login screen and are now ready to log in:

What is Trusteer Rapport?

- Software that a Business Connect user downloads to protect the computer and connection during the online session.

What does Trusteer Rapport do?

- Prevents Man-in-the-Browser and Man-in-the-Middle attacks
- Disables key logging and screen capturing of credentials and personal information
- Stops phishing attacks from stealing login credentials and data
- Removes and prevents financial malware from residing on the computer

Trusteer Rapport is not:

- Virus protection or Firewall

3. Post Installation

How can I tell if I am protected?

You can always be assured you are protected when the green icon is visible next to your browser's address bar, as shown above.

If Rapport detects financial Malware on the PC you will be presented with the following message:

If the above message persists even after rebooting your computer twice, please contact:

HomeTrust eBanking Support at 855.202.0020

For more information about Trusteer Rapport and how it works, visit www.hometrustbanking.com/business/trusteer_rapport.php