

# Det@ct SOLUTIONS

Online transactions protection portfolio



# A GUIDE TO PROTECT ON-LINE TRANSACTIONS

The intention of this whitepaper is to provide a holistic overview of the online banking security problems and the way Easy Solutions, a leading and innovative security vendor, approach to this problem by providing an easy-to-implement solution that goes beyond the simple anti-phishing solution but protecting virtually the consequences of any kind of Identity Theft using two factor authentication via Hardware Device Identification plus the power of Transaction Anomaly Detection.

## THE EASYSOLUTIONS APPROACH TO IDENTITY THEFT AND FRAUD PROTECTION

The Easy Solutions portfolio providing complete proactive solutions against identity theft and fraud includes:



An innovative authentication solution to implement a two factor authentication scheme using a proprietary patent-pending algorithm by extending the authentication process to the device where the transactions are being launched.



A Fraud Prevention Solution that work at the transaction level by authorizing in real time every transaction according to specific user transactional habits that the product is learning over time.

## THE TECHNICAL PROBLEM

The irresistibility for criminals to attack Internet banking lies in their ability to compromise the present user authentication procedures by impersonating the identity of a legitimate accountholder in order to gain access to bank accounts.

Phishing is online identity theft in which confidential information is obtained from an individual. It is distinguished from offline identity theft such as card skimming and dumpster diving, as well as from large-scale data compromises in which information about many individuals is obtained at once. Phishing includes many different types of attacks, including:

- Deceptive attacks, in which users are tricked by fraudulent messages into giving out information.
- Malware attacks, in which malicious software causes data compromises.
- DNS-based attacks, in which the lookup of host names is altered to send users to a fraudulent server.

Phishing targets many kinds of confidential information, including user names and passwords, social security numbers, credit card numbers, bank account numbers, and personal information such as birthdates and mothers' maiden names.

The Gartner Group estimates that the direct phishing-related loss to US banks and credit card issuers in 2003 was \$1.2 billion. Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Phishing also causes substantial hardship for victimized consumers, due to the difficulty of repairing credit damaged by fraudulent activity.

## THE BUSSINES PROBLEM

Online Identity Theft is perpetrated in many different ways. Phishers are technically innovative, and can afford to invest in technology. It is a common misconception that phishers are amateurs. This is not the case for the most dangerous phishing attacks which are carried out as professional organized crimes. As financial institutions have increased their online presence, the economic value of compromising account information has increased dramatically. Criminals such as phishers can afford an investment in technology commensurate with the illegal benefits gained by their crimes.

The financial industry is losing money at an accelerate level not only by the phishing problem itself but also for the following related issues:

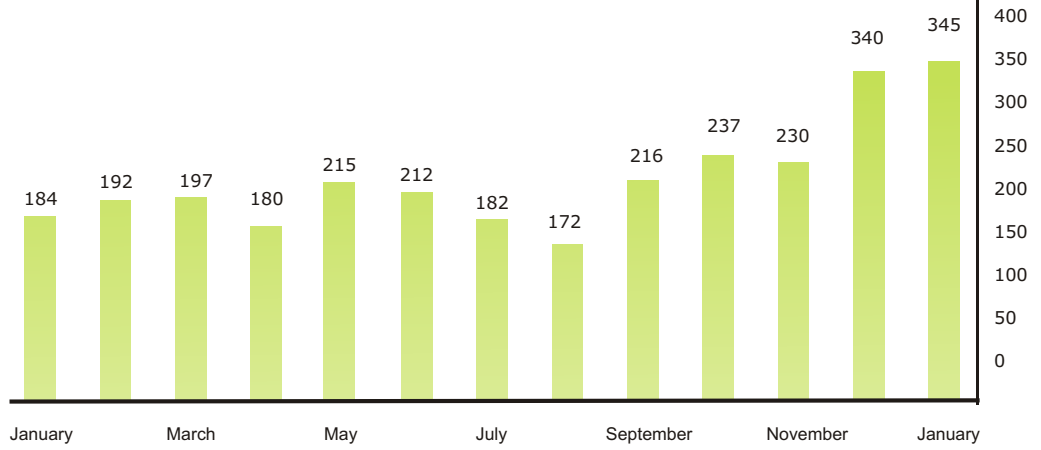
- Moving the accountholder to more expensive transactional channels due to the lack of confidence from the online service.
- Loss of reputation.
- In more sophisticated phishing attacks other transactional channels are also compromised including typically ATMs and IVR Systems.

## THE FACTS

Cybercriminals have a sustained model for Identity Theft and therefore are willing to invest large amounts of money and time studying their next target to get their maximum profitability by a successful attack. The following figures show the growth of phishing in the last year representing a series of successful attacks that have left huge loss for the banking industry but at the same time large profits for cybercriminals.

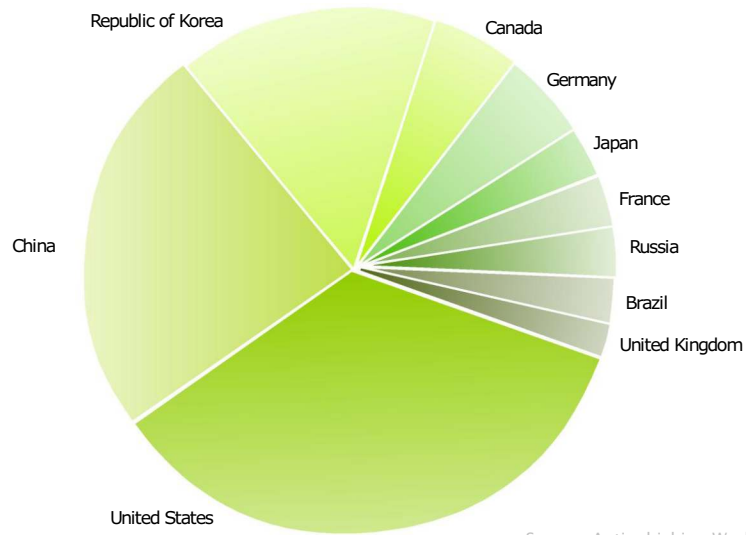
# THE FACTS

Password Stealing  
Malicious Code  
Unique  
Applications



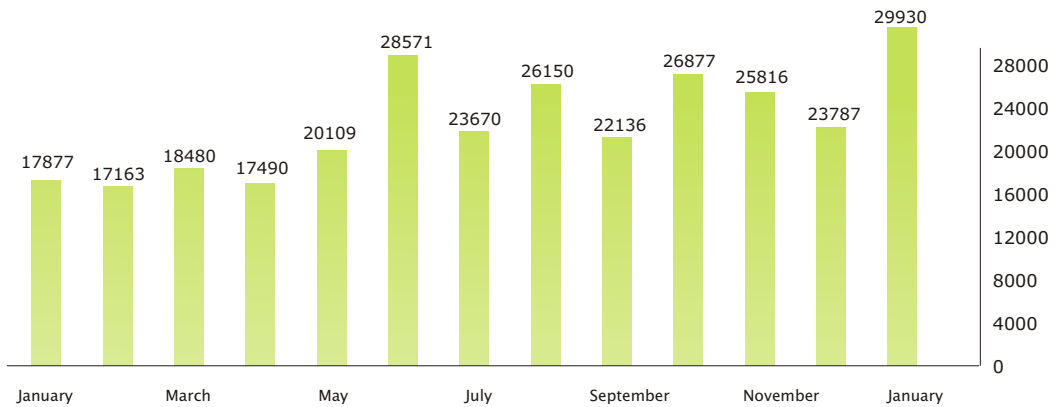
Source: Anti-phishing Working Group.

Top 10  
phishing sites  
hosting countries



Source: Anti-phishing Working Group.

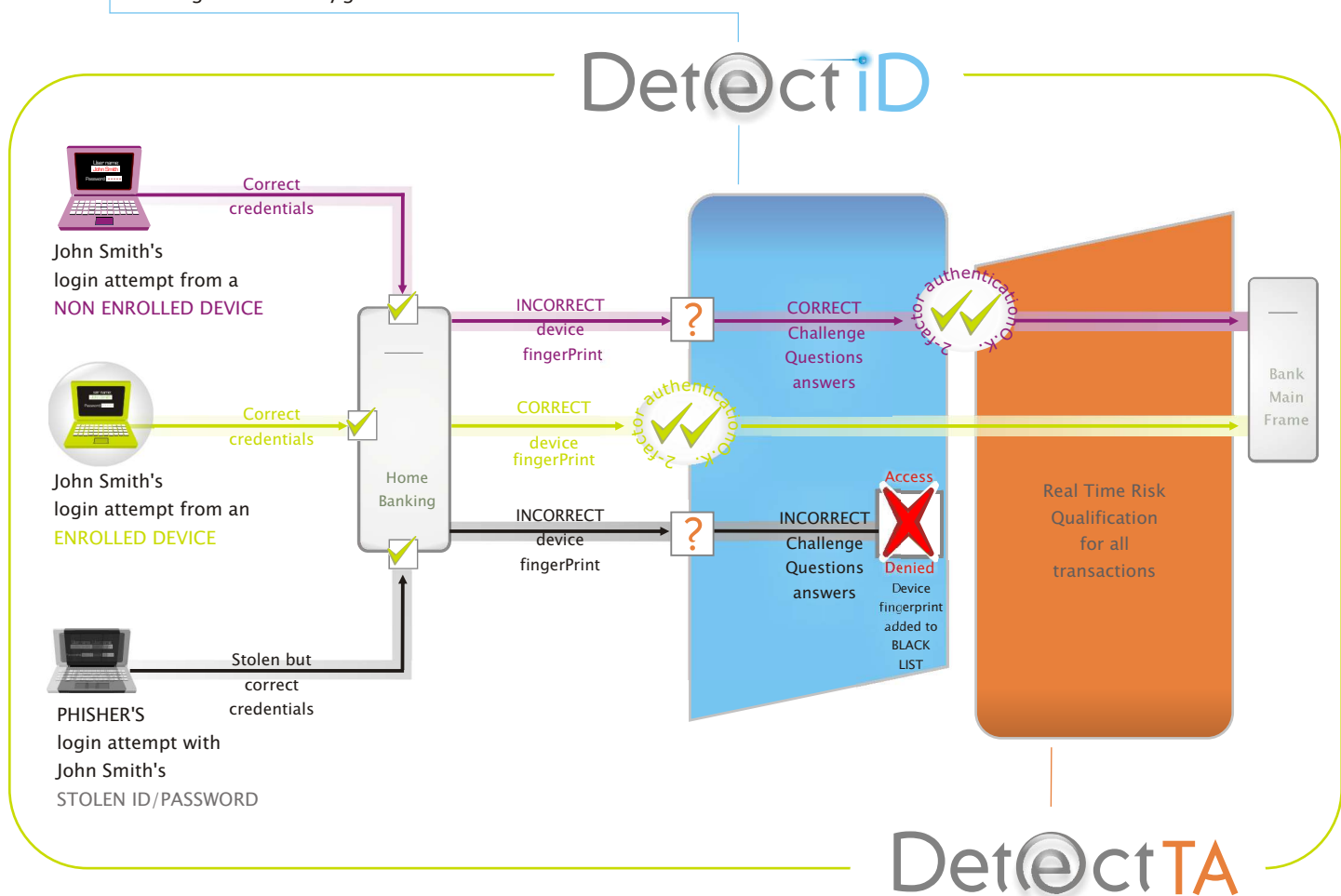
Phishing reports  
received:  
January 2006  
January 2007



Source: Anti-phishing Working Group.

# TOPOLOGY AND FLOW OF THE EASYSOLUTIONS APPROACH

Working at the device level, Detect iD captures hardware specific information that is used to feed the proprietary algorithm to define a fingerprint per device. This scheme allows creating 2-factor authentication scenario where the users/password combination is tied to devices based on which Detect iD can define, in real time, the level of confidence that can be expected from any Internet Banking session at any given moment.



Working at the transactional level, Detect TA is able to learn the transactional behaviour of every single account and its normal user to determine in real time the level of risk of an outgoing transaction.

## DEVICE ID AUTHENTICATION



# Detect iD

## Device ID Authentication Engine

Detect iD is the first step toward reducing the risk of compromising end user with identity theft attacks, phishing attacks and ultimately the loss of money and confidence in the internet as the most effective and cost reducing transactional vehicle.

Some of the Detect iD key features are:

- **Security Image Authentication:** Using this characteristic each user defines a security image that allows the user to verify that they are indeed at the bank's website and not at some scammer's fake site.
- **Challenge Questions Authentication:** This additional authentication scheme is applied via challenge questions plus additional transaction anomaly detection from Detect TA when a user is attempting to login into the system from a non-enrolled device. It is possible to maximize the user mobility and flexibility without losing security strength.
- **User's Device White Lists:** This feature allows an end user to enroll more than one device as a valid token for the strong authentication systems.
- **Institution's Device Black List:** Once a device is detected trying to carry out fraudulent activity, its fingerprint is added to the institutional blacklist. In this way it's possible to anticipate fraudulent activity. Furthermore, Easy Solutions via SSU (Special Security Updates) populates the black list database with malicious fingerprint found around the world. All customers benefit from the world-wide collective experience.
- **Easy Implementation:** Detect iD has been designed and developed for easy integration with the Customer's current business and security environments. Detect iD supports Web Services to reduce the amount of code that has to be added in the authentication routine of the current web application.

## ONLINE TRANSACTIONS ANOMALY DETECTION

# DetectTA

Online Transactions Anomaly Detection Engine

DetectTA is the state of the art fraud prevention for the online users stopping not only fraudulent activities generated by cybercriminals in the Identity Theft and phishing field but also any other forms of online financial criminal activity.

Some key features of DetectTA are:

- ▲ **Real Time Risk Qualification:** DetectTA determines in real time the risk qualification of an ongoing transaction and can trigger additional validation scheme for a given transaction like challenge questions.
- ▲ **End User Transactional Profiles:** The end user can create specific transactional profiles when he or she is using a device that is not part of the end user's white list. This feature, working along the power of real time transaction anomaly detection, can provide the flexibility that the user desires and the security that the institution requires in a win-win deal.
- ▲ **Institution Transactional Profiles:** When no end user is activated the institution can enforce a restrictive transactional profile when the end user is in a device that is not part of its white list.
- ▲ **Suspicious Activity Alert:** DetectTA is loaded with specific patterns that has been found during fraudulent activity attacks like funds consolidations of very small transaction from multiples account into a single account or point-to-point activity from two accounts involving an exaggerate numbers of small transaction.
- ▲ **User Defined Rules:** This feature allows a user or institution to enforce certain rules to the transactional engine in order to avoid the occurrence of transactions related with terrorism and money laundry that primarily use the internet as transactional vehicle

Start PROTECTING  
your ONLINE TRANSACTIONS  
with

Det@ct  
SOLUTIONS  
TODAY!

[info@easysol.net](mailto:info@easysol.net)



EASYSOLUTIONS

© 2007