

The Growth of Phishing Attacks & The eW@LL Solution's Protection



Contents

Introduction – What is Phishing?

Phishing Facts

Technology Solutions

eW@LL Solution

Summary

Introduction

What is Phishing?

“In computing, phishing, short for password harvesting fishing, is the luring of sensitive information, such as passwords and other personal information, from a victim by masquerading as someone trustworthy with a real need for such information.”

-Wikipedia, The Free Encyclopedia

Introduction

How do criminals Phish?

1. They hijack users and send them to fraudulent websites of trusted brands such as well-known banks, online retailers and credit card companies
2. Phishing attacks use 'spoofed' e-mails to lure recipients into browse fraudulent websites.
3. The fraudulent websites are designed to fool recipients into divulging personal financial data.
(e.g. credit card numbers, account usernames and passwords, social security numbers)

Consumers are suffering credit card fraud, identity theft, and financial loss

-Anti-Phishing Working Group (APWG)

Phishing Facts

Phishing Statistics:

- Number of unique phishing attacks reported in July: **1,974**
*A “unique phishing attack” in this analysis is defined as a single email blast sent out at one time targeting one company or organization, and having one unique subject line.
- Average monthly growth rate in phishing attacks : **50%**
- Organizations most targeted by phishing attacks **Citibank (682)**
*HSBC has had 22 attacks from Jan to July 2004
- Country hosting the most phishing Web sites: **USA (35%)**

-July Report, Anti-Phishing Working Group (APWG)

Phishing Facts

Damages:

- 5% of targeted recipients respond to phishing emails
(Source: Anti-Phishing Working Group (APWG))
- US banks and credit card issuers suffered a loss close to \$1.2 billion in 2003 because of the phishing phenomenon
(Source: Symantec Corporation)

Countries Hosting Phishing Sites:

US	35.0%
South Korea	16.0%
China	15.0%
Russia	7.0%
UK	5.5%
Mexico	4.5%
Taiwan	2.5%

(Source: July Report Anti-Phishing Working Group (APWG))

Phishing Facts

Ease of obtaining Phishing techniques:

- "Do it yourself" phishing kits are freely available on the Internet. They contain graphics, web code and text necessary to make bogus websites that look and feel like real online banking sites.

(Source: Sophos Plc.)

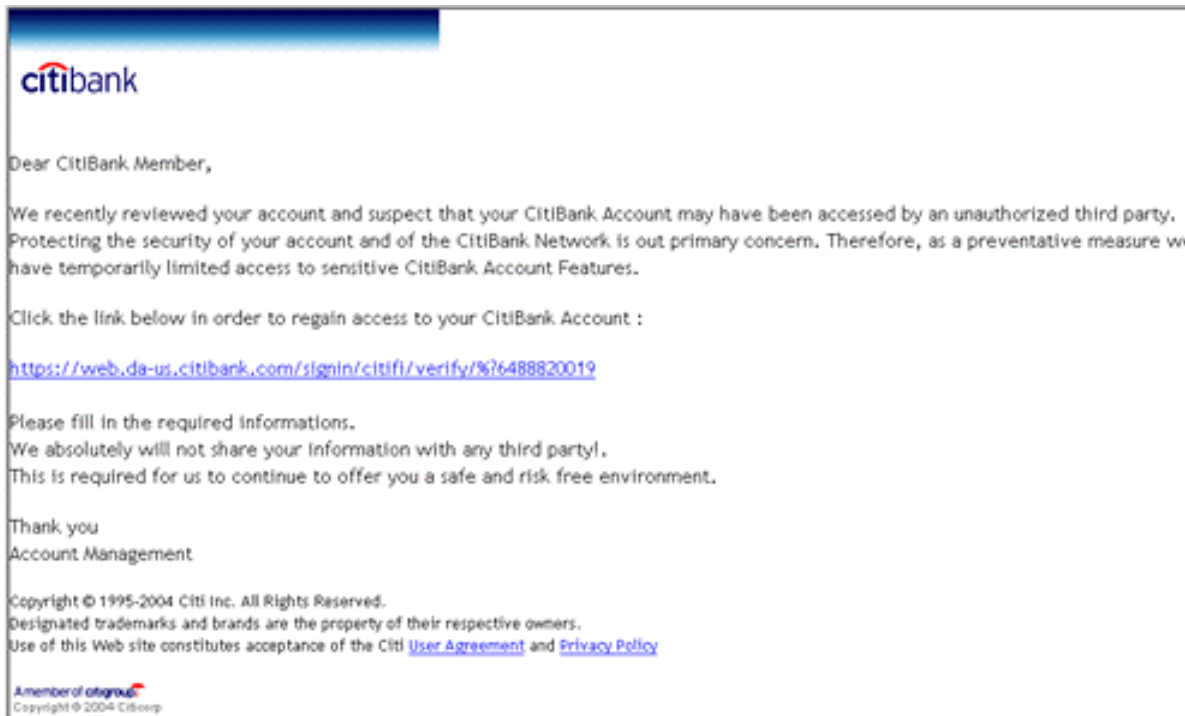
Customers' reactions:

- More than 65% of surveyed respondents said it was unacceptable for companies to do nothing about this criminal activity.
- 96% of users surveyed want companies to consider new technologies to help authenticate email and online sites

(Source: TechWeb News)

Phishing Facts

Phishing Email:



Phishing Facts

Phishing Email:



Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below:

<https://aribada.ebay.com/saw-cgi/eBayISAPI.dll?PlaceCCInfo>

If your account information is not updated within **48 hours** then your ability to sell or bid on eBay will become restricted.

Thank you

The eBay Billing Department.

Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



Technology Solutions

Technology characteristics:

For a preventative technology solution to be effective, it must have the following characteristics:

- Minimize end-user training
- Use of exiting standards-based technologies
- Unilateral deployment must add value
- Must be cost-effective for both senders, recipients, and Internet infrastructure providers

-Anti-Phishing Working Group (APWG)

Technology Solutions

Current Preventative Solutions:

1. Strong Website Authentication

Strongly authenticates any users visiting a business web site using two-factor authentication. Limit end-user training as much as possible

Positive Aspects	Downsides
<p>Phisher can't log into real site without the right physical token such as smart card, even if a user falls for a phishing attack.</p> <p>Users are given a stronger sense of trust in their transactions with business web site.</p>	<p>Users need more education.</p> <p>Set up time delays.</p> <p>Desktop software installation.</p> <p>High management costs.</p> <p>Potentially high cost per user.</p>

-Anti-Phishing Working Group (APWG)

Technology Solutions

Current Preventative Solutions:

2. Mail Server Authentication

Use enhanced DNS capabilities to verify the IP address of sender's email server

Positive Aspects	Downsides
Easy to configure at senders mail servers	Sender and recipient gateways are required to use these methods.
Makes it harder for phishers to be anonymous.	SMTP sender is not visible to recipient ("From:" address still can be spoofed)
Legitimate business email can be better identified – lower spam false positives	Will be a problem for anyone using 3 rd party emailing services
	Doesn't accommodate email forwarding.

-Anti-Phishing Working Group (APWG)

Technology Solutions

Current Preventative Solutions:

3. Mail Authentication via Digital Signature

Use existing industry standard S/MIME digital signatures to sign outbound mail to provide signature verification at the gateway or email client

Positive Aspects	Downsides
Would work without any additional software	Recipients still have to inspect the "From:" address for misleading domains.
"From:" address impossible to spoof without detection.	Not all email clients supports S/MIME
Phishers must register with a certificate authority to send phishing emails; stronger identity audit trail to prosecute phishers.	Recipients may not check certificate revocation status
Legitimate business email can better identified by end-user.	Sender and recipient gateways must both understand S/MIME digital signatures if using gateway server to verify signatures

-Anti-Phishing Working Group (APWG)

eW@LL's Solution

How eW@LL protects against Phishing:

eW@LL's technologies can overcome Phishing problem cost-effectively while using existing standard-based systems and needing little or no education for email users. eSm@rt addressing, Sender Confirmation Engine, and Recipient Key provide an impenetrable barrier to malicious messages sent for the purposes of Phishing.

Scenarios:

1. **Stop The Spoofing Of Emails**
2. **Open Safety Channel**
3. **Collect And Report Fraudulent Messages**

eW@LL's Solution

Stop The Spoofing Of Emails:

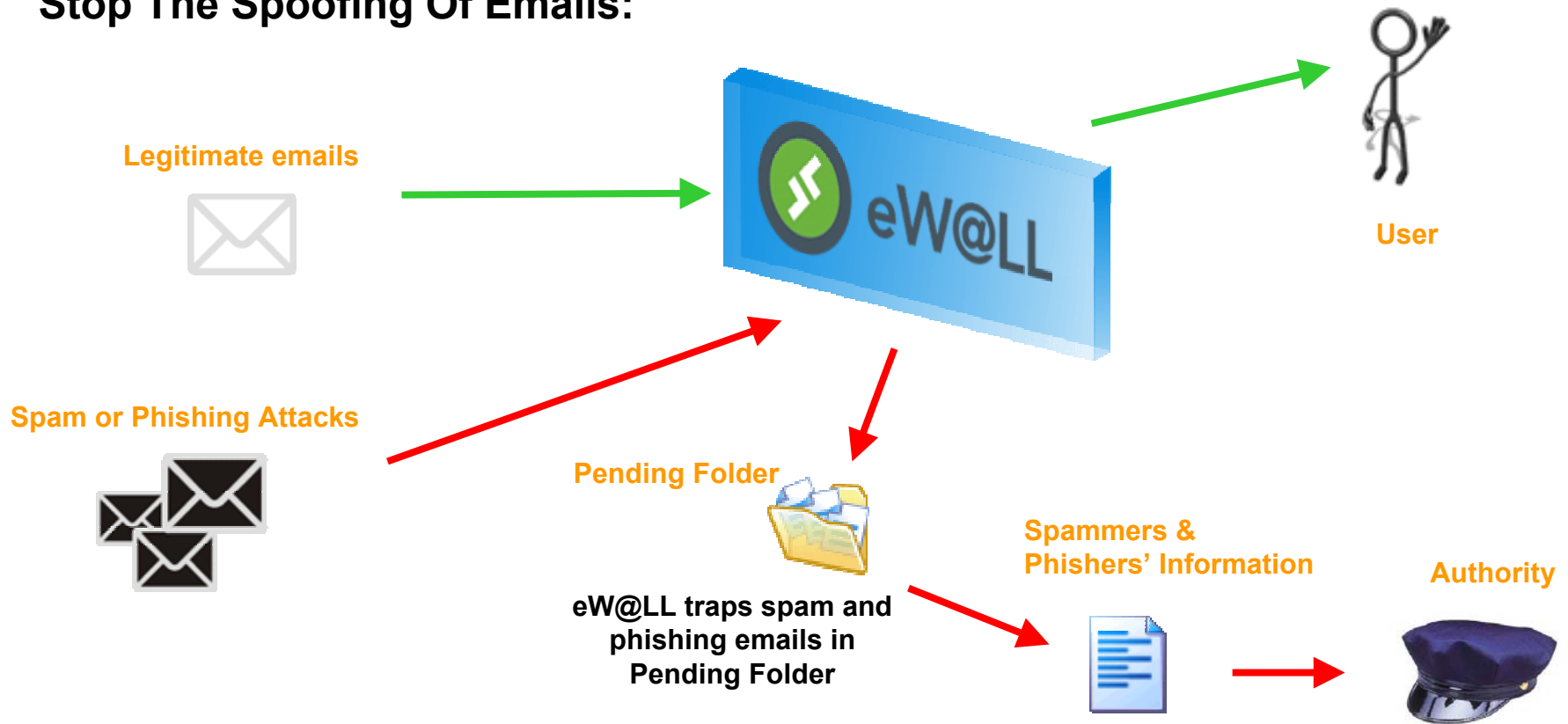
eW@LL's Sender Confirmation Engine™ is a powerful tool designed to protect the recipient from spoofed emails (those containing a fictitious From: address).

A unprecedented technology, **eW@LL's Delivery Path Verification™** can verify the sender's identity even if he or she has been added to a user's approved table (whitelist or confirmed list).

eW@LL enables individual users to report fraudulent messages trapped in pending folder to appropriate authorities.

eW@LL's Solution

Stop The Spoofing Of Emails:



eW@LL's Solution

Open Safety Channel:

eW@LL's eSm@rt™ addressing can open a one-to-one safety channel for users to receive legitimate messages from banks, credit unions and/or any other business enterprises.

With the cooperation of Telecoms/ISPs all users can safely continue to use their commercial email and Internet online services for any transactions without the threat of having their identity stolen or coerced from them by the unscrupulous organizations or individuals which prey upon the honesty and integrity of their victim.

eW@LL's Solution

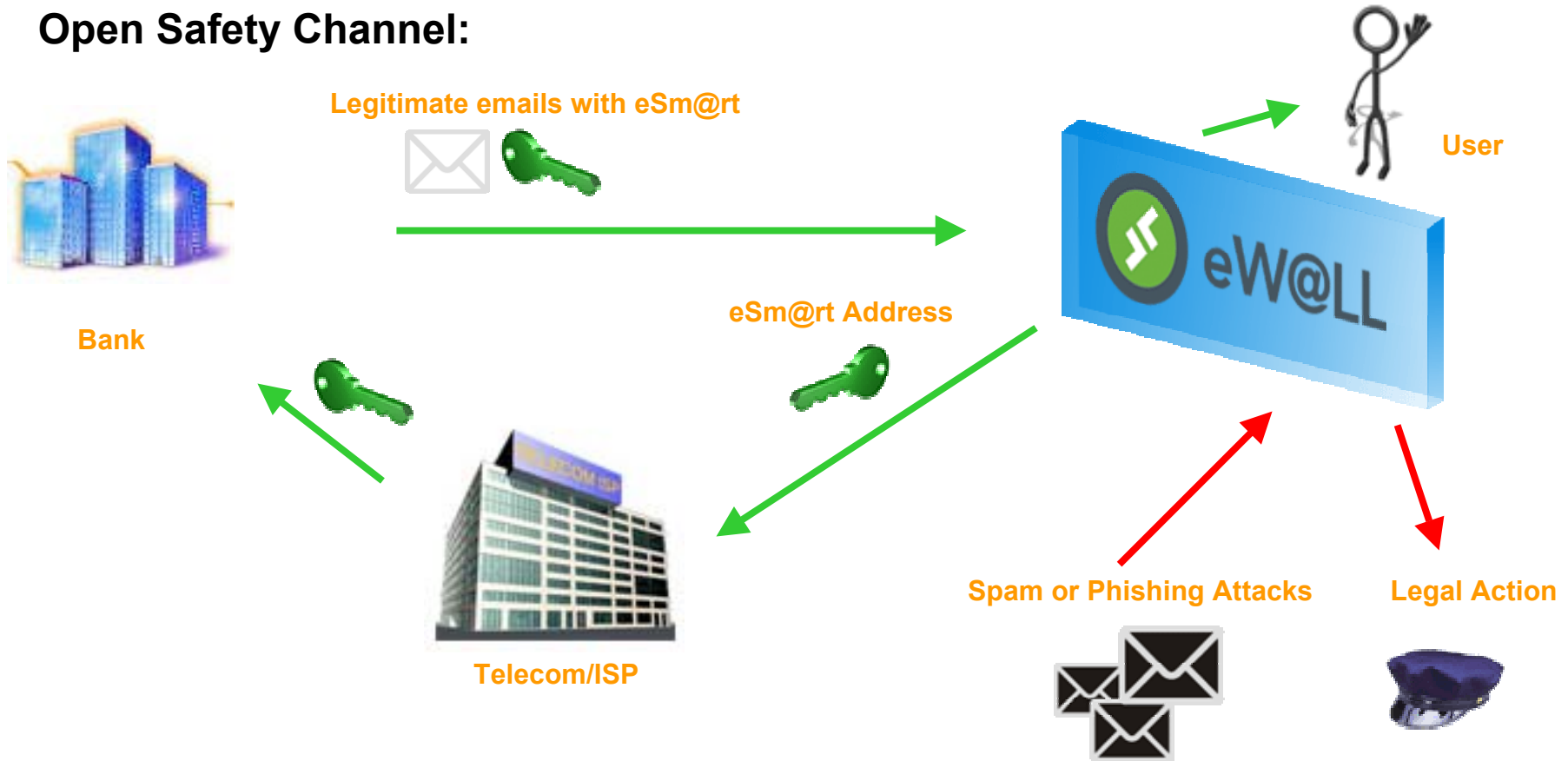
Open Safety Channel:

Steps:

1. ISP will setup a web page to aid their users to create eSm@rt address for banks and financial institution
2. Users login to the ISP's webpage with their existing credentials
3. Users generate an eSm@rt address with a simple mouse click
4. Users submit the eSm@rt address as their contact email address and the financial institutions would update the "Customer Profiles". (ISP and Banks work in cooperation to provide these services)
5. Any financial messages sent to users other than through this eSm@rt address would be void and possibly fraudulent.

eW@LL's Solution

Open Safety Channel:



eW@LL's Solution

Positive Aspects:

- Minimize the rate of phishing attacks.
- eW@LL will trace and record senders' header information; stronger identity audit trail to prosecute phishers.
- Only Legitimate emails will be sent through the eSm@rt addresses since phishers only use spoofed addresses.
- No 3rd party desktop software to install.
- Minimal user training and intervention thus permitting Global deployment
- Legitimate business messages are identified – lower spam false positives.
- Users are given a stronger sense of trust by their ISPs and business companies.
- Simple and Cost Effective. Use existing standard systems.
- Low management costs.
- Only ISPs have to install eW@LL Solution, users and senders do not have to.

Prerequisite:

- Users' ISPs must install eW@LL .

Summary

- **Phishing**, short for password harvesting fishing, is a serious problem that is rapidly growing. Most major banks and credit card issuers have been hit with phishing attacks and are suffering great losses.
- Phishers do not require a high-level of skills for phishing since the tools are readily available on the internet.
- Customers expect companies to use proactive measures against the problem.
- Current Preventative Solutions are Strong Website Authentication, Mail Server Authentication, and Mail Authentication via Digital Signature. These methods result in a higher operational costs, more user education, new software installation, or new standards
- The eW@LL technologies can overcome the Phishing problem cost effectively while using existing standard-based systems with less recipient education than any current product offering.

Thank You

eW@LL: Now you have control™

Gennux Microsystem Corp.
info@gennux.com
<http://www.gennux.com>