



Trusteer Rapport Add-On: Payment Card Protection

The explosive growth of e-commerce has enabled hackers and fraudsters to target payment card data used by consumers and businesses to conduct online transactions. Yet, lack of control over end user systems makes endpoints one of the weakest links in the protection of payment card data from malware and phishing attacks. Trusteer Rapport Payment Card Protection effectively mitigates the risk of payment card data theft.

Trusteer Protects Payment Card Data Entry at the End Point

Trusteer Rapport Payment Card Protection provides real-time detection and prevention of card number theft by financial malware and phishing sites. It provides the following capabilities:

Card Number Entry Detection and Protection

Trusteer Rapport detects the entry of card numbers by looking for BINs specified by the bank or card issuer (first 6 digits of the card number). Once a target BIN is typed in by the user, Trusteer Rapport initiates encryption of all keystrokes entered into the page, blocking key-logging malware from capturing the full credit card number.

Card Number Phishing Detection and Alerting

When a user enters credit card number into a locally stored web page or over an unsecured session (http), Trusteer Rapport issues a warning indicating that the user is about to enter sensitive data into a suspicious website. The user can choose to continue, add the site to a white list or abort the transaction.

The card issuer receives a real time alert when card number is entered into a suspicious site (the alert includes an encrypted card number and the address of the site). The fraud team can take immediate action such as cancelling the card and initiating a takedown of the phishing site. If the site is legitimate but does not follow security best practices, the card issuer can work with the site owner to mitigate the risk of card data theft.

Traditional Anti-Virus and Anti-Phishing Measures Fall Short

Anti-virus and anti-phishing solutions can't effectively protect users against financial malware and phishing attacks. It takes days or even weeks for anti-virus vendors to identify and remove new variants of financial malware. During that time, the malware is still undetected and cyber criminals can capture payment card data and conduct transactions minutes after getting end user machines infected with malware.


Anti-phishing solutions identify phishing sites only after card data theft has occurred and are unable to identify the data stolen prior to the site takedown.



Trusteer Rapport Add-On: Payment Card Protection

Trusteer Rapport: Industry-leading Endpoint Protection

Trusteer Rapport is a lightweight security solution that prevents sensitive data, such as account credentials and financial data, from being stolen from end user computers by malware and phishing attacks. Downloadable in seconds, Trusteer Rapport works in the background and doesn't change the user experience which ensures fast adoption. Trusteer Rapport can be quickly deployed by card issuers and is managed by a cloud-based application, providing visibility into malware activity across the end user base.



The image shows a payment form with the following fields: Credit Card Number, Payment Type (with logos for VISA, MasterCard, AMEX, DISCOVER, American Express, and others), Expiration Date (mm / yyyy), CVC, Country, City, State, Zip Code, and Home Telephone. A green warning box is overlaid on the form, containing the text: "Warning: It seems like you are entering payment card information into an unsecured or high-risk website. We recommend not entering card information into unsecured sites." Below the warning are two buttons: "Ignore, I trust this website" and "Get me out of this site".

Trusteer Rapport issues a warning to the user during card number entry into a suspicious site

Trusteer Rapport Add-On: Payment Card Protection Benefits

- Stops payment card number theft by zero-day malware
- Protects payment card data entry from key-loggers
- Notifies users before entering card numbers to suspicious sites
- Alerts the fraud team of card number phishing events in real time