EASYSOLUTIONS

Views of Latin American Consumers on Electronic Fraud – 2013

Customer Usage, Awareness, and Attitudes Regarding Electronic Fraud and Protection Methods

Summary: For the fourth year running, Easy Solutions has conducted a research study with consumers from all over Latin America to find out their perceptions and behavior regarding electronic fraud, security methods, and educational campaigns related to those topics.

The findings of this study provide a useful reference point for financial institutions and electronic service providers in the region, especially in relation to the implementation of security and communications technology aimed at the users of online banking and other electronic channels.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1

This report provides an analysis and evaluation of the data we collected on the views, attitudes and knowledge of Latin American consumers towards electronic fraud. Data was collected through a series of telephone interviews conducted in a variety of Latin American countries earlier this year.

> *Key Findings:*

Fear of fraud is the main factor inhibiting the use of the Internet as a transactional channel, but it is possible to change users' perceptions about security with the delivery of additional security measures, accompanied by educational materials about how to use those measures effectively.

Online and mobile banking continue to increase in usage and preference, while branch offices and ATM machines continue to fall out of favor. The rapid adoption of internet-connected tablets and smartphones reflects the great potential of these new channels.

40% of those interviewed don't remember any campaigns that their bank has conducted about electronic fraud. The knowledge of electronic threats like phishing, pharming and malware is still low, and the ongoing prevalence of these threats must also be addressed by bank educational campaigns.

For users, banks are the main parties responsible for electronic security, and it is expected that banks will provide secure authentication and transaction monitoring.

The use of strong authentication methods is still limited, and should be accompanied by education to improve user perceptions about security when using online banking.

One in three users say that they have installed some kind of protection on their computer other than an antivirus, which shows a willingness on the part of users to utilize these kinds of solutions.

Banks can play a more proactive role in incentivizing the use of anti-malware technology at the end-user level to prevent phishing, MITM and MITB attacks.

A multi-layered protection strategy is more necessary than ever to combat widespread user password recycling and to protect user data and money from theft.

EXECUTIVE SUMMARY

1

> *Recommendations:*

Banks should continue delivering additional security tools to users, accompanied by education, in order to:

Grow their user base, and increase the use of the Internet and other electronic channels that are less expensive to manage than physical branch offices.

Enhance the effectiveness of and strengthen trust in electronic transaction methods.

Combat economic losses and preserve their good reputations, which can be irreparably damaged by fraud.

ABOUT THE STUDY

2

As the only security provider focused on electronic fraud prevention and detection, Easy Solutions is at the forefront of research regarding the constantly evolving nature of electronic threats. Our innovative products and services are based on the dynamic needs of the web fraud detection market, offering protection against phishing, pharming, malware, MITM and MITB attacks, as well as solutions related to multi-factor authentication, safe browsing, and transactional risk qualification. With the suite of products and services that make up the company's Total Fraud Protection Strategy®, Easy Solutions is able to provide state-of-the-art fraud prevention that delivers a comprehensive view of fraud management and mitigation across different transactional channels and at all stages of a fraud incident. The information technology research and advisory firm Gartner has included Easy Solutions in its Magic Quadrant for Web Fraud Detection, in the "Visionaries" section of the quadrant. According to Gartner, "Visionaries have innovative research and development, a good understanding of their markets and solid strategies that poise them for healthy growth".

Easy Solutions is proud to present the fourth annual installment of its "Views of Latin American Consumers on Electronic Fraud" study, based on consumer research with users from Mexico, Central America, the Caribbean, the Andean nations, Brazil, and the Southern Cone. The study aims to find out the knowledge, opinions and attitudes of Latin American consumers with regard to the threats they face when using online and electronic banking and payment channels, and discover consumer views about what financial services providers and online retailers are doing or should be doing to keep their electronic transactions safe. These results are one of the information sources that help to shape the products and services of the Total Fraud Protection® strategy, and provide a reference point for the electronic security strategies and educational campaigns of financial institutions in the region.

> *Technical Profile:*

-Target Population: Over 20 years old and complete online transactions at least once a month
-Regions: Central America and the Caribbean (Costa Rica, the Dominican Republic, and Panama), the Andean Region (Colombia, Venezuela, and Ecuador), the Southern Cone (Chile and Argentina), Mexico, and Brazil.
-Weighted Average: The data was not weighed.
-Margin of Error: +/- 5% overall, +/- 11% by region, 95% confidence level, n=440
-Study Period: Telephone polls conducted in May-June 2013
-Provider: Mystery Shopper

PAYMENT CHANNELS: USAGE AND PREFERENCES

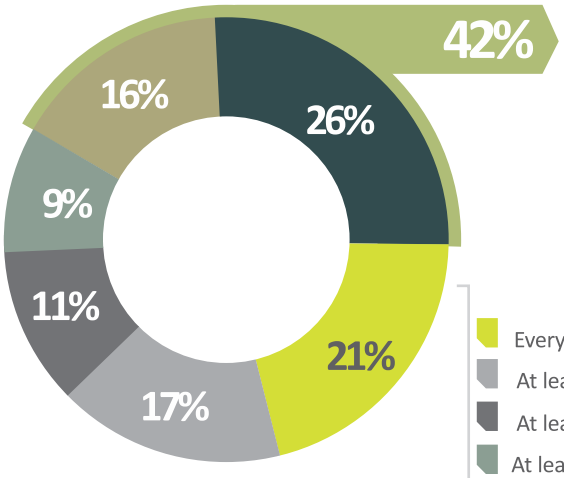
3

> Fear of Fraud is the #1 Reason More People Don't Use Online Banking

In addition to analyzing the views and opinions of those who regularly use the Internet for banking and shopping, it is also important to examine those users who don't use the Internet for anything related to finance or commerce. As incredible as it may seem in this day and age, a whopping 42% of the people we contacted over the age of 20 don't regularly use the internet for making transactions or purchases, with 26% never using the Internet for this purpose at all.

The main reason these users cited for not utilizing online banking services was fear of electronic fraud. More than half of those who don't use Internet banking services mentioned that they don't trust the platform in some way. However, online banking portals are more convenient for customers to use and incur fewer expenses for banks in their day-to-day operations than physical branch offices. Financial institutions that promote further adoption of electronic channels among their customer base have the potential to further minimize operational costs while improving service delivery to their clients. Therefore, fighting against fraud is not only vital for preventing economic losses and protecting a bank's reputation; it is also essential for staying competitive and ensuring a financial institution's future growth.

> Frequency of Internet Use for Banking Transactions, Payments, or Purchases



Overall number of people contacted (Over 20 years old): 770

How often do you use the Internet to make banking transactions, check your account balance, pay for services, pay taxes, or make any other payment or purchase?

Why don't you use the Internet for banking transactions, payments or purchases more frequently?

- Fear of electronic fraud or robbery/It doesn't seem safe	38%
- Don't trust that the transaction will be performed correctly	17%
- Don't have access to a computer or the Internet	10%
- Don't know how to use a computer or the Internet	11%
- Because it costs extra to use this channel	9%
- Don't have a credit card	9%
- The bank doesn't have an Internet portal for transactions	6%
- Don't have a bank account	21%

PAYMENT CHANNELS: USAGE AND PREFERENCES

3

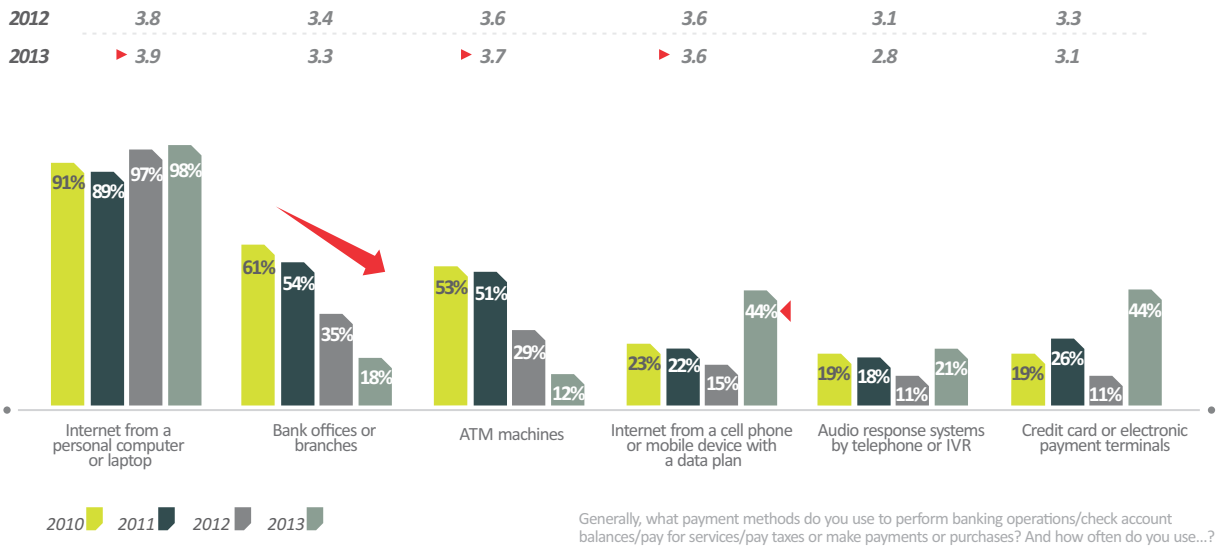
> *Mobile and Online Banking are Rapidly Replacing Branch Offices and ATM Machines*

In Latin America, users are increasingly turning to the Internet and mobile channels to perform transactions and make payments and purchases. Growth in the use of mobile Internet in particular exploded from only 15% last year to 44% this year, while usage of physical branch offices and ATM machines is in free fall.

Credit card and electronic payment terminals also showed a marked increase from last year, with 44% of respondents using them for banking transactions. Coupled with the large decrease in the use of ATM machines, we can infer that consumers are increasingly taking cash out of their transactions entirely, managing their accounts from the Internet and using a credit or debit card for payments at retail outlets.

The Internet remains the most frequently-used channel. Online banking users utilized the channel an average of 3.9 times a month, with 65% performing some kind of transaction online at least once a week.

> *Monthly Frequency of Use*



Generally, what payment methods do you use to perform banking operations/check account balances/pay for services/pay taxes or make payments or purchases? And how often do you use...?

PAYMENT CHANNELS: USAGE AND PREFERENCES

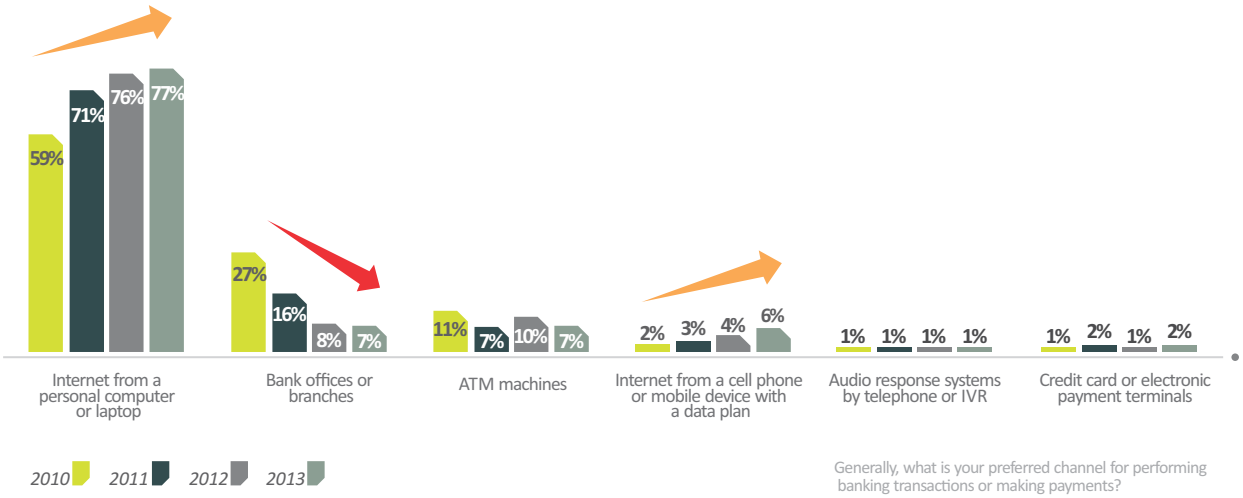
3

> The Internet Remains the Most Preferred Channel for Banking and Payments

The rise of Internet and mobile banking at the expense of branch offices and ATM machines is even starker when respondents were asked which channel they prefer to use. The Internet was the preferred channel for performing banking transactions and making payments by an overwhelming margin. 77% of those interviewed named the Internet as their favorite channel for these purposes.

The comparatively low preference for using mobile channels for transactions and payments as compared to the Internet, even when taking its greater convenience into account, suggests that there is a still a lot of room for this channel to grow.

> Preferred method for banking transactions or payments in general



Generally, what is your preferred channel for performing banking transactions or making payments?

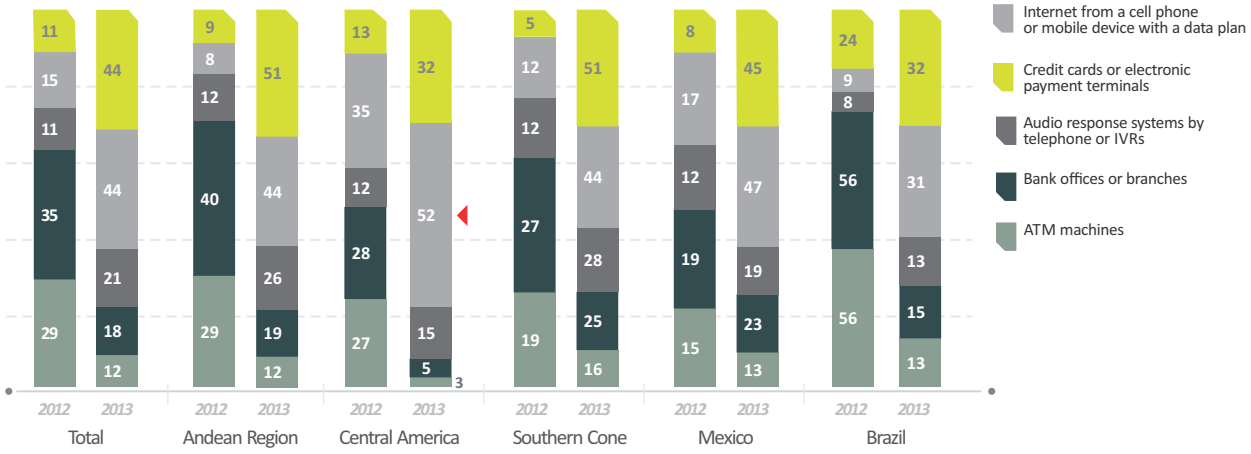
THE POTENTIAL OF MOBILE BANKING

4

> *Mobile Banking on the Rise All Over Latin America*

Growth in the use of mobile Internet is happening everywhere in Latin America. In the region as a whole, the employment of mobile as a payment channel nearly tripled. Central America is the region in Latin America with the highest use of mobile payment, at 52% of internet banking users, as well as the lowest reported use of branch offices, at a paltry 5%. Every region in Latin America also showed a marked decrease in the use of ATM machines, and all regions except Mexico also registered a large drop in the use of branch offices, which suggests that mobile is eating into the usage of these traditional channels.

> *Use of payments methods and channels*



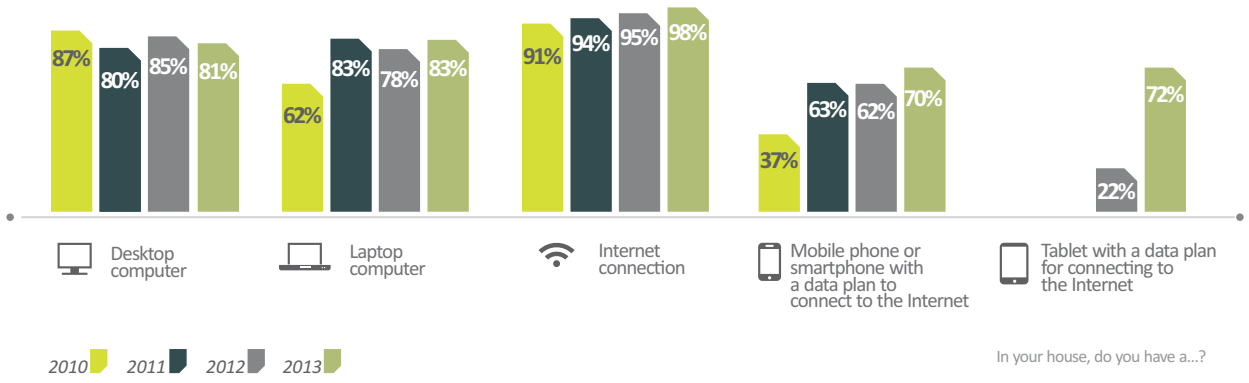
> *Tablets: Explosive Growth, Easy Internet Access*

The tablet mobile device, a gadget that did not even exist until 2010, is already in the homes of 72% of all Latin American online banking customers. This is more than triple the amount from last year. Tablet possession has already surpassed smartphone ownership, and tablets are poised to overtake desktop and laptop computers as the most common household device within the next year or two.

THE POTENTIAL OF MOBILE BANKING

4

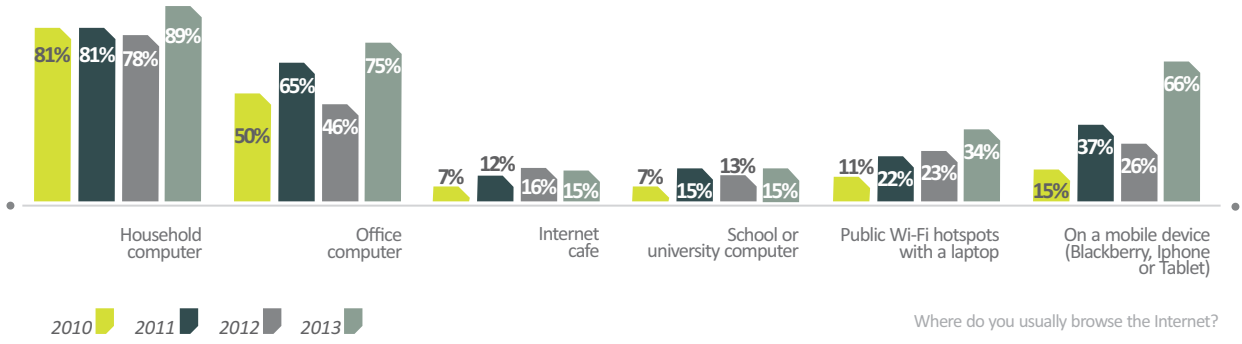
> Trends in devices for accessing the Internet



In your house, do you have a...?

> More People are Connecting to the Internet from Mobile Devices

The household computer is still the number one choice for accessing the Internet, followed by the office computer. But the amount of respondents accessing the Internet from a mobile device more than doubled from last year. Not so long ago you had to be connected through a cable or at least located near a wireless hotspot to access the Internet, but the physical limitations to Internet access are receding as mobile broadband becomes more popular. While smartphones and tablets offer unparalleled convenience by allowing users to perform banking transactions and make purchases from anywhere, they also pose new security challenges that must be confronted by financial institutions and online retailers as these devices become more ubiquitous.



Where do you usually browse the Internet?

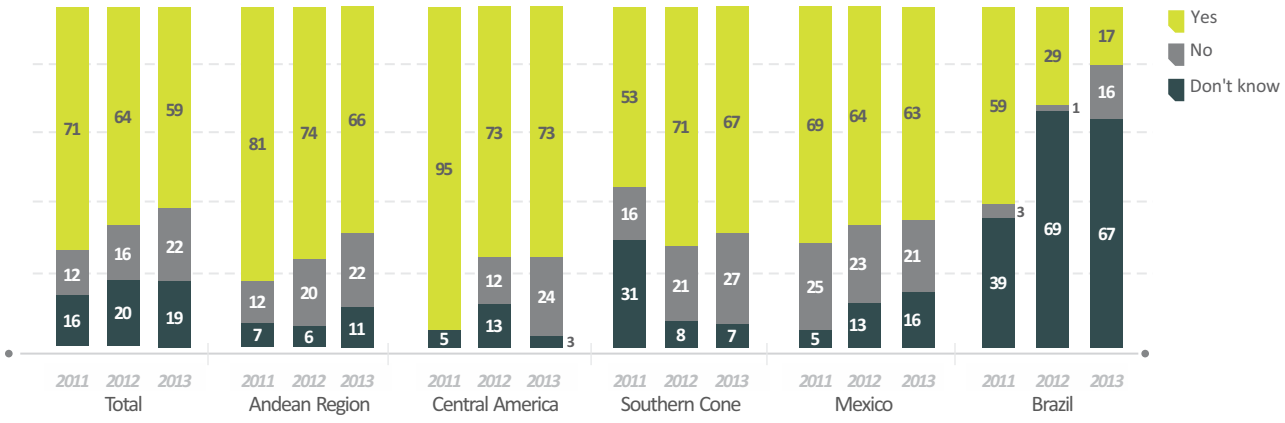
AWARENESS OF EDUCATIONAL CAMPAIGNS AND THREATS

5

> *Educational Campaigns Need Enforcement, Especially in Brazil*

Although the majority of users know that their bank conducts educational campaigns about electronic fraud prevention, about 40% of users in the region are not familiar with these kinds of initiatives. Awareness is even lower in Brazil, where a meager 17% of users have any idea about such campaigns. More alarmingly, the awareness of educational campaigns decreased or stayed flat compared to last year in every part of Latin America.

It is essential that financial institutions reinforce and remain steadfast in their educational strategies to decrease the amount of fraud victims and improve the perception of security surrounding online banking and other electronic channels.



Does your bank conduct educational campaigns to warn and teach their users to protect themselves against electronic fraud?

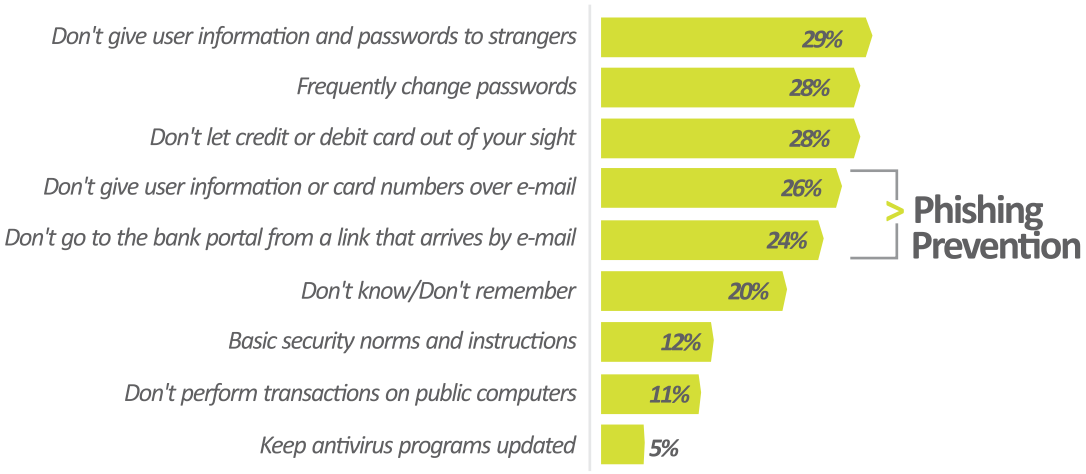
> *Users Are Aware of Campaigns against Phishing*

Campaigns against phishing have generated some awareness; users mainly remember prevention campaigns offered by their banks focused on changing passwords frequently and not using e-mail links to access bank portals. Still, 20% of those who recalled that their bank conducted educational campaigns could not remember anything about the content of those campaigns. Banks still have some work to do in getting their users to recall and apply the messages they want to convey in their campaigns so that they are more effective and easier for users to retain.

AWARENESS OF EDUCATIONAL CAMPAIGNS AND THREATS

5

> Types of Educational Campaigns Conducted by Banks



What were the topics of your bank's campaigns?

Responses per person: 1.8

> Perceptions about Improvements in Internet Security are Polarized

Opinion is divided on whether security for online transactions and purchases has improved over the course of the past year; 59% of those interviewed feel that security has remained the same or worsened.

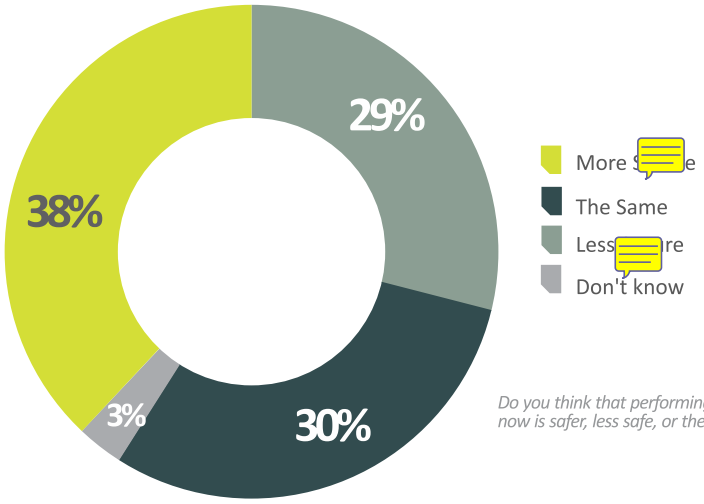
When asked if they were anxious about theft happening on various kinds of Internet portals, users overwhelmingly said that they were very worried about it. Users were concerned the most about virtual banking portals, with 83% of respondents saying that possible theft on these websites worried them a lot. Large majorities also worried about some kind of robbery occurring on government, healthcare and social networking websites.

Since fear of being a victim of fraud is the main reason that users are reluctant to utilize the Internet as a transactional channel, it is imperative to teach users to protect themselves against any online threats, and to be alert for any activity that seems suspicious.

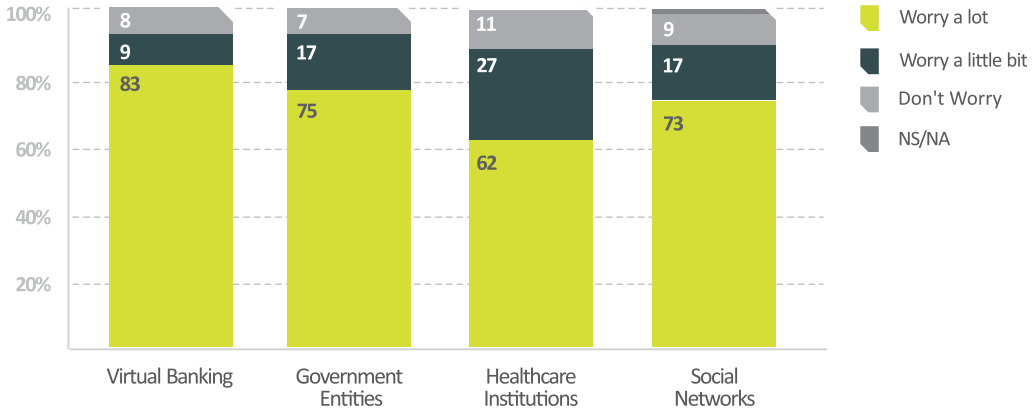
AWARENESS OF EDUCATIONAL CAMPAIGNS AND THREATS

5

> *Perceptions on How Security Has Evolved During the Past Year*



Do you think that performing transactions on the Internet now is safer, less safe, or the same as one year ago?



How much do you worry that your confidential information might be stolen on websites or portals related to...?

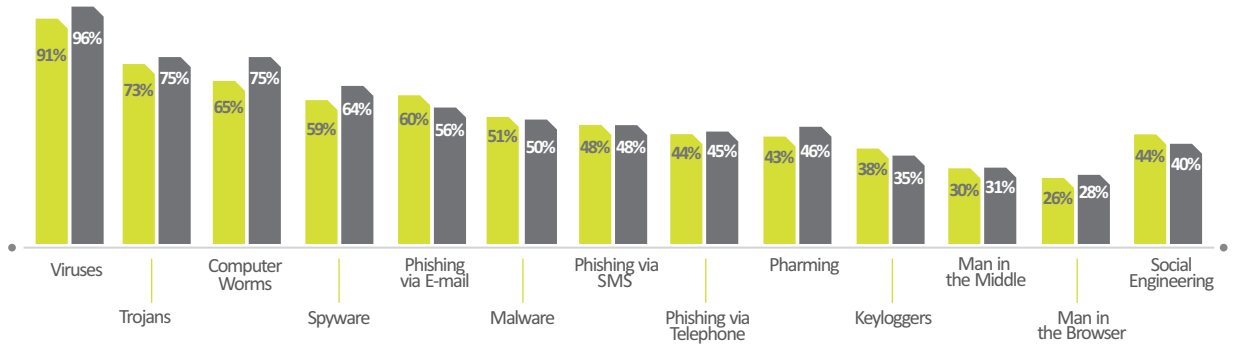
AWARENESS OF EDUCATIONAL CAMPAIGNS AND THREATS

5

> Users are Still Unaware of a Dizzying Array of Threats

There is still a widespread lack of knowledge and awareness related to common electronic threats in Latin America. While a large portion of users are familiar with dangers such as viruses and Trojans, only about half of users know about online threats like phishing, pharming and malware. More sophisticated threats like social engineering, man-in-the-middle and man-in-the-browser attacks are only known by a third of online users. Knowledge of threats like phishing, malware and keylogging software actually decreased from the previous year, suggesting that some reinforcement about these topics in future educational campaigns might be useful.

> Knowledge of Electronic Threats



Now, I am going to read some of the threats that you could be exposed to when performing a banking transaction or making a payment or purchase online. Please tell me if you have heard of the following:

> The Large Gap between Awareness and Seeking Protection

Awareness of the threats facing online transactions is only one piece of the anti-fraud puzzle. Many users who know about particular threats have not taken any actions to protect themselves against them. The vast majority of users don't have protection against malware, which exposes them to robbery of their credentials and pharming, MITM, and MITB attacks. Almost half of those who have heard of pharming, MITM, and MITB attacks have no protection against these threats, signifying a very large gap between awareness and action that leaves users vulnerable to fraud. These figures indicate that there is a great need to educate users about how to protect themselves against different forms of electronic fraud and to provide them with the tools they need to do so, putting greater emphasis on those that are less known and therefore potentially more dangerous.

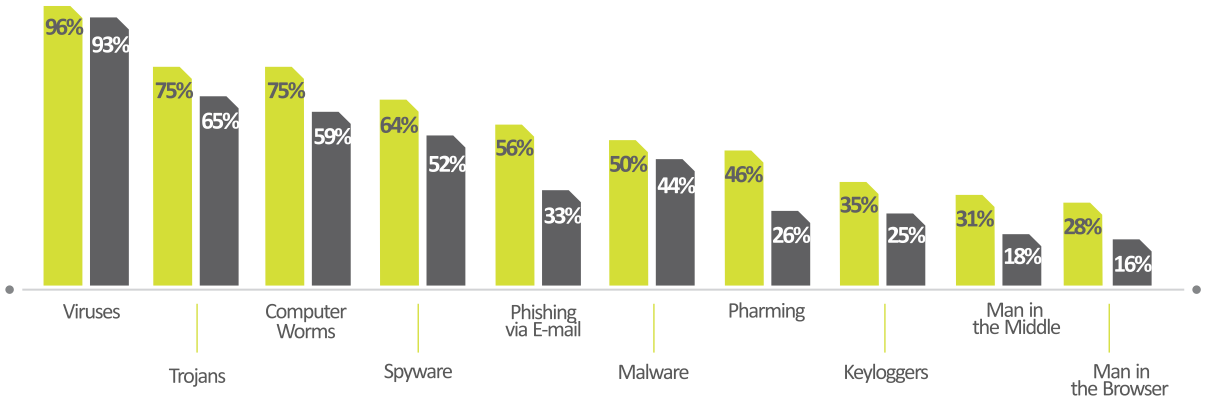
AWARENESS OF EDUCATIONAL CAMPAIGNS AND THREATS

5

> Threat Awareness vs. Protection

> The gap between awareness and protection:

2012	11%	21%	21%	20%	38%	17%	40%	29%	47%	45%
2013	3%	13%	21%	19%	41%	12%	43%	29%	42%	43%



Know about the threat

Have protection against it on their computer

I am going to read to you a list of threats that you might be exposed to when performing a banking transaction, making a payment or shopping on the Internet. Please tell me if you know or have heard of any of the following threats, and whether you have protection against them...

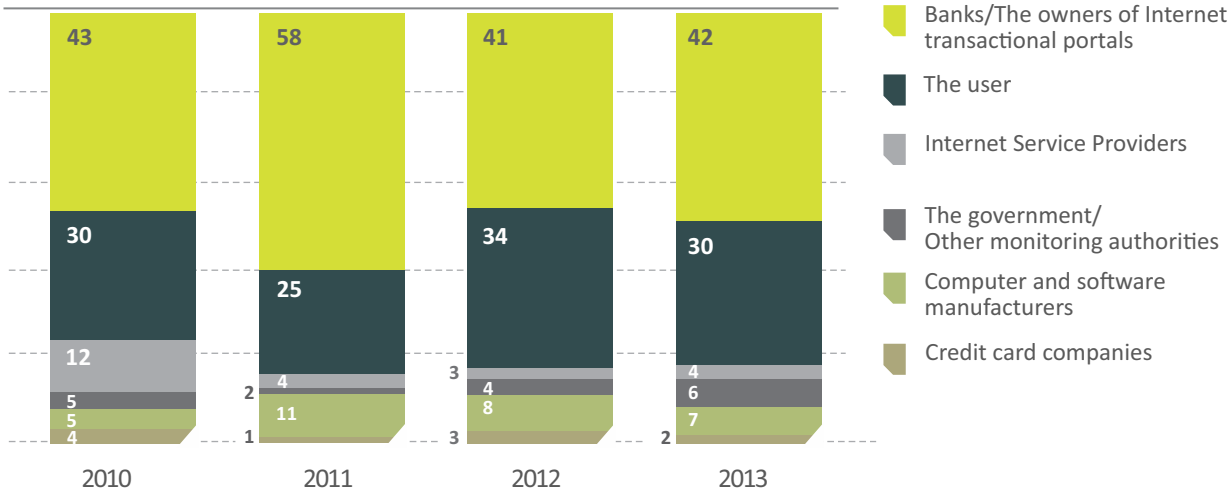
RESPONSIBILITY FOR FRAUD

6

> *Latin American Users See Banks as the Main Party Responsible for Electronic Security*

42% of online banking users think that banks should shoulder the most responsibility for the security of electronic transactions. The users themselves are in second place for accepting responsibility with 30%, followed by computer and software manufacturers.

> *Responsibility for Fraud*



In terms of electronic fraud, who do you think is primarily responsible for ensuring that electronic transactions are secure?

> *Customers are Trying to Protect Themselves*

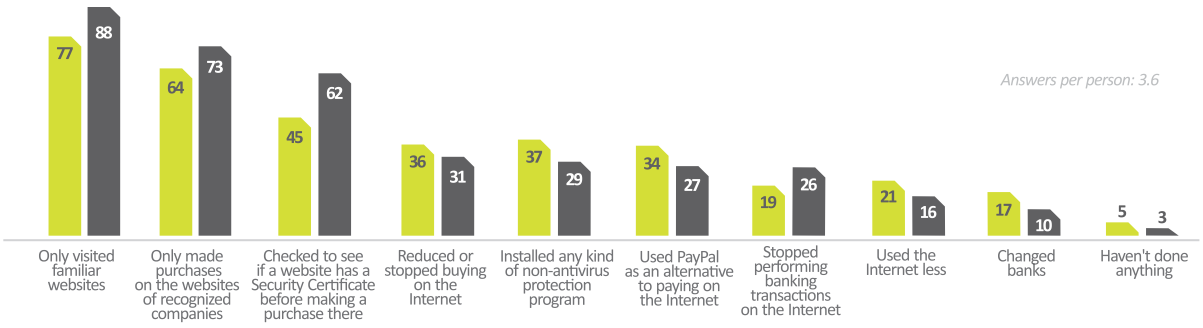
One of every three of those interviewed said that they have installed some kind of protection program, other than an antivirus, to protect against electronic fraud. This shows that users are willing to employ these kinds of programs.

Users have been much more eager to make simple behavioral changes aimed at reducing vulnerability to fraud. The top actions taken as a protective measure against fraud were to only visit familiar websites, only make purchases on well-known websites, and verify that websites have the proper security certificate. All of these modest, uncomplicated techniques for avoiding fraudulent websites increased in popularity from last year, which suggests that users find them easy to incorporate into their normal browsing behavior.

RESPONSIBILITY FOR FRAUD

6

> Personal Actions Taken for Protection

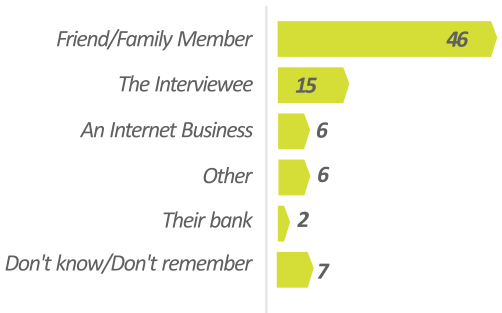


Some people have taken certain actions to protect themselves against fraud or robbery on the Internet. Have you taken one of the following actions?

> Many Customers Have Installed Anti-Fraud Programs that They Don't Understand

While 29% of those interviewed installed a protection program (apart from antivirus) on their device because someone they know recommended it or through their own initiative, one-third of those who have installed such a program don't really know what kind of security it provides. Usually, the user installed this program on the advice of a friend or family member. Without professional guidance, it is possible that these users could fall victim to deceptive programs that may not offer any protection whatsoever or even be a disguised form of malicious software. Banks can and should play a more proactive role in encouraging the use of these kinds of solutions that protect against malware, and MITM and MITB attacks.

> Program Recommendation:



Who recommended the protection program that you installed on your computer?

Do you know which threat the program you installed on your computer protects against?

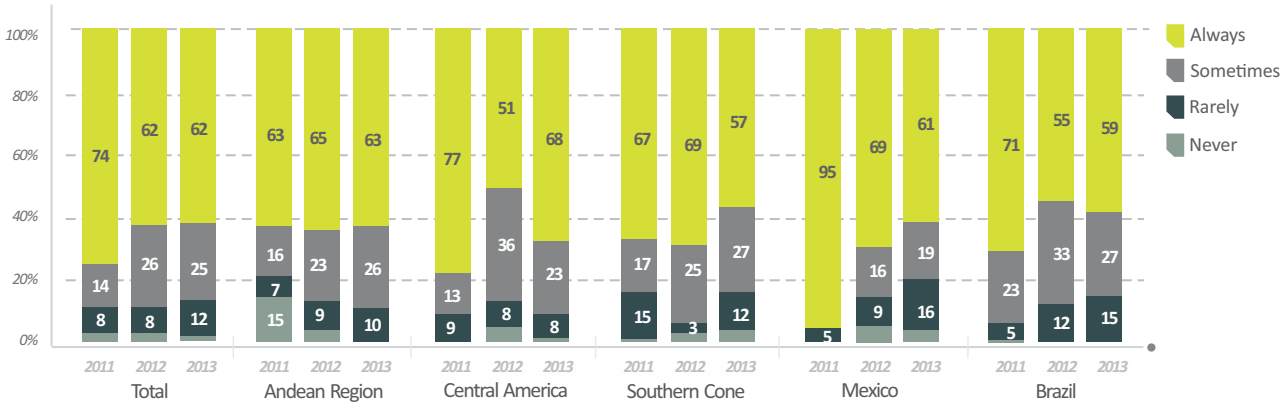
RESPONSIBILITY FOR FRAUD

6

> *Simple Behavioral Changes Can Also Help Prevent Fraud*

Another simple action that users could take to reduce vulnerability to fraud is to habitually check their bank account and credit card statements for any possible illegitimate transactions. Almost 40% of users are not accustomed to revising the status of their bank accounts and/or credit cards, even though it is a straightforward and effective method for detecting fraud. Emphasizing how crucial it is to go over financial statements on a regular basis is an essential message to convey in any anti-fraud campaign conducted by a financial institution.

> *Checking Bank/Credit Card Statements*



Are you accustomed to checking the reported transactions on your banking and/or credit card statements in detail?

RESPONSIBILITY FOR FRAUD

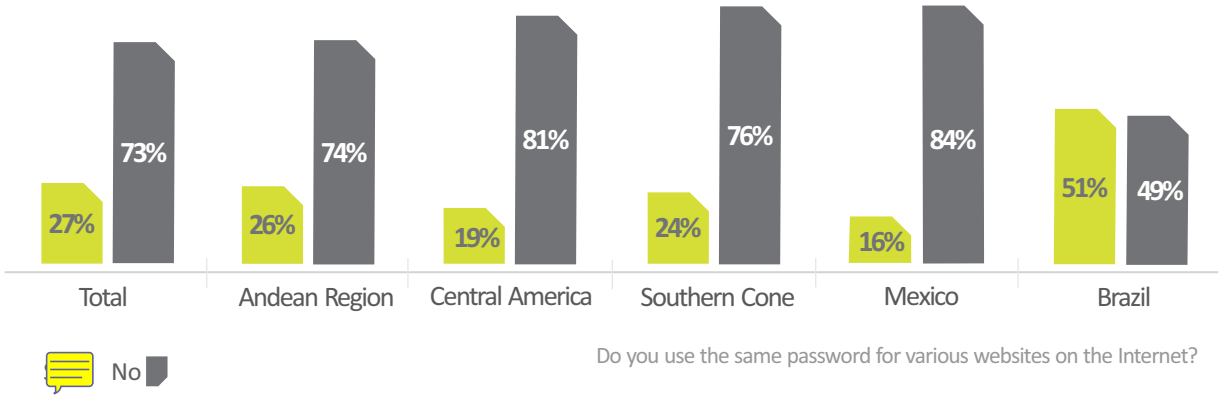
6

> *Password Recycling is Much More Common than It Should Be*

One-quarter of users (and half in Brazil) use the same user name and password for various websites. This exposes users to different kinds of malware that tries to access these accounts in an automated way, or to attacks where credentials stolen from one popular portal are simply plugged into another in case that particular user recycles their password for more than one website.

The typical user in Latin America uses an average of about 5 websites that require a user name and password; compare this to the United Kingdom, where according to a study from Experian, the average user logs into 26 different websites that require login credentials, and only uses five different passwords to cover them all. As internet-connected mobile devices and passwords continue to rise in popularity in Latin America, the amount of websites Latin Americans will need to log into will only increase, causing password recycling to rise exponentially. This makes multi-layered protection and strong authentication methods absolutely essential for keeping user data and money safe from theft.

Average number of web pages used that require a user name and password: 5.1
Password recycling: Yes/No



Do you use the same password for various websites on the Internet?

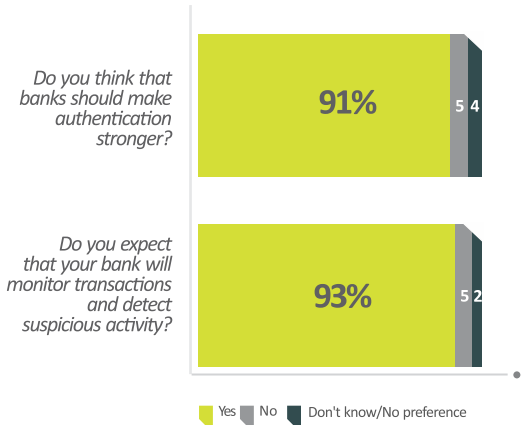
SECURITY METHODS

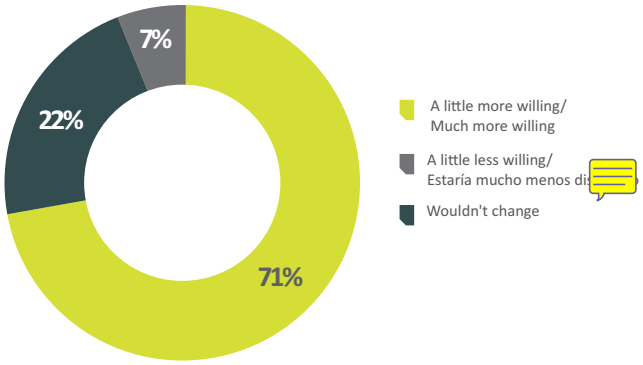
7

> Users Expect Strong Security, but Are Not Sure It's Enough

Users expect more secure authentication and transaction monitoring as an essential part of the online banking experience. Over 90% of users anticipate that their bank will provide such security measures. About half of users would be more willing to use online banking and shopping sites if stronger security measures were put in place, suggesting that banks should implement stronger security methods to generate greater confidence in the use of the Internet as a transactional channel.

> Users that expect stronger authentication and transaction monitoring





If new security methods were implemented (in addition to a user name and password) on websites, how much more willing would you be interact, make transactions or purchases, or enter confidential information on these sites?

> Knowledge of Strong Authentication Methods is High, But Use and Trust in them is Low

The use of strong authentication methods, aside from a secondary password, is low. While a large majority of users know about various types of strong authentication, their use and trust in these methods tends to be much lower, which suggests that users are hearing messages about these security measures but are not convinced that they actually work. Challenge questions and security images generate the lowest amount of confidence among users, with less than a quarter of respondents believing them to be secure.

Confidence in security methods is totally reliant on the perception of users. Users are getting the message that these security measures exist, but don't always feel the urgency to implement them. Banks should accompany the delivery of their security tools with educational materials that explain how to correctly and effectively use the solutions so that they will have a positive impact on trust and perceptions of security.

SECURITY METHODS

7

> Knowledge, usage and trust in security methods

> The Gap Between Trust and Use

	Challenge Questions	Secondary Password	Security Images	Authentication Tokens	Digital Fingerprint Reader	Grid Cards	Passwords sent by text message to a mobile phone
2012	53%	38%	45%	32%	19%	32%	28%
2013	63%	45%	64%	50%	8%	24%	66%

Which of the following security methods for accessing electronic transactions have you heard of?
Which methods do you usually use?
Which are the two methods that you have the most confidence in?

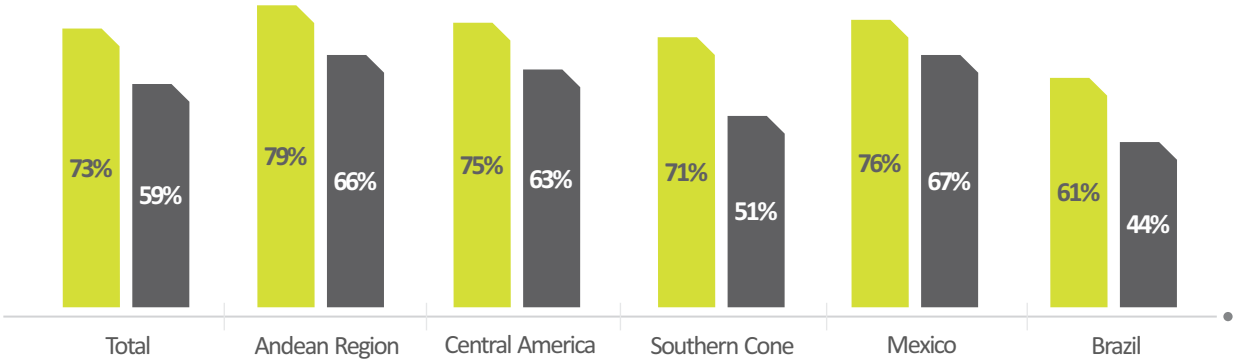
> Users are Willing to Use Additional Security, but Less Willing to Pay for It

Users show a lot of interest in new security methods offered by their banks, which shows that they are eager to sacrifice some convenience to obtain more security. However, about 40% of users are not willing to pay for this security, though willingness to pay is up slightly from last year. Brazil and the Southern Cone have the least inclination to pay for additional security methods, while the Andean Region and Mexico show the most enthusiasm to pay.

SECURITY METHODS

7

> *Willingness to use and pay for additional security methods*



Very Willing to use

Very willing to use and pay for

If your bank decided to implement an optional, stronger security method (in addition to a user name and password), how willing would you be to use this new method?

Would you be willing to pay an additional charge to use this new, stronger security method from your bank?

The vision that sets Easy Solutions apart when it comes to fraud prevention is based on a comprehensive approach that addresses the different stages in the life cycle of an electronic attack: from attack planning, to stealing account credentials, and all the way up to withdrawing money from accounts.

This approach doesn't just allow for fraud to be prevented in a truly proactive way, before attacks are even launched and therefore minimizing the crime's impact and losses; it has also proven to be the most effective way to prevent fraud, because there is no one-size-fits-all solution to the various and constantly evolving forms of electronic fraud.

The Easy Solutions ***Total Fraud Protection®*** Strategy, in addition to covering all of the different stages of an attack, also includes protection for multiple transaction channels and authentication factors, making it truly "total" and complete.

In addition to the effectiveness of the Easy Solutions approach, the different products and services of the T***otal Fraud Protection®*** Strategy are designed to be easily integrated and implemented in stages, depending on the company's security plans and strategies. The products and services also help institutions comply with various regulations.

At a minimum, a layered security program should be designed to detect strange or unusual behavior when the customer logs into the system and when carrying out electronic transfers to third parties. Enhanced security is necessary for business accounts.

The various levels of the Easy Solutions ***Total Fraud Protection®*** Strategy, which not only provide the best proactive protection against different kinds of electronic fraud, but also help to comply with local and international laws and regulations, are described below.

> LAYER 1: Detect Monitoring Services – Proactive Protection against Phishing Detect Monitoring Services monitors and classifies every user connection to a financial institution's website in real time. This layer of security proactively detects website visits from phishers as well as malicious activity on the website such as copying or altering original material. Any fraudulent websites that target the institution's customers are quickly deactivated.

> Layer 2: Detect Safe Browsing – Protection against Phishing, Pharming, Malware, and Man-in-the-Middle and Man-in-the-Browser attacks at the end-user level Detect Safe Browsing is a tool that blocks online banking sessions from computers infected with malware or a poisoned hosts file. This security layer works by scanning a computer when it attempts to connect to a protected website. If DSB detects hosts file poisoning or malicious processes, the user is advised not to carry out the online banking session.

Layer 3: Complex Device Authentication DetectID® is a sophisticated strong authentication solution that permits the flexible integration of different authentication factors on the same platform: second password, security image, challenge questions, tokens, grid cards, and device authentication. The "true" authentication of devices done by DetectID creates a complex digital fingerprint based on the hardware information of the device.

Layer 4: DetectTA® - Real-Time Risk Qualification Detect TA® authorizes or denies every electronic transaction of a customer in real time. This layer of security compares the individual transaction with the user's transaction history and/or any established rules. These enhanced controls include transaction value thresholds, a limit on transactions allowed per day, and allowable payment windows (e.g. day and time), among others.

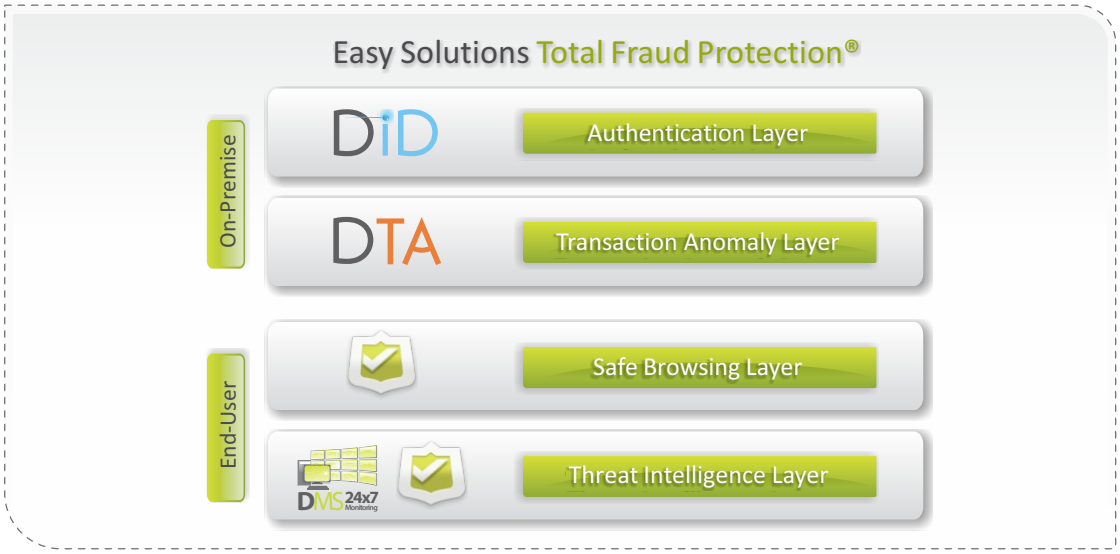
Layer 5: Detect Professional Services Easy Solutions maximizes the return on investment in security through its Direct Professional Services, designed to increase the speed of implementation and get the desired results in terms of authentication and security detection from day one. From the initial analysis to the implementation and training, including consultations about security services, the Detect Professional Services Portfolio is the best choice to ensure the rapid achievement of your business objectives.

For further information about our research or the ***Easy Solutions Total Fraud Protection*** strategy, please contact us at info@easysol.net.

ABOUT EASY SOLUTIONS

9

Easy Solutions is the only security vendor focused on the comprehensive detection and prevention of electronic fraud across all devices, channels and clouds. Our products range from anti-phishing and secure browsing to multifactor authentication and transaction anomaly detection.



The online activities of 32 million users of over 120 leading financial services companies, security firms, retailers, airlines and other entities in the United States and abroad are protected by Easy Solutions fraud prevention systems. Easy Solutions is attractive to companies that want a one-stop shop for most fraud-related prevention services.

EASYSOLUTIONS

Headquarters:
1401 Sawgrass Corporate Parkway, Sunrise, FL 33323
– Tel. +1-866-5244782
Latin America:
Cra. 13A No. 98 – 21 Of. 401 Bogotá, Colombia
– Tel. +57 1- 7425570
info@easysol.net
www.easysol.net