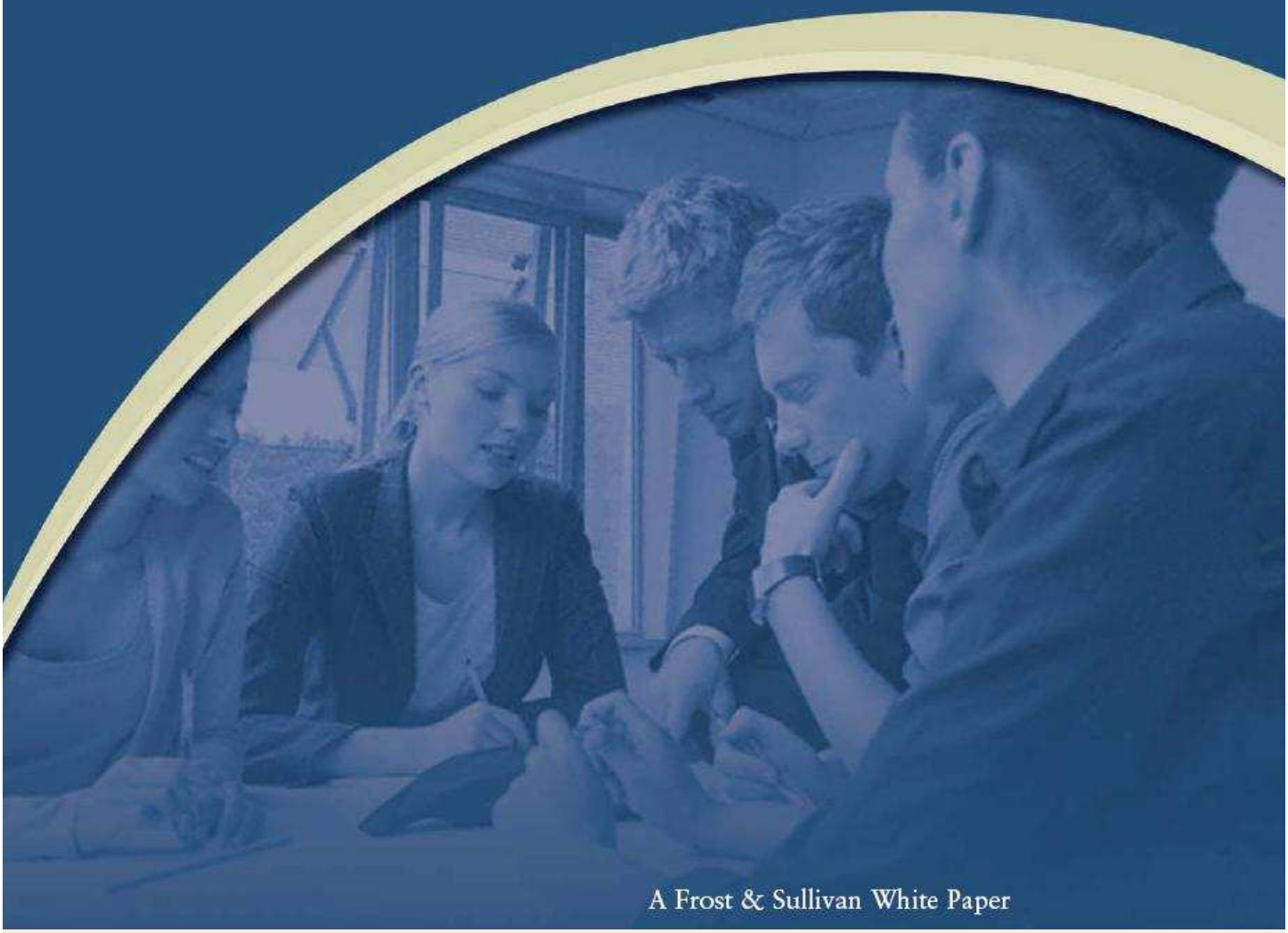
FROST & SULLIVAN

Key IT Anti-Fraud Challenges for Banking & Financial Institutions in Latin America



A Frost & Sullivan White Paper

EASYSOLUTIONS

TABLE OF CONTENTS

Latin American IT Security Markets Overview 03

Rising Internet Usage and Vulnerabilities 04

Low Threat Awareness Drives Fraud 05

Phishing: The Rising Threat 06

How Users Deal With Fraud 07

Explosive Growth in Online Fraud 08

Fraud: A Bank Responsibility 09

How to Minimize Threats 10

ABOUT EASY SOLUTIONS 11

ABOUT FROST & SULLIVAN 12

Market Overview

Network Security vendors and Managed Security Services (MSS) providers have been operating more proactively in the Latin American region since the 21st century. The region is still in a developing stage of adoption and has been experiencing strong growth rates over the past 5 years, with Compound Annual Growth Rates superior to 20%.

Despite the strong global economic recession experienced in both 2008 and 2009, the IT Security markets grew considerably in 2009. The Network Security markets grew **19.5%** and the MSS markets **25.1%**. This growth is significantly higher than the more established markets in the USA and countries in Western Europe.

One of the most important factors driving the Latin American IT Security markets in 2009 was the exponential growth in both the quantity and complexity of virtual threats. Unfortunately, the Latin American region currently hosts one of the largest and most active hacker communities in the world. The most common virtual threats include Viruses, Trojans, Malwares and Phishing attempts.

In addition, increased focus on the company's "core business" and compliance to local, regional and international regulations are also powerful drivers that leverage the growth of the Latin American IT Security markets. Examples of international compliance that have greatly affected the region in 2010 were the Payment Card Industry Data Security Standards (PCI DSS), Sarbanes-Oxley and Basel II.

On the other hand, there are still important market barriers that restrain further growth of the Latin American IT Security markets. Some of the most important include:

- lack of quantifiable return on investment (ROI) of IT security solutions
- lack of IT security budget and cultural barrier
- political and economic instability

"Companies in Latin America have been increasing their perception regarding virtual threats and consequently have invested more in IT Security over the past years."
Frost & Sullivan Latin America

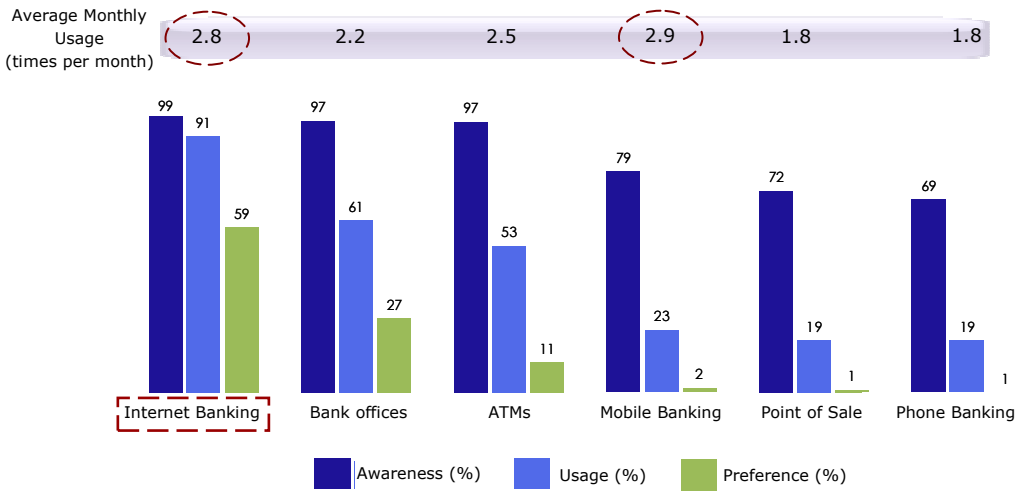
Rising Internet Usage and Vulnerabilities

The increasing penetration of Internet in Latin America is a strong driver for the usage of Internet Banking.

In 2009, approximately **20%** of households in the region already had Internet broadband capabilities. Internet banking is by far the most preferred vehicle for conducting financial transactions, with an impressive **59%** of users in Latin America preferring online transactions.

On the other hand, users have very low preference levels for conducting their financial transactions in both bank offices and ATM machines, with **27%** and **11%** preference respectively.

Latin American users' banking awareness, usage and preference



N = 375

Source: marketteam; Frost & Sullivan

When taking into consideration the frequency of use, both Internet Banking and Mobile Banking are the most used methods of online transactions.

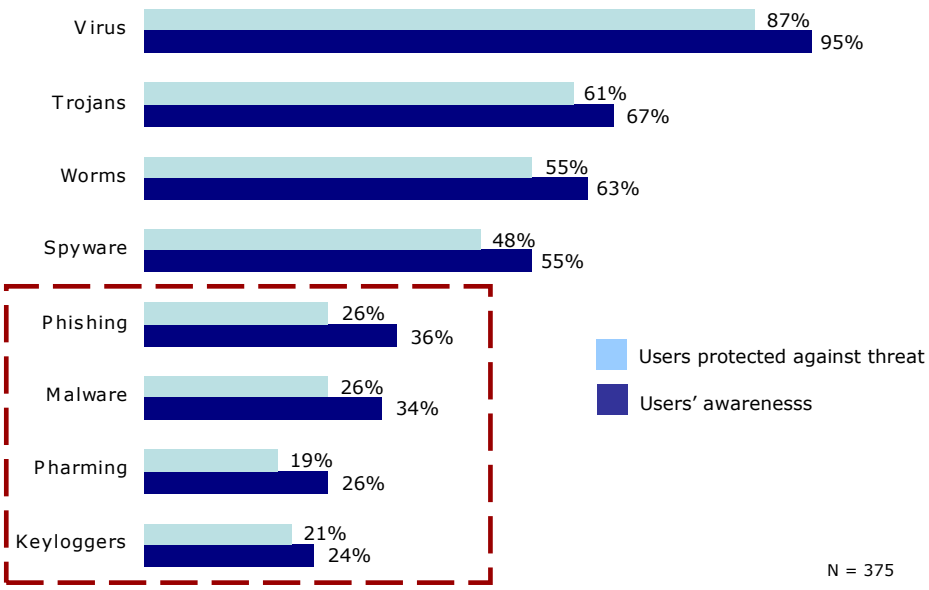
It is extremely interesting to note that **59%** of interviewees did not consider that there was a decrease in virtual threats in 2010 when compared to 2009. This clearly shows the lack of confidence Internet users have in their financial institutions and e-commerce platforms in Latin America.

Low Threat Awareness Drives Fraud

Banking services over the Internet and the increase in the workforce mobility are two strong global virtual fraud drivers. Threat awareness levels in the entire Latin American region are relatively low, particularly when compared to more developed countries. Low awareness levels result in lack of prevention solutions which in turn increases the risk of Internet fraud.

Even though more common threats such as Virus, Trojans, Worms and Spyware have higher levels of awareness, other menacing threats are still acknowledged by few.

Latin American users' virtual threat awareness and current protection levels



N = 375

Source: marketteam; Frost & Sullivan

Threats with significantly low levels of awareness and consequently even lower levels of current protection include Phishing, Malware, Pharming and Keyloggers. All of these threats have current awareness levels inferior to **40%** and current protection levels inferior to **30%**, maximizing user's vulnerabilities to virtual frauds.

The lack of awareness of dangerous IT threats is a powerful driver for the increase of fraud in both Internet Banking and E-commerce platforms.

Phishing: The Rising Threat

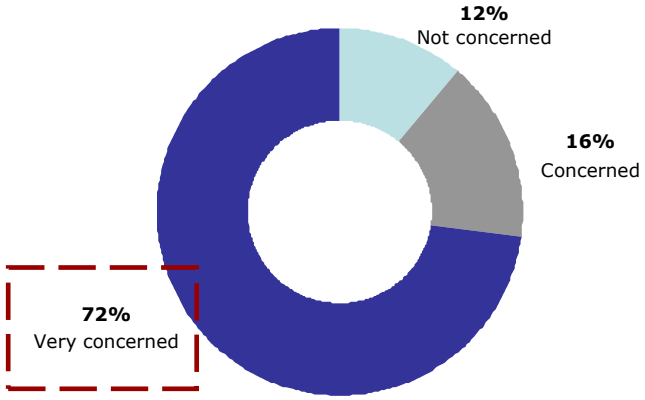
The Problem

Phishing is currently one of the most dangerous virtual threats in Latin America. It is a criminal, fraudulent mechanism which uses the Internet to acquire susceptible personal information, such as usernames, passwords or credit card details by masquerading as a reliable business website or electronic communication.

A common mistake is to think that phishing attacks occur only via email. Phishing attacks have also been occurring through other means of communications, the most common being via telephone and short message services (SMS).

Virtual criminals are increasingly creative and have been using popular social networks, important news events, celebrities and financial institutions in order to lure their victims. Furthermore, banks and financial institutions in Latin America are more and more suffering from sophisticated and evolved Phishing attacks such as Pharming and Malware.

Latin American users' concern regarding Phishing atacks



N = 375

Source: marketteam; Frost & Sullivan

When explained the definition of Phishing attacks, **72%** of Latin American users became extremely concerned regarding the privacy of their confidential information. Users who know little about Phishing attacks and who do not have Anti-Phishing solutions in place are at constant risk whenever online.

Anti-Phishing solutions as well as authentication services have experienced high growth rates in the Latin American region in 2010, particularly driven by the Financial & Banking vertical.

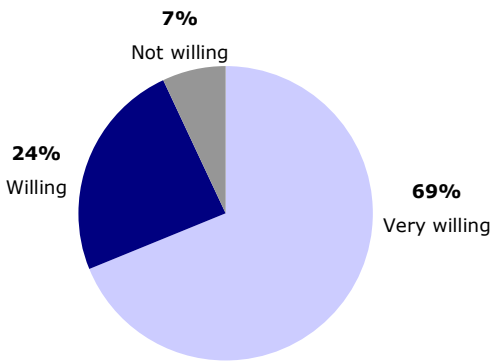
How Users Deal with Fraud

***22%** of users of online transactions in Latin America have stopped using online banking, and **10%** have changed their bank due to fraud incidents.*

An impressive **95%** of users of online transactions believe their banks should implement more robust security solutions in order to minimize the risks of fraud. It is also interesting to note that **89%** expect transaction monitoring from their banks to detect malicious activities.

In parallel, **69%** of users are very willing to use optional security solutions, and only **7%** disapprove additional security measures.

Willingness of users of online transactions in Latin America to use additional security measures



N = 375

Source: marketteam; Frost & Sullivan

Top 5 User Reactions to Online Fraud:

- Only accesses websites users are accustomed to
- Only uses e-commerce websites they are accustomed to
- Checks for Security Certificates on websites prior to online shopping
- Decreased or ceased shopping online
- Ceased to execute online financial transactions

Source: marketteam; Frost & Sullivan

Even though identifying that websites have Security Certificates prior to online transactions is a user reaction to Fraud issues, only a relatively **small percentage** of online transaction users in Latin America do so.

Even though the majority of users are willing to implement additional security methods, **47%** are not willing to pay an additional charge, as they consider their banks responsible for their online security.

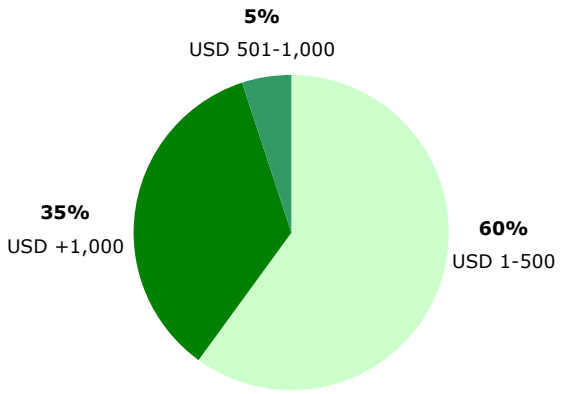
Banking Frauds on the Rise

Most Common Frauds in Latin America in 2010
Credit/Debit card cloning
E-commerce related frauds
Phishing
Fraudulent transactions involving ATMs

Source: Frost & Sullivan

The cloning of both credit and debit cards was the most common fraud in Latin America in 2010, followed by virtual frauds including online shopping. Unauthorized online shopping is becoming an increasingly common phishing attack within users of online transactions. In addition, there has been a sharp increase in fraudulent transactions involving **ATMs**.

Latin American Frauds by individual value in 2010



Source: marketteam; Frost & Sullivan

If we analyze the frauds that occured in Latin America in 2010 in depth, we can conclude that **35%** involved sums superior to $1,000 USD. The average fraud in Latin America was a substantial $941 USD.

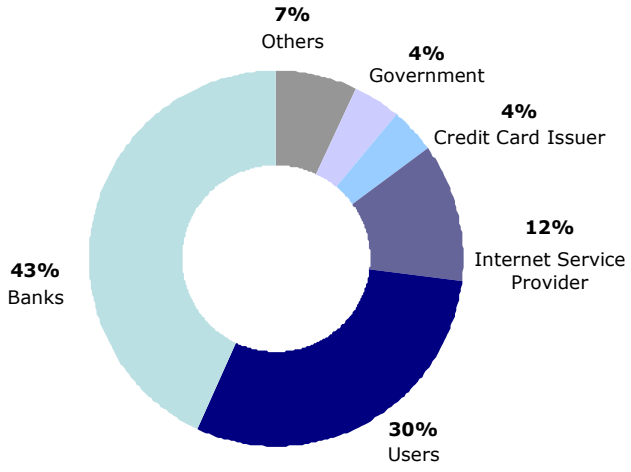
8% of users of online transactions in Latin America stated that they suffered from at least 1 fraud attack in the last 12 months. This number is potentially much higher as a large amount of frauds are not detected by users due to lack of attention on credit cards and banking bills.

Fraud: A Bank Responsibility

*It is interesting to note that **59%** of users blame online service providers, such as banks, ISP and credit card issuers, for online frauds.*

43% of users in Latin America consider banks as the main entity responsible for securing electronic transactions. Because users bestow their trust in banks for all of their financial transactions, banks are in the spotlight whenever there is electronic fraud.

Fraud responsibility according to Latin American Users



N = 375

Source: marketteam; Frost & Sullivan

Not only the banks are to blame

30% of Latin American users view themselves as responsible for virtual fraud. In addition, Internet Service Providers, the enabler of the Internet connection, are also considered responsible for **12%** of the fraud. Credit Cards and the Government should also help create a safer online environment, according to Latin American users.

How to Minimize Threats

E-commerce and Internet Banking stakeholders should invest in effective proven technologies such as Multi-Factor Authentication and Managed Security Services specialized in Fraud Protection.

Banks should inform their users on how to have a more proactive approach towards identifying potential virtual threats. They should empower clients with the knowledge to ensure they can minimize the risk of frauds. In order to do so, banks and other online shopping stakeholders must constantly invest in network security solutions and managed security services specialized in fraud prevention and detection.

Key Technologies to minimize virtual frauds
Multi-factor authentication solutions or professional services
Individual real-time transaction analysis
Proactive anti-phishing and anti-pharming services
ATM malware monitoring

Source: Frost & Sullivan

Authentication services are expected to grow approximately **28%** in terms of revenues in 2010, mainly driven by the Banking, Finance and Government verticals. Authentication is considered as one of the most effective preventive solutions to growing threats such as Phishing and online Identity Theft.

Other extremely powerful IT Security solutions include real-time and individual transactions analysis, website certifications and 24x7 ATM monitoring.

Security measures such as tokens, passwords sent via SMS and web-site authentication images are also used by financial institutions. Unfortunately **more than half** the users of online transactions in Latin America do not trust these security methods. The most effective solutions includes a variety of authentication solutions, a truly strong **multi-factor authentication approach**.

"The top Financial Institutions in Latin America are partnering with innovative IT Security providers in order to minimize the vulnerability of their own clients."
Frost & Sullivan Latin America

About Easy Solutions

Easy Solutions is the only technology security vendor focused exclusively on Fraud Protection, providing multi-channel solutions against Phishing and Pharming, Multi-factor Authentication and Risk Based Transaction Qualification.

Easy Solutions' Total Fraud Protection Strategy is the state of the art in fraud prevention and a unique differentiator in the industry. Easy Solutions delivers a holistic view of fraud management across different transactional channels and at any stage of the fraud incident.

• Detect Monitoring Service (DMS): 24/7 real time monitoring to rapidly identify, shut down and recover from Phishing attacks. DMS' proactive approach stops a Phishing attack even before it is launched.

• Detect Safe Browsing: Pharming and Phishing protection at the end user's computer level to avoid re-direction to fake websites.

• Detect ID: Multi-factor/multi-channel authentication combined with malware detection and end-user policy enforcement.

• Detect TA: Multi-channel fraud protection solution that provides real time qualification at the transactional level based on the user habits profile.

• Detect ID Web Authenticator: Strong authentication solution that controls the access to critical applications.

Easy Solutions' team works closely with leading financial enterprises and industry leaders in other security disciplines supporting a wide range of heterogeneous platforms.

Easy Solutions is a member of the Anti-phishing Working Group (APWG) and ABA (American Banker Associations). For more information, please contact us at info@easysol.net.

EASYSOLUTIONS

EASY SOLUTIONS

Headquarters:

1401 Sawgrass Corporate Parkway, Sunrise, FL 33323 Phone: +1-866-524-4782

Latin America:

Calle 93A No. 14 – 17 Of. 506 Bogota, Colombia Tel. +57 1- 236 2455

www.easysol.net

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages over 45 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 35 offices on six continents. To join our Growth Partnership, please visit www.frost.com.