BEST SECURITY PRACTICES IN ONLINE BANKING PLATFORMS
TABLE OF CONTENTS

BEST SECURITY PRACTICES
Home banking platforms have been implemented as an ever more efficient channel through for banking transactions. However these web-based applications are exposed over the Internet making their users a very appealing target for mal-intentioned individuals.

EASY SOLUTIONS’ FOCUS ON PROTECTION
Easy Solutions recommends implementing robust authentication strategies to strengthen the authentication process, not only for pressure in meeting with regulations, but also for the high exposure of e-banking platforms to attacks.

DetectID
DetectID is the only authentication platform that combines the potentiality of detecting malicious processes during the authentication process with the objective of shielding the authentication cycle from malware.

ABOUT EASY SOLUTIONS, INC
Easy Solutions is the only security vendor focused exclusively on fraud prevention; providing anti-phishing services and research, multifactor authentication and anomaly transaction detection.
For several years now, electronic banking platforms have been implemented as an ever more efficient channel through which banking transactions can be done without having to leave the house or office.

In the end, however, these home banking platforms are web-based applications that are exposed over the Internet making their users a very appealing target for mal-intentioned individuals. These are some reasons why e-banking platforms are such an alluring objective for criminals to attack:

- E-banking Platforms are openly exposed over the Internet;
- The users are very appealing, since ultimately their intention is to carrying out a financial transaction;

The evolution history of these attacks began more than 7 years ago initiating what quickly became known as phishing. Its sophistication has increased on par with the new security technologies adopted by the bank industry intended to mitigate the problem.

The following graph shows the evolution of the security problem affecting the e-banking platforms over the last years.

TREND:
Shift towards blended malware attacks
In its report of April 2, 2009 "The War on Phishing is Far From Over", Gartner shows the results of this attack methodology on the U.S. population where 5 million consumers lost money due to phishing or its variants through the end of September 2008.

For Easy Solutions, some of the issues that make us conclude the war against Phishing is far from over are the following:

- The authentication schemes currently in use base their robustness on the end-user's decisions, which make them entirely vulnerable to social engineering attacks. For example, in authentication schemes based on One Time Password (OTP), the end-users should determine that they're connected to the right website and consequently log in using their OTP;

- The authentication GAP, which is the technical term commonly used for referring to the intrinsic vulnerability of the authentication process. In highly exposed environments, such as the e-banking platforms, this GAP is reflected in the little or total lack of control the authenticating institution (financial institution) has on the authenticating elements (users) since no control exists on the medium (the Internet and computer connection used in accessing the home banking platform);

This opened the doors to malicious people who carry out attacks against e-banking platforms, who focus their efforts on pharming attacks + malware that allows:

- Poisoning the hosts file to add re-directing entries as shown in the following graph
More sophisticated attacks involving malware + pharming + man-in-the-middle Proxy, in which the targeted e-banking sites are re-directed to the loopback address 127.0.0.1 or local host; where a man-in-the-middle Proxy is running listening to the communications between the client and the server which enables the attacker to modify the messages in real time.

The following graph shows a real case in Latin America of a hosts file modified by an attack of this nature.

Next, a hypothetical example is presented that shows the process of stealing credentials in this type of attack.

The user enters into the real home banking platform through the Man-in-the-Middle Proxy

Once the user enters his/her credentials, the Man-in-the-Middle Proxy captures them, as shown in the following graph.

Credentials entered by the user in the browser
The capture platform provides the attacker with all the necessary information to: hijack the session, using the session cookie, and the access credentials including the OTP, with which they'll have 30 to 60 seconds to use it before it expires.

A point worth mentioning is that this same platform allows the attacker to manipulate the data moving between client and server. That way the attacker can wait for the moment a transaction takes place in order to manipulate the data of the account receiving the funds while the transaction is on its way to the e-banking platform.

Since December 3 of 2008, when the first great password stealing malware appeared as a Mozilla plug-in that stole information sent out to 100 financial sites including anz.com, bankofamerica.com, lloydstsb.co.uk and PayPal, the evolution of these types of attacks has been unparalleled.

Gartner, in its report New Bank-Targeted Trojan via Firefox Saps Consumer Confidence, considers that these types of attacks will be copied and improved as criminals continue innovating on unauthorized access to financial accounts.
Easy Solutions recommends implementing robust authentication strategies to strengthen the authentication process not only for pressure in meeting with regulations but also for the high exposure of e-banking platforms to phishing and pharming attacks which can compromise the organization’s image and produce financial losses.

When defining authentication strategies, it is important to keep in mind the different vectors of phishing and pharming attacks. Some are presented here:

- Social Engineering attacks that mislead the end user.
- Man in the Middle attacks that listen the communication between client and server.
- Man in the Browser attacks that re-direct the end-user to counterfeit sites with the intention of stealing the end user credentials.
- Malware attacks that poison the hosts file and/or DNS to re-direct the user to counterfeit sites with the intent of stealing the end user’s credentials;
- Trojan Proxy that installs a http redirector running in the local address 127.0.0.1 that re-directs all of the browser’s traffic to this Proxy making a copy of the messages and sending them to the attacker;

From all of the above, it can be concluded that there is not any single strategy that covers all the different dangers threatening the e-banking platforms. On the contrary, focusing on a multi-layer protection approach is the best alternative for massive authentication processes of applications that are highly exposed on the Internet, including a mix of different factors that allow:

- Shielding the authentication cycle from malicious processes that can affect the end user’s station;
- Providing user-to-site authentication strategies which allow the end-user to verify that the connection is indeed established with the correct site;
- Implementing authentication factors that eliminate user decisions from the authentication equation;
Easy Solutions’ Total Fraud Protection (ETFP) combines different technologies that allow it to stop a fraud attack during any phase.

To summarize, it is important to define an authentication strategy which grows on the foundation of a platform that can add multiple security factors and/or methods for the authentication of applications exposed on the Internet.

The different products that make up the protection strategy involve a focus on multi-level protection as described below.

Implementing authentication factors based on knowledge (what the bank knows about the end-user);

Implementing authentication factors based on something that the user has (OTP, USB Device, etc);

Offering complementary protection for the end-user’s station;

Communicating the occurrence of potential transaction frauds to the end-user;

Easy Solutions’ Total Fraud Protection (ETFP) combines different technologies that allow it to stop a fraud attack during any phase.
DetectID is the only authentication platform that combines the potentiality of detecting malicious processes during the authentication process with the objective of shielding the authentication cycle from malware.

The following graph shows how DetectID keeps a registry of the processes running in the end-device while a session of online banking is taking place.
DetectID allows taking the user out of the authentication equation by means of its powerful device authentication engine, which through the use of hardware allows truly authenticating a device.

DetectID implements the user-to-site authentication concept by means of IdentiSite® which allows each user to define a secret image with the bank to identify when he/she is truly connected with the entity.
DetectID also includes a proprietary implementation of OTP (One Time Password) that allows out of band authentication schemes via email or mobile phone. Integration with leading technologies of the physical OTP industry such as Vasco and RSA is also possible.

The following graph compares the different factors and authentication methods with the security they offer and the resistance to different threats that affect e-banking platforms, as shown in this study.

<table>
<thead>
<tr>
<th>Factors</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Offers Strong Authentication</td>
</tr>
<tr>
<td>Passwords</td>
<td>✓</td>
</tr>
<tr>
<td>One time Password (OTPs)</td>
<td>✓</td>
</tr>
<tr>
<td>Coordination Cards</td>
<td>✓</td>
</tr>
<tr>
<td>Device Authentication</td>
<td>✓</td>
</tr>
<tr>
<td>Image Authentication</td>
<td>✓</td>
</tr>
<tr>
<td>Challenge Questions</td>
<td>✓</td>
</tr>
<tr>
<td>USB Tokens</td>
<td>✓</td>
</tr>
<tr>
<td>Digital Certificates</td>
<td>✓</td>
</tr>
<tr>
<td>Authentication + Malware Detection</td>
<td>✓</td>
</tr>
<tr>
<td>DetectID Authentication Framework</td>
<td>✓</td>
</tr>
</tbody>
</table>
Easy Solutions is simplifying the way businesses deal with and effectively deploy security for online transactions. We provide 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.