

The HP Anti-phishing Toolbar

A Simple Solution to "Phishing" and "Pharming"



This woman is smiling. What she doesn't know is that she has just been phished and her personal information has been stolen.

Table of contents

Abstract	2
Costs of online fraud: Who gets hurt?	2
Federal Guidelines	2
ID theft: Tricks of the trade	3
Going deeper: SSL is not enough	3
Password safety: A multifaceted challenge	4
A simple solution: The HP Anti-phishing Toolbar	4
Competitive approaches: Partial solutions	5
Summary	6

Abstract: Identity theft is the most prevalent and destructive of all crimes. As a major source of fraud losses and consumer concern, it poses significant challenges to any organization that collects and retains a user's personal and financial data. New privacy legislation and stringent regulations are spurring changes in the way essential customer data is managed. This paper offers a new technology to mitigate the risks of the ID theft attacks of "phishing" and "pharming."

The HP Anti-phishing Toolbar offers an enhanced password generator and a proven anti-phishing solution. The user only needs to remember one master password; the toolbar generates a unique strong password for each site. With a different strong password for each site, user accounts are kept safe. The toolbar conveniently fills in the username and password with a single click, saving consumers

the hassle of remembering different logons and passwords. Since the generated password depends on the secure label, the toolbar only sends a password to a site when the site's certificate is present. If all users do to log in is click on the button, they cannot be phished or pharmed. It also lets users securely label sites to prevent being fooled by fake sites.

The HP Anti-phishing Toolbar is a unique two-factor authentication solution that financial organizations can offer their clients to help reduce the costs of online fraud and phishing. It also satisfies the FFIEC issued guidelines for authentication in Internet banking. The toolbar can be customized with the provider's logo, keeping their brand in front of their customers. As a reminder of who supplied the superior anti-phishing solution and an enhanced password generator, the toolbar's branding capability creates additional customer loyalty.

An urgent e-mail warns that your customer's online banking account will be terminated unless the customer follows a link, logs in, and updates account information. But the link takes the customer to a fake site designed to steal passwords and personal information! This online scam is called phishing and it's big business—most banks and online services are under attack from fraudsters that prey on their customers. Phishing and its related crime of pharming risk undoing the user trust necessary for shopping and conducting business online.

Costs of online fraud: Who gets hurt?

Reading today's newspapers it is easy to see that the pace of serious security breaches is accelerating. The Anti-Phishing Working Group has seen a steady rise in attacks, from 727 new fraudulent websites in August 2004 to 5259 new websites reported in August 2005. According to the Privacy Rights Clearinghouse, from February through August of 2005 there were over fifty serious data breaches at businesses, government agencies, and universities affecting more than fifty million identities. In addition, the number of IT security incidents reported worldwide to organizations such as CERT has in fact risen dramatically over the past several years.

In 2005, over nine million U.S. consumers were bilked for \$52.65 billion dollars in fraud losses. Five billion dollars were absorbed by consumers. The time to fix a victim's financial affairs is weeks, months, or years, and there are few laws that allow for recourse. So, it's

no surprise that a recent Forrester study found that 53% of consumers were concerned about online fraud and that 13% of consumers have actually been victimized.

The other losers in the identity theft phenomenon are merchants that bear the rest of the fraud losses that are in turn passed on to consumers in the form of higher prices. Financial institutions might also incur added tangible costs such as re-issuing cards and the untold, but very real, damage to their brands in the form of undermined customer confidence.

Do these numbers constitute a new international crime wave? No. The re-sale of customer information by insiders is not new, but the rise of the Internet supercharges the opportunity for fraudulent abuse. The worldwide web is a hostile environment with few laws, naïve consumers, and a growing reservoir of well-equipped adversaries. What is new is privacy legislation, such as CA SB1386, Payment Card Industry standards, Gramm-Leach-Bliley, and BASEL II, that brings consumer fraud into the light of day by forcing organizations to notify consumers if there has been a security breach.

Federal guidelines

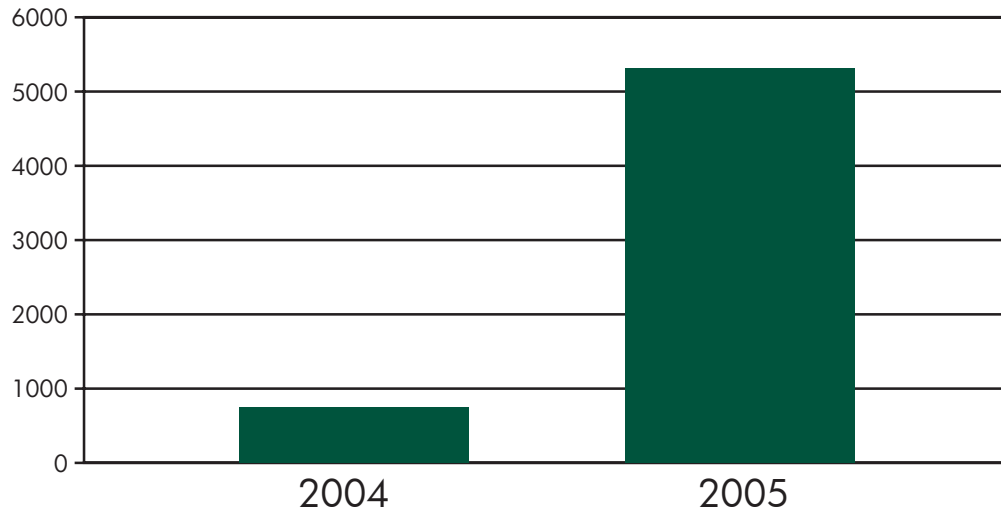
Recently, the Federal Financial Institutions Examination Council (FFIEC) issued guidelines for banks offering Internet-based financial services. The "Authentication in an Internet Banking Environment" guidance describes enhanced authentication methods, including two-factor identification, that regulators expect banks to use when authenticating the identity of customers using online services. Financial institutions in the U.S. will be expected to strengthen their online

"If you're exchanging sensitive data online and you're not worried about identity theft, you should be. Several new attacks are released every day to steal your data or co-opt your account."

—Larry Seltzer, eweek.com

Chart 1. New Fraudulent Websites

Source: The Anti-Phishing Working Group



authentication procedures by the end of 2006. Many banks in the U.K. and Europe already offer two-factor authentication options for their customers, including a variety of different one-time password solutions.

Two-factor authentication provides:

- Enhanced levels of security
- The ability to monitor usage patterns and automatically trigger responses when unusual events occur
- Minimized exposure time when passwords are stolen

ID theft: Tricks of the trade

What are the tools and techniques of the identity thief? The tried and true methods of dumpster diving, laptop theft, and social engineering still work. Users are the weakest link in any anti-phishing system. If they can easily trick users into compromising their sensitive data, attackers do not have to attempt a more difficult direct attack on system security.

With so many people going online, getting users to provide confidential information has only gotten easier. Two newer techniques are phishing and pharming. Phishing uses spoofed e-mails to lead consumers to counterfeit websites where they divulge sensitive data such as credit card numbers, account usernames, passwords, and Social Security numbers. Phishers hijack the brand names of trusted firms such as banks, online retailers, and credit card companies to convince recipients to respond.

Pharming is "crimeware" placed on a PC that misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning. Once

information is obtained, an adversary impersonates victims in order to gain access to their finances or to frame them for a crime. Stolen identities have become as valuable as cash to organized crime organizations and the professional hacker.

Going deeper: SSL is not enough

SSL certificates were invented to protect Internet users from online fraud, but they aren't working. Certificates don't automatically help the user identify a site. No certificate information is displayed unless the user asks for it. It takes three or four clicks to get the information and technical expertise to understand what is being shown. Looking for the padlock icon in the browser doesn't help because fraudulent sites can easily obtain security certificates that seem legitimate.

For example, an attacker trying to impersonate PayPal could set up a fake site at a reasonable-looking URL (<https://paypal.security-update.com/>) and purchase a valid SSL certificate for that site. Because the certificate is valid and its domain name matches the URL, the browser is satisfied and will show the padlock icon. But not everyone will realize that a URL beginning with <https://paypal.security-update.com/> actually has nothing to do with the real PayPal.

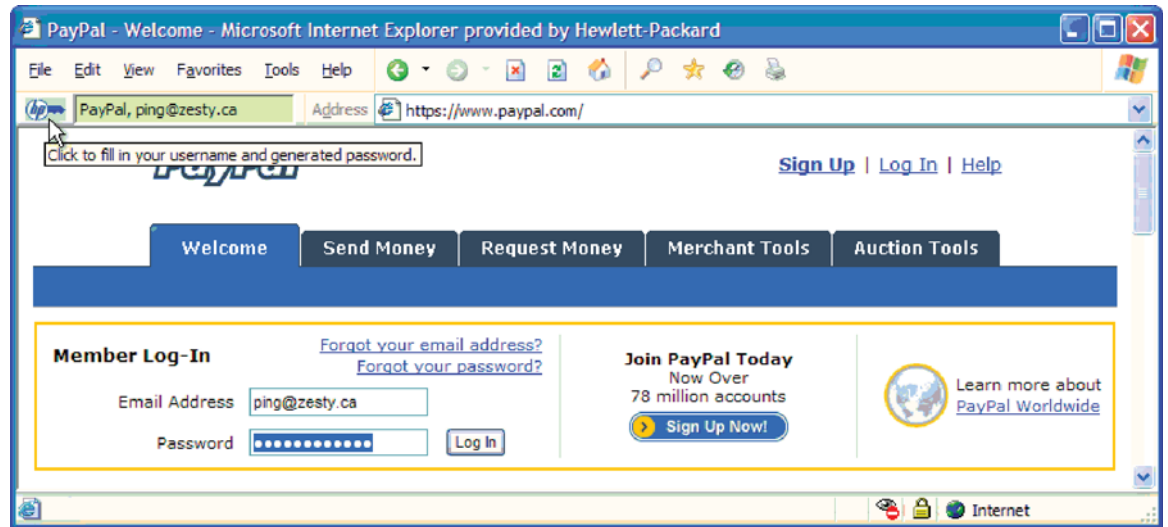
As a defense against phishing attacks, consumers are told not to click on links in e-mails, but to type in URLs instead. That's safer, but it still leaves users vulnerable to a pharming attack in which a malicious party hijacks the bank's real domain name to make it point to a different site.

What is two-factor authentication?

Two-factor authentication is any authentication protocol that requires two independent ways to establish identity and privileges. This contrasts with traditional password authentication, which requires only one factor (knowledge of a password) in order to gain access to a system.

—Wikipedia.com

Figure 1. The HP Anti-phishing Tool Bar provides a text field to help users identify sites, calculate site-specific passwords, and fill in the login form upon clicking the button.



Password safety: A multifaceted challenge

Although phishers try to collect all kinds of personal information, passwords are a prime target. A password conveys control over an online account, enables one to make purchases or transfers, and is the key to obtain other information. There are at least four problems with passwords on the Internet:

- 1. Fraudulent websites impersonate legitimate websites, and fakes are hard to detect.**
The only way to be sure you're at the right website is to look for the padlock, examine the URL, extract the domain name, and determine that it's the correct domain. That's too hard. Finding the domain name in a URL is tricky, and even when it is shown separately, domain names can fool people.
- 2. People often use the same password at many different sites.**
Reusing the same password at multiple sites is risky, because a break-in at any one site compromises all your accounts. But for most people, remembering many different passwords is too much trouble.
- 3. People often choose weak passwords because it's annoying to type strong passwords.**
The more often you must type a password, the less likely you are to choose a long or complicated password. And that makes the password more vulnerable to being guessed or cracked.
- 4. Typing passwords frequently makes people more likely to give away passwords by mistake.**
People are accustomed to entering their passwords every time they visit a secure site several times a day.

It is dangerous to be in the habit of typing a password without thinking, in response to any login prompt, without examination to see if it is legitimate.

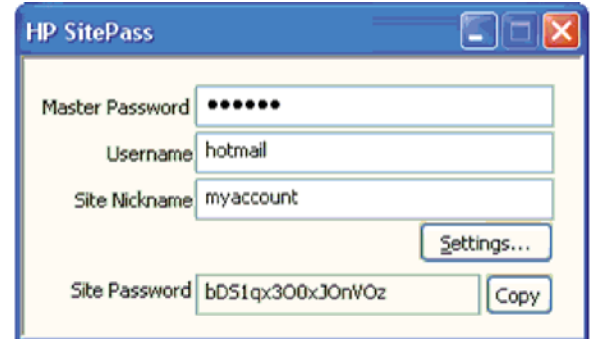
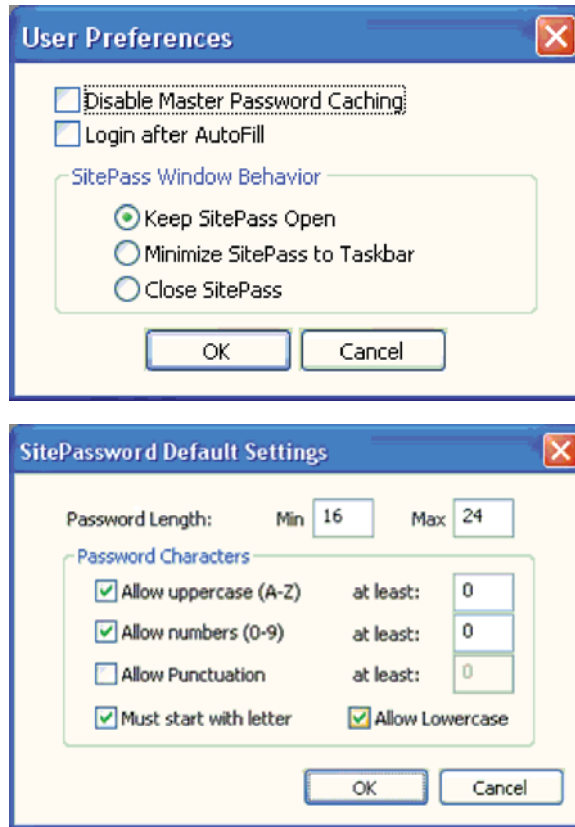
A simple solution: the HP Anti-phishing Toolbar

The HP Anti-phishing Toolbar tackles all four password safety problems. It is a simple, easy-to-use, non-intrusive, and very secure extension to Microsoft® Windows® Internet Explorer®. The HP Anti-phishing Tool Bar provides a text field to help users identify sites, calculate site-specific password, and complete login forms upon the click of a button.

Installing the HP Anti-phishing Toolbar adds two elements to the toolbar: a button and a text field (figure 1). The text field lets users assign a name to any secure site they visit. The name, comprised of any text, is associated with the organization name and the root CA (Certificate Authority) key. Once users set a name for a site, it appears in the text field every time they visit that site. If it doesn't display, then users know that something phishy is going on. If users pay attention to the HP Anti-phishing Toolbar field, they are protected against impersonators. And obvious color-coding provides visual cues to quickly identify a secure site.

Clicking the button causes the HP Anti-phishing Toolbar to compute a site-specific password (figure 2), based on a cryptographic operation with the master password. It automatically fills that password into the password field on the current page (the password generated is

Figure 2. The first time a user clicks on the HP Security Toolbar button, the Site Password window appears for entry of the master password. Once entered, a single click is sufficient to log in to any other site until the user closes this window. Nothing is ever stored on disk.



12 characters in length). As a further convenience, the text field can also keep track of the username. If a consumer adds a comma and username to the text field, the HP Anti-phishing Toolbar completes both the username and the generated password upon clicking the button. This is especially handy for different usernames at different secure sites.

With the HP Anti-phishing Toolbar, logging in is easy: just click the button. It's also safer: each site gets a different password, and because the site name cannot appear without the correct SSL certificate, the button simply won't work at an impostor's site. It also satisfies the FFIEC requirement for two-factor authentication.

Competitive approaches: Partial solutions

The HP Anti-phishing Toolbar is not the first anti-phishing tool. But the toolbar uniquely addresses all four password problems while providing its benefits on existing password-protected websites. Some tools display the site name from the SSL certificate, optionally with a user-selected logo. Others display a risk rating and the hosting country of the current

website. With both solutions, the user is likely to be focusing on the password-entering task rather than examining the indicator.

Another solution displays a user-selected image with the password prompt. The user is expected not to enter a password if the image is wrong or missing. Again, because users must enter the password, they may not recall that an image should display. This is easy to forget because only a few sites have adopted this technology. This solution also requires significant changes to the website; a user cannot choose to use the system on other websites.

Another solution automatically hashes the passwords entered in ordinary password fields with the domain name of the site. An impostor site would receive a different password because it resides at a different domain. Although this tool allows users to have a unique password per site, it does not help users identify sites. Thus, after completing a fake login procedure, a site can ask the user for other personal data. With the HP Anti-phishing Toolbar, the user clicks on the button and discovers that the tool didn't fill in a password, indicating that something is unusual.

Another solution uses a "white hat/black hat" approach that identifies sites as valid or invalid. The PC must maintain a list for both valid sites (white hat)

and phishing sites (black hat). The problem is, the first time users go to a site that is not on either list, they cannot determine the status of the site. Should the user risk entering logon information or do nothing? If it is a phishing site and the user enters identity information before it is reported to Microsoft® as a phishing site, the user's identity has been compromised.

Smart cards, which are plastic cards usually about the size of a credit card, contain an embedded integrated circuit. Although smart cards can provide two-factor identification when visiting secure sites, the downside is that users may need a stack of them—one for each issuing entity.

Summary

The HP Anti-phishing Toolbar mitigates the risks of ID theft from phishing and pharming

HP Atalla Security Products offers enhanced anti-phishing technology for the consumer's browser. The HP Anti-phishing Toolbar sits among the browser's other tools. Users save reminders about the relationships they have with secure sites. The toolbar will display this reminder every time the user visits the sites. After following a link, users check that the expected reminder displays. If so, they know they are using the correct site. Visited websites cannot determine the contents of the HP Anti-phishing Toolbar. The displayed information is provided solely by the user—a crucial difference when compared to other anti-phishing toolbar solutions.

The HP Anti-phishing Toolbar also provides an integrated password utility that conveniently fills in the username and password for a secure site with a

single click. Users need to remember just one master password, and the toolbar utility generates a different password for each site. The Toolbar securely labels websites to keep users safe from fake sites and provides an immediate indication that the site can be trusted or that it may be a phishing site. Because the generated password depends on the site validation, the toolbar only sends a password to a website when the certificate has been verified. Access to a secure site is provided with one click and key strokes cannot be recorded or logged as a result.

Banks and other financial institutions are the primary targets for fraud because they represent 84% of the websites being phished and pharmed today. A bank, or other organization with online services, may offer the HP Anti-phishing Toolbar to their customers as another line of defense against phishing and pharming while advertising their brand as part of the integrated password utility. Their brand remains a part of their customer's browser no matter which websites they visit. Unlike other offerings, the HP Anti-phishing Toolbar takes advantage of the existing Internet infrastructure and does not require modification of existing servers to effectively protect against phishing and pharming attacks.

For more information

To learn more about the HP Anti-phishing Toolbar, contact your HP Atalla Security Products representative or visit www.hp.com/go/Atalla. Be sure to ask for your free 45 day HP Anti-phishing Toolbar trial!

To learn more, visit www.hp.com/go/Atalla

© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft Windows and Internet Explorer are registered trademark of Microsoft Corporation in the U.S. and other countries.

July 2006

