FROST & SULLIVAN

Key Challenges in fighting Phishing and Pharming

A Frost & Sullivan White Paper

EASYSOLUTIONS

TABLE OF CONTENTS

SUMMARY

This white paper aims to inform the reader about the diverse and constantly-evolving phishing threats, and how these threats can account for a company's substantial loss in customers, productivity, and brand credibility.

OVERVIEW

Definition

Phishing 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.

Current Market Status

Even though vendors started to offer solutions more proactively since 2002, the Latin American market is still in a developing stage, becoming increasingly popular and more established in information technology outsourcing.

It is estimated that the growth in security threats will be higher in 2009 due to the international financial crisis, which has impacted several countries in the region during the first two quarters of the year (mostly Mexico, as its economy is severely interrelated to that of the U.S.), in a chain reaction which generated massive layoffs and dismissals. In this scenario, former employees might take advantage of their knowledge of the company's internal infrastructure to initiate attacks. The international financial crisis has postponed many ongoing and future outsourced security projects, mostly in multinational companies that have to comply with headquarter budgetary controls, even though in many cases, outsourcing means cost and investment reductions.

Other factors, such as the lack of quantifiable return on investment (ROI) and high prices, still limit the number of contracts signed for monitoring services and threat control in the region in the short term. In some vertical segments, such as banking and finance and the government, there is still a very strong sensitivity in outsourcing the management of confidential information with unfamiliar companies and personnel, which is also an inhibitor of stronger growth of this market in Latin America in the short-term.

Due to the robustness of the communications infrastructure, hardware and device purchasing power, and cultural barrier to IT adoption, the top 5 countries in Latin America most attacked by security threats are:

1. Mexico *
2. Brazil
3. Colombia *
4. Chile
5. Argentina

* Colombia and Mexico are the countries with highest penetration of malicious content.

Smaller countries like Ecuador, Bolivia and other countries were not seen as attractive by the phishing community. This has changed in recent years, due to the slow evolution of security mechanisms in these regions compared with that of more advanced countries, where phishers have greater difficulties to introduce threats.

Drivers

Which political/social factors are driving the adoption of anti-phishing solutions in Latin America?
As data breaches continue to grow, organizations are required to comply with government regulations which help secure customer data information and company financial information. The increase in mobile devices, threats and technology have created the need to secure networks. Regulation and compliance is a strong driver for the enterprise endpoint security market.

<u>Political aspects</u>:
In Latin America, the municipal, state, and federal governments are all investing in digital inclusion and infrastructure modernization projects, and the pressure from regulatory agencies and regulatory treaties on companies to adopt security measures are strong drivers for anti-phishing adoption in the region.

<u>Social aspects</u>:
Telcos and other MSS players investing in the development of the mid-market segment

Scarcity of qualified and experienced security personnel in the market (affects demand for in-house MSS personnel)

Banking services over Internet
The e-government initiatives and regulations foster the use, provision and promotion of electronic services over the Internet, as well as fostering the development of an electronic culture and habits. There exists a strong correlation among the e-banking culture, the percentage of people with a bank account, and the development and adoption of Internet banking services.

Home office, a security driver in the region
Telecommuting and remote access due to the emergence of the "virtual" company" and events such as the outbreak of virus (ex., AH1N1)

Economic crisis driving security issues
Due to the crisis, CIOs increased the importance and budget for securing companies' networks in order to protect confidential data from a company's ex-employees, who are familiar with the internal infrastructure of the company

Core business focus
Increasing integration and convergence of networks within and outside the enterprise, and companies' dependence on the network

Growth in services over the Internet (e-banking and e-commerce) and increased mobility of the workforce (through smartphones, laptops, and PDAs)

Increasingly variety of threats
Increasingly complex and diversified attacks, increased number of cybercrimes, and negative publicity caused by security breaches

Regulatory agencies pushing for security matters
Government institutions are increasing the use, provision and promotion of security services over the Internet due to strong legal penalties for companies that do not comply with security regulations, including ISO/IEC 27001:2005, Cobit 4.1 or ITIL in Latam or ENISA (European Network of Information Security Agency), OSSTM (Open Standard Security Testing Model) or ISM3 – Information Security Management Maturity Model) internationally

RESTRAINTS

Lack of knowledge in the differentiation of threats
Phishing's main problem is the diverse and ever-evolving technology used to base attacks. However, there are other strong barriers – mainly cultural - for the adoption of phishing protection services in Latin America:

Perception that network security products, mostly UTMs, can act as a substitute for a managed security service model

Lack of awareness about the current threats and available solutions in the market

Perception of high prices
Cost remains a powerful inhibitor, as decision makers ask how many benefits the company would receive by hiring a USD$30,000 annual subscription rather than hiring two people in-house

High import and service taxes increases the price of solutions

Price of MSS still remains prohibitive for many potential clients, mostly in the mid-market

Lack of quantifiable ROI

Fear of outsourcing security
Banking and financial verticals' lack of trust in outsourcing network security

Government's lack of trust in outsourcing personnel in some countries of the region

Trends and Technologies

Evolution of phishing attacks in the short, medium, and long-term

Short-term:

The increase in the volume and degree of vulnerabilities and attacks is turning electronic security into an increasingly complex and broad issue, so the need for specialized professionals and solutions reinforcing network and electronic security is becoming clearer to companies.

The pressure of regulatory acts, such as the Sarbanes-Oxley, Basel II, and compliance with payment card industry international regulations (PCI), is another strong driver of growth of the internet security market in the region in the short-term.

The enterprise scope will turn virtual by incorporating mobile workers, remote sites, home-offices and even vendors and partners within the same corporate network. In this context, security solutions appear as a strategic tool for a reliable and efficient network operations.

When analyzing industries, ISPs, banking and finance, and retail are the most attacked by security threats since the economic crisis began. By the end of the short-term, the advantages of detect monitoring services need to be much clearer to both corporations and medium-sized companies.

Medium-term:

Over the medium (2011 and 2012) and long-term (2013 and 2014), security threats in Latin America are expected to present an increasing growth rate pattern, mainly leveraged by new and improved telecommunications infrastructure, and due to new market entrants, such as Peru.

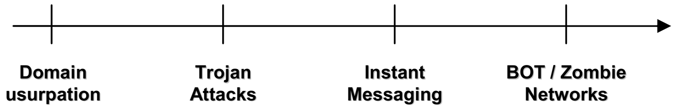
Vertical segments that are projected to leverage their market participation by the end of the medium-term are banking and finance, government, and retail. The threat detection and monitoring services business model will appear as an excellent enabler for a rich value chain. Consequently, the final beneficiary will be the client, which will be able to access efficient and integrated solutions.

Long-term:

The inevitable changes in pricing will redefine segmentation in the long term. The perceptions over the advantages of threat detection and monitoring services will become clearer and more widespread in all vertical segments, in corporations, and in the mid-market segment in Latin America. In addition, past experiences of companies which experienced any loss due to phishing will prevent other companies from costs and capital expenditures (CAPEX) for cybercrime losses.

Phishing evolution: The main change has nothing to do with technique, which basically is still taking advantage of the human factor as the weakest link, but with the objective and professionalization.

The following chart shows a tendency line of phishing threats:



UTMS, firewalls and other hardware/software solutions for threatening attacks
There is lack of market maturity. There are terms that are confusing, so it is possible to find offers that promise antivirus and phishing solutions that carry some truth, but the protection is not optimal, as the threats evolve and their detection can only be made through a history of behavior and not only through few proxy, certificates or DNS static parameters.

Is an "antivirus" the solution?
Without a doubt, antivirus software is helpful against malware, and some security vendors recommend customers to install this type of security products. However, an antivirus program cannot guarantee complete protection against Trojans and malware, as it can only capture threats listed in a vault which is updated a handful at a time.

Is an "UTM" the solution?
A UTM is a network device that provides a conventional network firewall service with multiple functions added, such as protection against threats, spam and viruses, working at the application level and creating the process as proxy traffic, analyzing, and letting the traffic according to the policy implemented in the device. However, UTMs can only capture static threats.

UTMS and firewalls – among others - act as complementary solutions, but for true protection, it is necessary for a security solution to base itself on deactivation services and prevention of fraudulent sites in real time.

What should a threat security suite contain to be effective?
Preventive measures: Previous research on existing threats, strong authentication processes, security and e-mail policies

Detection measures: In-depth industry knowledge; use of analysts as trusted advisors to improve security policies

Early notifications: Identify specific patterns and behaviors that typically occur at the early stages of a phishing attack

Phishing Alerts: Recover from phishing and malware attacks

Malware monitoring: Sustain an action plan where malicious code is attacking

Help in remediation: It is necessary that the solution be robust enough to be present during and after the threat detection/elimination, accompanied by a group of experts with sufficient knowledge to take preventive action over the threat, creating for the client innovative solutions based on the client's current security environment

Key Challenges

Taking advantage of human concern to overcome exposure to the AH1N1 virus, e-mails on this topic drew the most attention and consequently the “click” possibilities became greater.

Another concern is the crisis associated with unemployment, which has revealed fraudulent employment sites and emails offering jobs through the Internet or home. There exists a lack of clarity of rules of what is needed to protect a company from phishing and malware versus different protection mechanisms. Here is where Easy Solutions is working.

Nowadays, to avoid anti-phishing systems techniques, phishers have begun to improve several methods:

- To avoid anti-phishing text techniques that anti-phishing systems scans over websites, phishers use several Flash-based websites methods hiding a multimedia object.
- For current anti-phishing filters, phishers are using images instead of text to make it harder to detect text commonly used in phishing e-mails. A user facing a phishing site should be able to differentiate what text is and what an image is.
- New and improved telecommunications infrastructure gives to phishers the ability to control and access in new ways with new techniques for cybercrime.
- Large Internet-based companies such as AOL, MySpace, and PayPal, and retailers such as TJX Companies, have been victims and have had to spend large amounts of capital – and jeopardized branding -- due to phishing attacks:

Early phishing in AOL: Posing as an AOL staff member sending an instant message to a potential victim, phishers ask users to reveal passwords in order to "verify your account" or "confirm billing information. This way, hackers used phishing to obtain legitimate AOL accounts (1990).

PayPal: Users were redirecting to a fake site in an attempt to collect password details (2005).

MySpace: A computer worm altered links to redirect visitors to designed websites, stealing login details (2006).

Banamex: Despite all preventive phishing attacks through the use of OTP tokens (One-Time Passwords and keys for a single use), in 2006 phishers attacked the Banamex OTP token (named NetKey), using it as an excuse of the system itself, based on the token, to generate confusion among users and ask them to provide the passwords. This is not the first attack to this entity. (2006)

Banco Chile: A phishing email with the bank's logo: "During our regular maintenance and verification processes, we have detected an error in the information we have associated with your account." The mail content specifies some factors which could provoke the error and contains a phishing link at the bottom of the email. (2008)

Twitter: A phishing scam spreading quickly via direct message, "Hi, this you on here?", and providing a phishing link which can take your personal information and hijack accounts. (2009)

CLASSIFYING THE MENACE: PHISHING

How it Works

What phishing is and what's the difference among similar threats
Phishing incidents are like waves: in a certain period the company can experience a number of reported incidents and the next to have none. A wide mistake is to think that phishing attacks occur only via email. Although it is the most common way of propagation, there are a variety of attacks, such as:

Deceptive Phishing: It is the most common one. Consists of a deceptive email masquerading as a trusted company. The recipient clicks on the link contained in the message, unconsciously being readdressed to a fraudulent website.

Malware-Based Phishing: Refers to a variant of phishing attacks that involves the execution of malicious software on the user's computer. The user must perform some functions that allow the execution of the malware on the computer (open an attachment, visit a website and download a program, etc.).

Keyloggers / Screen loggers: *Keyloggers* are programs that record keystrokes when installed in the computer, with access to a registered website. Data are recorded by the program and sent to the phisher over Internet. Screen loggers have the same function, but capture screen images.

Session Hijacking: Describes the assault that occurs once the user has accessed any website registered by the software. These programs are often disguised as browser components.

Web Trojans: Program with pop-up screen appearance over legitimate web pages validations. The user might think he or she is entering details on a real website, while in reality it is being done in the malware.

System Reconfiguration Attacks: The attack takes place by changing the configuration parameters of the user's PC. *i.e. modifying the domain name system.*

DNS-Based Phishing ("Pharming"): This offense is based on interference in the domain name searching process by modifying the domain name resolution sending the user to a different IP address.

Content-Injection Phishing: The phisher introduces fraudulent content into a legitimate website.

Data Theft: Malicious code that collects sensitive information stored within the machines in which it is installed.

Man-in-the-Middle Phishing: The phisher takes a position between user's PC and the server filtering, reading and modifying information.

Hosts File Poisoning: This is another option for pharming. In this case the attack is carried out by the host's card index hosted on DNS' servers.

Spear Phishing: One of the newest phishing strategies. It targets a specific company and uses e-mails to train individuals at various locations.

Which kind of sites get attacked?
Phishers target banks customers and online payment services mainly. To lure this type of information, phishers commonly withdraw social networks (nowadays a prime target of phishing), auction websites, and online payment processors. Attacks are typically carried out by e-mail or instant messaging, persuading users to enter personal details at a fake website, which appears to be the legitimate one.

How does the attack work?
Identical URLs: Most phishing methods use misspelled URLs or use sub-domains provided in emails which appear to belong to the legitimate organization. A sub-domain generally includes parts of the real domain: www.realdomain.section.com/, but actually this URL points to a different webpage due to the "section" word in the domain. JavaScript commands are being used in order to alter the address bar by placing a picture over a legitimate URL, or by closing the original address bar and opening a new one with the legitimate URL.

Certificates: Also known as IDN spoofing, phishers use URLs with IDNs in web browsers that visually might look identical to a trusted organization's web address, but open URL redirectors to disguise malicious URLs with a trusted domain. Certificates do not solve this problem, as it is possible for a phisher to purchase a valid certificate, and afterwards modify initial content to spoof a real website.

Most common certificates are:
CISSP - Certified Information System Security Professional
CISA - Certified Information System Auditor
CISM - Certified Information Security Manager
CFE - Certified Fraud Examiner

CIFI - Certified Information Forensics Investigator
CIA – Certified Internal Auditor

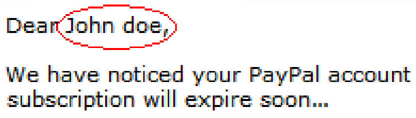
Cross-site Scripting: A type of attack which is very difficult to spot without a specialist's knowledge; this is when phishers use errors in a trusted website's own scripts against the victim. The script directs the user to sign in at their own web page (the web address and security certificates seem to be correct), but in reality the link to the website is crafted to carry out the attack.

Pop-Up Windows: Other frequent used technique is to show a popup window requesting credentials on top of the legitimate website, in a way that seems that the website is requesting this sensitive information. This is mostly used in banks.

Recognizing a phishing attack at a company or at home
Usually, phishing attacks encourage the victim to take immediate action, to reply promptly in order to avoid an account cancellation – an act first and think later tactic in which the victim does not want to lose money they did not spend.

Without proper threat detection/monitoring services, end users would need remarkable skills in order to detect a fake website:

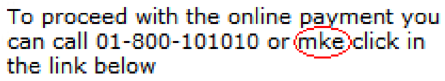
Your name in the content of the email is not sufficient to confirm the legitimacy of the sender:



Dear John doe,

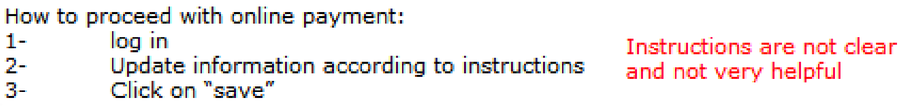
We have noticed your PayPal account subscription will expire soon...

Look for grammatical errors or typos in the content:



To proceed with the online payment you can call 01-800-101010 or mke click in the link below

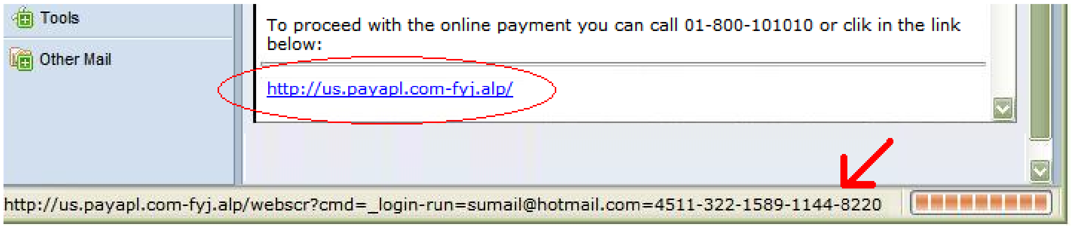
Usually, real mails from real websites provide clear instructions to the user to carry out payments; these instructions must be clear and helpful:



How to proceed with online payment:
1- log in
2- Update information according to instructions
3- Click on "save"

Instructions are not clear and not very helpful

Generally no links are provided within the body text, and when provided, they are a copy-paste style:



To proceed with the online payment you can call 01-800-101010 or clik in the link below:

http://us.payapl.com-fyj.alp/

http://us.payapl.com-fyj.alp/webscr?cmd=_login-run=sumail@hotmail.com=4511-322-1589-1144-8220

Challenges

How phishing attacks can affect your business

One of the main problems that phishing raises to financial institutions is linked not only to economic loss due to fraud, but also to a loss of confidence in the brand and corporate image.

From a technical standpoint, phishing is a theft of credentials. From a business standpoint, it is the receipt of a fraudulent transaction. Easy Solutions DMS reacts by detecting and removing the threat, and if a user happens to fall into the trap, Detect TA stops fraudulent transactions.

SUCCESS CASE

Challenge

Success Case: A traditional diary company in Equador

One of the diaries with a major production volume in Ecuador and distributed in the whole country, suffered a denial of service on their website during the first few days of September, 2009.

Solution

Easy Solutions signed a contract through a reseller in Quito, Ecuador, in order to investigate the origin of the assault to the service, and to define the strategies of mitigation in order to eliminate the problem.

The platform, “Detect Monitoring Service (On Demand),” was contracted to react immediately against this incident. Easy Solutions, with the collaboration of the diary team, took two days to implement the collection of backsliders scripts, finding the potential sources of the incident and defining the necessary strategies of mitigation.

Impact

The assault was contained successfully and the image and quality of the service provided by Easy Solutions, allowed the entity to realize the importance of having mechanisms for real-time monitoring of malicious activity on the Internet portal.

DETECT MONITORING SERVICE

Identification Accuracy

Overview

DMS is used to address phishing issues for customers. It is a real-time connections monitoring service that reaches transactional sites on the client side, with the client's information correlated with data obtained from malicious activity in the industry.

Real time solutions suite - DMS de Easy Solutions

Early Notification

DetectCA proprietary methodology can identify specific patterns and behaviors that typically occur at the early stages of a phishing attack, providing a way to stop an attack even before it becomes a real threat.

Malware Monitoring Services

Easy Solutions monitors on a daily basis hundreds of samples of new financially-motivated malware which enables the company to proactively and quickly implement an action plan when a malicious code is attacking clients.

Phishing Alerts

Detect Monitoring Services prevents, detects and recovers from phishing and malware attacks. The solution addresses the entire lifecycle of an alert, providing the right, just-in-time help when clients need it most.

Reporting the Threat

Security Partners

Easy Solutions works directly with top internet security leaders to provide the most advanced anti-phishing solution. With a 24/7 SLA, Easy Solutions affords clients modularized solutions to prevent and detect phishing attacks in the network.

Structure of business partners throughout the region, serving Colombia, Venezuela, Ecuador, Chile, Argentina and now all of Latin America, except for Brazil.

Differentiators from Similar Security Suites in the Market

The result of the DMS real-time proactive monitoring is the detection of new fraud sites activated against protected institutions and disabling them. DMS, unlike other similar solution suites, offers users the ability to not only detect the threat but also clear it. No other industry has it in a same package. Compared to other security suites, DMS is the only offer to not only detect the threat but also deactivate it.

The objective of Easy Solutions is not just protection from phishing. Phishing is perhaps the instigator of a more complex problem of fraud in financial institutions. This is why DMS is a key part of what Easy Solutions calls a "total strategy to protect against fraud," in which it is possible to stop a criminal attack regardless of the stage of evolution.

Performance

Complementary Solutions
Detect Safe Browsing: This is an extension of DMS created to protect the beginning of pharming in the end user.

Differentiator: Easy Solutions has integrated the solution for DMS with Detect Safe Browsing, allowing the market to have an integral protection. Traditional Anti-Phishing and Anti-Pharming solutions have no concern for the end user. Detect Safe Browsing, from Easy Solutions installs an agent in the customer's end users that reports every malicious behavior, including malware, host file infections, and the like.

Security and Administration

Confidential Information Management
Easy Solutions does not retain information that may be sensitive to the client.

Support
Detect Monitoring Service provides 7x24x365 real time monitoring to rapidly identify, shut down, and recover from online scams that mislead customers through fraudulent use of their corporate identity.

Detect Monitoring Service effectively handles the lifecycle of any phishing attacks, providing clients with the just-in-time help and the right protection when they need it most by integrating the power of 7x24 real time monitoring with the in-place incident response systems – even enabling the end user to report a fraudulent case needing to be investigated.

Removing the Threat

Database Updates
The data base update is done through several methods: The model is purely based on behavior patterns and proprietary patterns.

- **Secondary Information to correlate information:** Through a geolocation database that is updated daily, Easy Solutions identifies with a high degree of accuracy from which country a connection belongs and who the service provider is. Additionally it allows to identify if the IP is recognized as an anonymous proxy or not.

- **Proprietary Patterns:** Allows to identify if the connection is injecting parameters to the transactional site. Basically it analyzes the behavior of the connection. Easy Solutions does not use black lists for this purpose, but a historical behavior from IP connections or if the IP is rarely attempting to connect more times than it historically does to this transactional site. Within proprietary patterns there are two basic engines:

- Google, which has a secure innovation strategy called "Google Safe Browsing," where Google qualifies each URL that is navigating over the Internet to know if this URL is hosting phishing or if it has been used as a propagation array for malicious code.

- PhishTank is a database which allows users who have experienced phishing to report anomalies and new phish sites, and lists those which are already disappearing.

New Threats Identification
Easy Solutions Strategy for total protection against fraud: Easy Solutions not only cares for the detection of fraud but also cares about how to authenticate the end user and how to protect the financial institution. This suite is comprised of 3 products:

1. DMS
2. Detect ID: Is a multifactor detection platform / multi-channel allows you to move to the side of the financial transaction, authenticate the customer when approaching the transactional platform
3. Detect TA

Complementary Solutions

Detect Safe Browsing
Detect Safe Browsing from Easy Solutions is an innovative tool to fight against the serious threat of pharming, in which antivirus and spyware removal software are not effective. It scans the Host's file and processes, detecting malware that can poison the DNS Server and Host's file on the victim's computer. Once detected, it is able to delete or stop the malware and direct the user to protected sites.

Detect Safe Browsing provides real-time protection against pharming based on a proprietary cross validation scheme, to guarantee that the end user will not be re-directed to fraudulent websites. It also combats pharming at the end user level, making it unique in the security industry.

DSB Features:

- Effective protection against pharming, where antivirus are not effective
- Proactive detection of malware that re-directs to fraudulent websites
- Simple and easy installation and use
- Easy access to unlimited protected sites
- Designed for end-users in a home or business environment.
- Know the end-user experience
- Customizable and flexible remediation
- Customizable look & feel

Detect TA

Detect TA builds a transactional pattern for each account or user. Detect TA knows at which time a person makes a transaction, in which account, which public services the individual pays, all connection parameters, which kind of equipment is used to make transactions between accounts, and the like. Detect TA multi-channel, and learns if a person shops online at supermarkets, by phone and so on. When a new transaction arises, Detect TA rates the transactions and compares it to the customer's historical transactions and is able to find parameters that trigger particular risk in the transaction. Easy Solutions call it "risk score in real time."

Detect TA is a statistic-based heuristic engine that dynamically builds a financial risk array of each customer once a transaction arises; the financial risk matrix is adjusted to reflect that learning. There is a phase in which this matrix must be initialized. When a financial institution begins in Detect TA, it must extract the transactional history so Detect TA can initially index all financial risk arrays. Thereafter, the engine starts to calculate the risk matrix based on historical transaction behavior.

Detect Social Engineering Assessment

Social Engineering is generally agreed upon as the weakest link in the security chain. Many of the most damaging security violations are due to employee security breaches and the use of social engineering in malicious attacks is rising.

Detect Social Engineering Assessment (DSEA) addresses the risk of this rapidly evolving threat as part of an overall risk management strategy, helping organizations to strengthen the employee's commitment to a security-aware culture and can be complemented with Detect Monitoring Service and Detect Safe Browsing for enhanced protection against social-engineering attacks that integrate technology, like phishing and pharming.

ABOUT EASY SOLUTIONS

EASYSOLUTIONS

Easy Solutions is simplifying the way businesses deal with and effectively deploy security for online transactions. The company provides solutions for identifying and preventing online transaction fraud while helping institutions comply with existing US domestic and international two factor authentication requirements. Using our advanced transaction fraud prevention solutions, we help protect online businesses and enterprise applications from phishing attacks, online credential theft and Internet fraud threats.

Our software solutions are simple to manage and easy to deploy. Our patent-pending technologies provide accurate identification of devices with unprecedented accuracy while protecting users by monitoring transaction behavior for activity associated with fraudulent activity. By simplifying online transaction security, Easy Solutions provides consumers and online merchants and financial institutions the ability to focus on their business instead of worrying about the safety of their transactions.

Online security experts with years of extensive knowledge and experience in protecting enterprises from traditional security threats, online fraud and Internet phishing attacks developed Easy Solutions' intellectual property and technologies. Working closely with the leading security companies and leading financial enterprises with large online customer communities, Easy Solutions continuously collect and understands the latest methods used by online criminals.

This knowledge is combined with our patent pending behavioral monitoring that protects users on a per transaction basis. The transaction monitoring is backed up with continuous identification of attributes collected from end-user devices to create a unique device fingerprinting that enables forensic identification. These capabilities are delivered in a simple effective software package providing our customers the ability to protect sensitive customer transactions and data while complying with business regulatory compliance issues.

One of the most important aspects of our solution is that no change in behavior is required on behalf of the users and the implementation is easy for both the business and its customers. Easy Solutions is the only security vendor focused exclusively on fraud prevention; providing anti-phishing services and research, multifactor authentication and anomaly transaction detection.

The capacity to react to new threats in the antifraud protection field is based on our proprietary technology and in the methodology to face each threat in an integral way implemented through Easy Solutions' Total Fraud Protection Strategy.

Easy Solutions is a security vendor focused on the problem of fraud, with unique strategies in which the customer will find several advantages.

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 - Phone: +57 1- 2362455.
www.easysol.net

CONTACT US

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Auckland
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Dhaka
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Mexico City
Milan
Moscow
Mumbai
Manhattan
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting and Growth Team Membership empower clients to create a growth-focused culture that generates, evaluates and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 40 offices on six continents. For more information about Frost & Sullivan’s Growth Partnerships, visit http://www.frost.com.