Phantom Banking Transaction System

Data Protection Technology

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Phantom Banking Transaction System

Data Protection Technology

Overview

The updating financial industry system with Phantom Banking Transaction System, a data protection technology.

The baseline execution in protecting an operating system with a cryptoprocessor in place, as the financial industry is more vulnerable to being compromised, particularly, in the current trend of cryptocurrency. It requires current updates and/or patches to defend against such attacks.

The keystone of the security subsystem, eliminating the need to protect the rest of the subsystem with physical security measures and ensuring each system isolation within the framework of the finance industry. In additional to utilizing individually unique and auto-populated disposal firewalls, VPNs, and encryption infrastructure to ensure security. Assuring all anti-virus and configurations are current and up to date within the standard and practices.

Implementing randomized auto-penetration testing throughout the workday to ensure the responsiveness and effectiveness of the security infrastructure in place within the department. Implementing a secured shuffling server system to complete each verified financial transaction to ensure further privacy during the confidential payment process by running this encryption simultaneously but perpendicularly as a single method for every transactions.

This system would essentially create phantom transactions IDs with temporary codes that are to be assigned only at the completion of each transaction rather than standard and permanent routing numbers which can be compromised mid-transaction.

The daily reports of this process would be overseen, monitored and assessed for quality security assurance by security department. Lastly, isolating each suspicious behavior of foreign penetration attempts identified in real-time during this aggressive testing methodology.

Establishing that the financial industry has a higher risk of being compromised, it is recommended that you do not store your passwords on any of your devices, particularly mobile devices as they are often at higher risk and can be lost, man-made error. Password complexity is essential for baseline user protection. It is not recommended using birthdays, pet names or any information that can be easily retrieved by social media or from any of the various mass digital citizen directories online.

Research is key in both defense as well as for the attackers. Again, with readily user information available an attacker can obtain information by your content posted on your social media accounts or even google. Then moving on the second line of offense, social engineering, and phishing after that baseline of databases. User information can be bought and sold from dating sites and even retail, our digital footprints out there and the name of the game is data.

Anonemis Research
Simenona Martinez
AnonemisResearch.com