

Tools to Protect Against Identity Theft

Mario A. Garcia

Texas A&M University-Corpus Christi



Identity Theft - Definition



- Identity theft, Web spoofing, identity fraud are terms used to refer to crimes in which a cyber-criminal wrongfully obtains and uses another person's personal information in some way that involves fraud or deception.
- Identity theft is becoming one of the most common and attractive forms of theft in the world. It has affected millions of people in recent years.

Identity Theft – How to



- Cyber-criminals can gain access to personal information in many different ways.
 - “dumpster diving”,
 - social engineering,
 - scamming people into giving personal information to them.
 - hack into databases that contain people’s information,
 - abuse the access that they have been given through their employer,
 - illegally collect personal information that is entered into a computer by the user.
 - One of the most common attacks used by cyber-criminals is to scam people into giving up their personal information by deceiving individuals that they work for a legitimate business.

Identity Theft Facts



- The Federal Trade Commission (FTC) reported that about 10 million Americans were affected by identity theft.
- The cost to victims was approximately five billion dollars.
- According to the Anti- Phishing Working Group (APWG), 2,870 phishing sites appeared in March 2005, a 28% increase per month since July 2004.
- A survey sponsored by TRUSTe found 70% of the respondents had visited a phishing site;
 - over 15% admitted to having provided personal data to a phishing site;
 - US consumers have lost an estimated \$500 million as a result of these attacks.

Identity Theft Facts



- The US Secret Service and the San Francisco Electronic Crimes Task Force reported that an average of 30 attack sites are detected each day.
- The total dollar losses are estimated at more than \$54 million compared to \$17 million for 2001.
- A majority of these fraud complaints are intrusions, auction fraud, credit card/debit fraud, and computer intrusion.
- 15,244 unique phishing attacks and 7,197 unique phishing sites were reported in December 2005, with 121 legitimate brands being hijacked.

Characteristics of Attacks



- Logos. The spoof site uses logos found on the honest site to imitate its appearance.
- Suspicious urls. Spoof sites are located on servers that have no relationship with the honest site.
- The spoof site's url may contain the honest site's url as a substring (http://www.ebaymode.com), or may be similar to the honest url (<http://www.paypa1.com>).

Characteristics of Attacks



- IP addresses are sometimes used to disguise the host name (<http://25255255255/top.htm>).
- Others use @ marks to obscure their host names
(<http://ebay.com:top@255255255255/top.html>),
- Contain suspicious usernames in their urls
(<http://middleman/http://www.ebay.com>.)

Characteristics of Attacks



- User input. All spoof sites contain messages to fool the user into entering sensitive information, such as password, social security number, etc.
- Short lived. Most spoof sites are available for only a few hours or days – just enough time for the attacker to spoof a high enough number of users.

Characteristics of Attacks



- Copies. Attackers copy html from the honest site and make minimal changes.
- Two consequences are:
 - (i) some spoof pages actually contain links to images (e.g. logos and buttons) on the honest site, rather than storing copies,
 - (ii) the names of fields and html code remain as on the honest site.

Characteristics of Attacks



- Sloppiness or lack of familiarity with English. Many spoof pages have silly misspellings, grammatical errors, and inconsistencies.
- In the Best Buy scam, the fake web page listed a telephone number with a Seattle area code for a Staten Island, NY, mailing address.
- HTTPS is uncommon. Most spoof web sites do not use https even if the honest site does. This simplifies setting up the spoof site.

Characteristics of Attacks



- Most phishing attacks trick users into submitting their personal information using a web form.
- The appearance of a web site and its web forms are easy to spoof.

Characteristics of Attacks



- A web site can control what it looks like in a user's browser, so a site's appearance does not reliably reflect the site's true identity.
- Users tend to decide site identity based on appearance,
 - e.g., “This site looks exactly like the PayPal site that I have been to before. So it must be a PayPal site”.

Characteristics of Attacks



- Web forms are used for submitting insensitive data as well as sensitive data.
- Even though SSL encryption can indicate to the browser that the input data is sensitive, phishing sites do not use SSL and the browser fails to effectively visually differentiate an SSL connection from a non-SSL one.

Homepage

News

Economy

Culture

Sci-Tech

Special Reports

Weather

Polls

Your feedback

Contact Us

About Aljazeera

Code of Ethics

Services

Frequencies

Wednesday 30 August 2006, 19:27 Makka Time, 16:27 GMT

Hackers have stolen personal information - including credit card details - from thousands of customers of the US telecoms firm AT&T.

The company said on Tuesday that "fewer than 19,000 customers" were affected the theft - which affected customers of AT&T's online retail store.

The telecoms giant said it had shut down the store and contacted credit card companies to warn them of the theft, which took place at the weekend.

The company said the unauthorised access was found within hours of the breach.

A spokesman for AT&T, Walt Sharp, said no fraudulent credit charges had been reported so far.

Priscilla Hill-Ardoin, AT&T's chief privacy officer, said: "We recognise that there is an active market for illegally obtained personal information.

"We are committed to both protecting our customers' privacy and to weeding out and punishing the violators."

AT&T also said it would also pay for credit monitoring services to assist in protecting the customers involved.

The data theft involved people who had bought equipment for high-speed internet access.

**Hackers breached AT&T's network at the weekend****RELATED****Related:**

- [Israeli 'hackers' target Hezbollah TV](#)
- [Pro-Palestinian hackers hit Israeli sites](#)
- [Hackers take aim at web services](#)

Tools:

- [Email Article](#)
- [Print Article](#)
- [Send Your Feedback](#)

- Army blamed for Sri Lanka aid killings
- Prisoners donate hair to fight slick

Top Science & Technology Stories

- Universal backs free music site
- Europe putting sharks in the soup
- All clear for Atlantis
- Game on for Chinese heroes

**Fresh News**
Wherever You Are

AUDIENCE PANEL
Click here to join

Features**Tiger haven?**

[India hard pressed to save endangered species](#)
Jaqpreet Luthra

India's Silicon Valley

[Has Bangalore lost its byte?](#)
Sudha G. Tilak



Verified by Visa

Dear Visa® customer,

Before activating your card, read this important information for cardholders!

You have been sent this invitation because the records of Visa Corporate indicate you are a current or former Visa card holder. To ensure your Visa card's security, it is important that you protect your Visa card online with a personal password. Please take a moment, and activate for Verified by Visa now.

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

Activate Now for Verified by Visa

Thank you for your support.
Visa Service Department



VISA SECURITY PROGRAM

Printable page

→ Verified by Visa

[How It Works](#)

[Places to Shop](#)

[Participating Card Issuers](#)

[FAQ](#)

[Privacy & Security](#)

[Terms & Conditions](#)

[Zero Liability](#)

[Continuous Monitoring](#)

[Identity Theft Assistance](#)

[3-Digit Code](#)

[Visa Security Summit](#)

Verified by Visa

Protect your Visa card online with a personal password

Visa provides reassurance that only you can use your Visa card online. Learn more about the benefits of Verified by Visa.



Activate Now for Verified by Visa

Enter your card number (without spaces).

SUBMIT

[Privacy & Security](#) | [Terms & Conditions](#)

How It Works >

Learn how Verified by Visa protects your Visa card when shopping online.

Places to Shop >

Where can you shop with Verified by Visa? Find out here.

Participating Card Issuers >

Find out if your card issuer is participating.

FAQ >

Get answers to frequently asked questions about Verified by Visa.



➤ **Visa Security Tips**
Protect Yourself

➤ **Complete Fraud Protection**
Zero Liability



The forged address bar

- Verified by Visa
- How It Works
- Places to Shop
- Participating Card Issuers
- FAQ
- Privacy & Security
- Terms & Conditions

Verified by Visa

Protect your Visa card online with a personal password
Visa provides reassurance that only you can use your Visa card online. Learn more about the benefits of Verified by Visa.

Activate Now for Verified by Visa

Visa® Card Number:

Expiration Date (mm/yy):

Card Verification Value:

ATM PIN:

[Privacy & Security](#) | [Terms & Conditions](#)

How It Works
Learn how Verified by Visa protects your Visa card when shopping online.

Places to Shop
Where can you shop with Verified by Visa? Find out here.

Participating Card Issuers
Find out if your card issuer is participating.

Properties

General

Visa USA | Personal | Verified by Visa

Protocol: HyperText Transfer Protocol

Type: File

Connection: Not Encrypted

Address (URL): <http://200.251.251.10/.verified/>

Size: 20018 bytes

Created: 14.12.2004 r.

Modified: 14.12.2004 r.

The real URL

No secure session (lock) icon

Visa Identity Theft Analysis



- Even though the spoofed website looks different than the real site, it is still extremely convincing.
- The design of the page is clean and professional.
- In addition, the address bar is forged, aligning perfectly on the page and masking the actual URL of the page.
- Both pages have an address starting with <https://usa.visa.com>.

Visa Identity Theft Analysis



- The real URL of the page is visible in the properties page.
- The only other visible phishing clue is the missing padlock icon in the right part of the status bar, which is inconsistent with the 'https' in the forged address bar.
- In addition, the page does not contain any login screen.

Visa Identity Theft Analysis



- If the link is further examined, it turns out that it leads to the following URL:
'<http://usa.visa.com/track/dyredirect.jsp?rDirI=http://200.251.251.10/.verified/>'.
- This is a URL that is really on the visa.com page! It turns out that the phishers have used a redirect page on the visa.com site to redirect to the phish server.

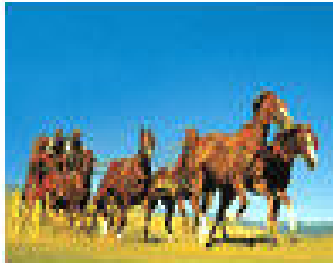
Visa Identity Theft Analysis



- To make the things even more convincing, the site checks the credit card number using a commonly available algorithm.
- This does not require or reveal any information about the bank account behind the CC, but it would reject a random bogus number, which could make the potential victim trust the site



WELLS
FARGO



Dear Wells Fargo Customer,

We are glad to inform you, that our bank is switching to new transactions security standards. The new updated technologies will ensure the security of your payments through our bank. Both software and hardware will be updated.

We kindly ask you to confirm your ATM card details here:

<https://online.wellsfargo.com/?customersupport=CONFIRMATION>

We offer you a new convenient and safe high-quality level of service to handle your ATM card.

© Wells Fargo Customer Support.



Search

The address bar is 'overwritten' perfectly

Not Yet Enrolled? It's Free!
Start viewing all your Wells Fargo accounts online.
> [Enroll Now](#)

Wells Fargo Transactions security standards update

Please enter your 16-digit Wells Fargo ATM card number, Expiration Date and PIN (Personal Identification Number).

As our bank is switching to new transactions security standards, we kindly ask you to confirm the details of your ATM card.

Note: your details will be transferred under secure HTTPS protocol and therefore cannot be intercepted or used by third parties.

ATM Card Number:

ATM PIN:

Expiration Date: (mm/yy)

Email Address:

Your email address will allow us to contact you regarding your online validation and use of *Wells Fargo*[®].

Yes, please keep me informed via email of new features, updates, and special offers at Wells Fargo.

[> Continue](#)

Brokerage Products: Not FDIC Insured • No Bank Guarantee • May Lose Value

Brokerage is offered through Wells Fargo Investments, LLC (member SIPC), a non-bank affiliate of Wells Fargo & Company and is intended only for United States residents. System response and account access times may vary due to a variety of factors.

No lock icon to indicate that the page is SSL secured

Wells Fargo Bank



- At first glance, it looks identical to the real Wells Fargo web page.
- The forged address bar is perfectly overwriting the “real” URL.
- However, the lock icon in the lower right corner of the page is missing, which contradicts with the ‘https’ displayed in the address bar.
- In addition, the true URL of the page can be seen by opening the properties page, which turns out to be <http://202.67.159.110:5180/index.php>.

Dear eBay User,

During our regular update and verification of the accounts,
we couldn't verify your current information.

Either your information has changed or it is incomplete.

If the account information is not updated to current information
within 5 days then, your access to bid or buy on eBay will be suspended.

go to the link below,

and re-enter your account information.

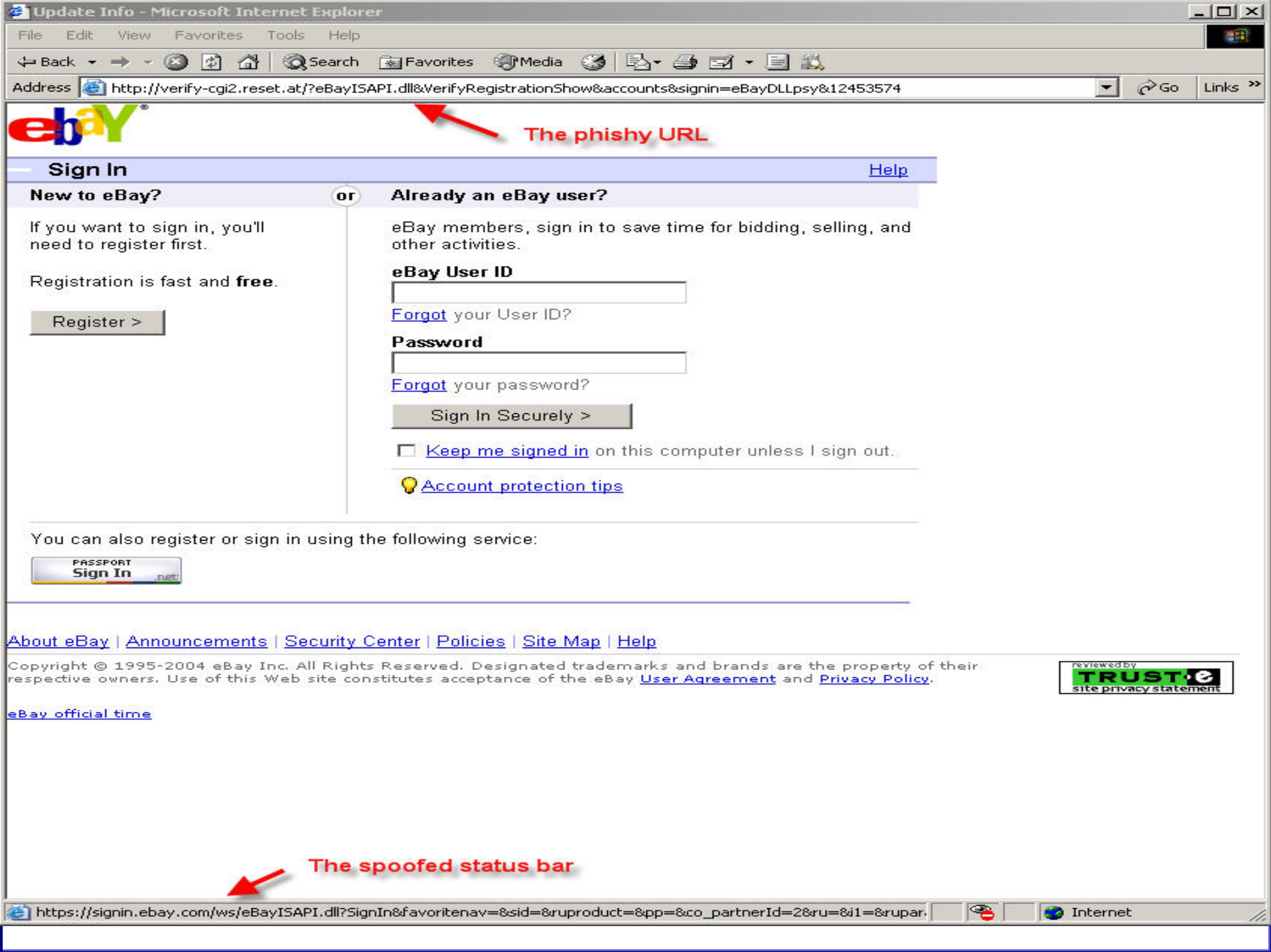
[Click here to update your account.](#)

*****Please Do Not Reply To This E-Mail As You Will Not Receive A Response*****

Thank you

Accounts Management

Copyright©1995-2005 eBay Inc.



ebay

Sign In [Help](#)

New to eBay?

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

[Register >](#)

or **Already an eBay user?**

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot](#) your User ID?

Password

[Forgot](#) your password?

[Sign In Securely >](#)

[Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#)

You can also register or sign in using the following service:

[PASSPORT Sign In .net](#)

[About eBay](#) | [Announcements](#) | [Security Center](#) | [Policies](#) | [Site Map](#) | [Help](#)

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](#).



[eBay official time](#)

The spoofed status bar



Online Banking Alert

Need additional
up to the minute
account
information?
[Sign In »](#)

Change of Email Address

Your primary e-mail address for Bank of America Online Banking has been changed.

- Did You Know? You can change your address, order checks and more online. [Sign in to Online Banking](#) and click on the "Customer Service" tab.

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact Bank of America with questions or comments, please [sign in to Online Banking](#) and visit the customer service section.



The legitimate site

Locations · Contact Us · Help · Sign In

PERSONAL ▾

Online Banking

[View demo](#) | [Learn more](#) | [Enroll](#)

Online ID:

 Remember my ID

Passcode:

Account in:

[Forgot your ID?](#)
[Reset passcode](#)

Nations Funds - Microsoft Internet Explorer

The popup window

Online Banking

Reset Passcode

Quick Help

Use this page to reset your passcode.

What do I need to know?

- To preserve your security

If you forgot your Online Banking passcode or would like to simply reset it, please complete all of the information, including your passcode.

Reset Passcode

Quick Help

Use this page to reset your passcode.

What do I need to know?

- To preserve your security, the **Back** button on your browser will be disabled while you are entering your personal information.
- Creating a unique online ID and passcode ensures that only you will have access to your accounts through Online Banking.
- When selecting your new passcode, consider modifying numbers that you already have memorized but that would not be obvious to someone attempting to guess.
- If you use uppercase or lowercase letters to reset your passcode, you must use the same capitalization whenever you sign in.

If you forgot your Online Banking passcode or would like to simply reset it, please complete all of the information, including your passcode.

State where your accounts were opened:

Online ID:
(5-20 digits)

Enter your passcode

Passcode:
(4-7 numbers and/or letters, case-sensitive)

Reenter your passcode:

Your ATM or Check Card Information

Your ATM or Check Card Number:

(Please enter the last eight digits of your ATM or Check Card in one of the following formats:
xxxx xxxx, xxxxx-xxxx, or xxxxxxxxx)

[Continue](#)

[Cancel](#)

Ameritrade Online Application



- This was first seen on April 22, 2005.
- The technology used for this was quite simple: merely a single-stage phish.
- This trick used the domain name, similar to the legitimate Ameritrade website, and tried to obtain the username/password for ameritrade.com accounts.

Thank you for opening your Ameritrade® account!

Your account must be funded before you can begin trading. For details about your funding choices, log on at www.ameritrading.net and choose Help Center from the Help menu. Then click Managing your account and Deposits.

You can make the most of your Ameritrade experience by checking out Ameritrade Streamer(TM)¹, setting up your watch lists, and taking a look at everything available to you under the Research menu.

Again, thank you for choosing Ameritrade. We look forward to serving you for years to come.

Sincerely,
Kenneth I Feldman
President, Private Client Division
Ameritrade





Secure Trading System Login

Log on

Please use your **UserID** and **password** to log on.

UserID:

Password:

Amerivest®

Amerivest changes all that with:

- Online portfolio advice.
- A simple, low annual fee.
- No trading commissions - no kidding!



Learn more about Amerivest!



*This product is not available to UK residents.

Need Help?

[Don't have a UserID yet?](#)

[Forgot your UserID?](#)

[Forgot your password?](#)

[Having trouble logging on?](#)

[Security Statement](#) | [Minimum Requirements](#) | [Cookies FAQ](#) | [Privacy Statement](#)

For technical/system questions contact a Client Services representative at 800-669-3900.

Unauthorized access and use is prohibited. Usage is monitored. Ameritrade, Division of Ameritrade, Inc., member NASD/SIPC. Ameritrade, and Ameritrade logo are trademarks or registered trademarks of Ameritrade IP Company, Inc. © 2005 Ameritrade IP Company, Inc. All rights reserved. Used with permission.



Client Log on

UserID / Account number

Password

Choose a start page

Home / Summary

[Log on assistance?](#)

The Asset Protection Guarantee

If you lose funds or securities from your account due to unauthorized activity through no fault of your own, we'll reimburse you.

We promise you this protection.

Log on and visit our [Security Center](#)



Ameritrade Online Application



- The only differences reported of this site are:
 - the domain name being relatively close,
 - the missing security certificate, and
 - the failure to see HTTPS on the URL.
- As soon as the false site had both text boxes filled, it would redirect the user to the real site.

Washington Mutual Bank



- This was first seen on February 24, 2005. The e-mail overall is believable and the redirected URL is cleverly chosen and quite close to the actual URL address of WAMU.

personal banking

PERSONAL
ONLINE BANKING

NEW ACCOUNT
CHOICES

LOANS &
CREDIT CARDS

CUSTOMER
SERVICE

secure 

Log On for Online Services

New to Online Services?

You'll need a User ID and password to:

- Access your accounts online
- Pay bills online - **new free!**
- Send us a secure message

[create User ID](#)

Returning User?

Personal Bill Pay™ service is free! To enroll or use, log on and select Pay Bills.

User ID:

Password: *

[Forgot your password?](#)

* Your Password is case sensitive and must be entered exactly as created (i.e. upper and lower case letters).

Need help? Use [Site Helper](#) or call **eCare®** Customer Service at 1.800.798.7000.

[Protect yourself against fraud.](#) Washington Mutual will never ask customers for their Password or PIN through e-mail or phone calls.

FDIC Insured

 EQUAL HOUSING LENDER

Confirm your Washington Mutual Online Account

First Name* MI Last Name*

E-mail Address*

Address*

City*

State*

ZIP Code*

ATM/Visa Check Card Number*

Expiration Date*

..

Card Verification Number*

PIN*

[next](#)

*Denotes required field

Need help? Use [Site Helper](#) or call **eCare**[®] customer service at 1.800.788.7000.

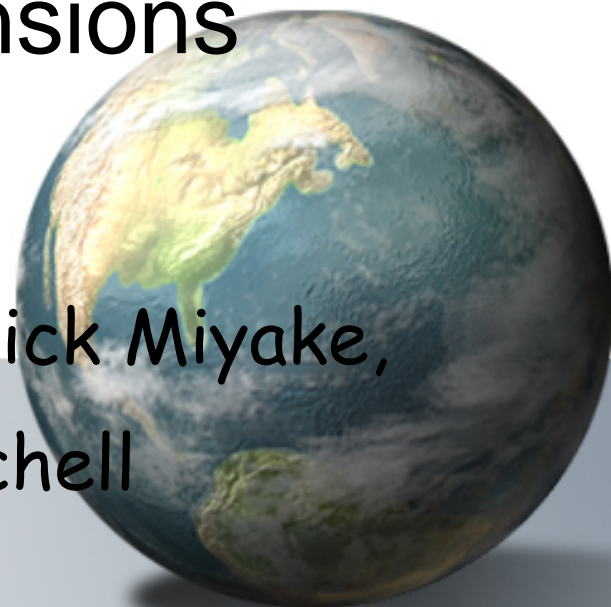
FDIC Insured
 EQUAL HOUSING LENDER

Stronger Password Authentication Using Browser Extensions

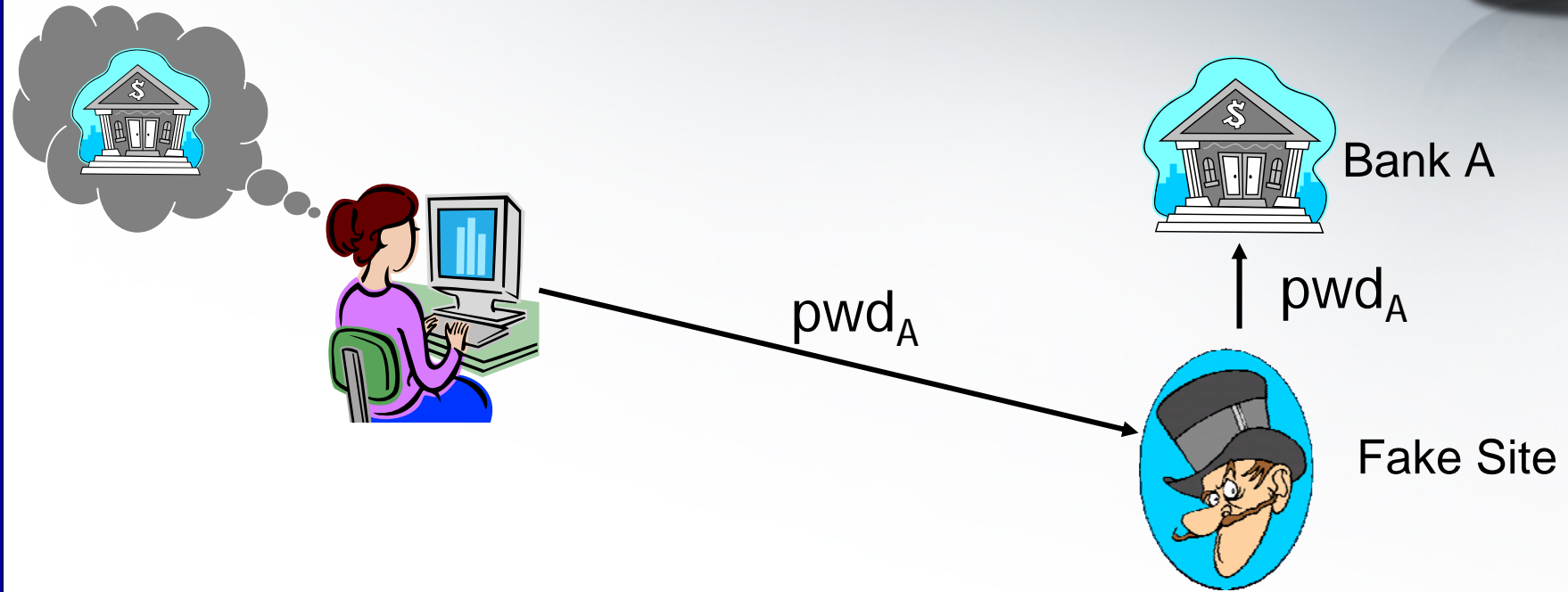
Blake Ross, Collin Jackson, Nick Miyake,
Dan Boneh, John Mitchell

Stanford University

<http://crypto.stanford.edu/PwdHash>

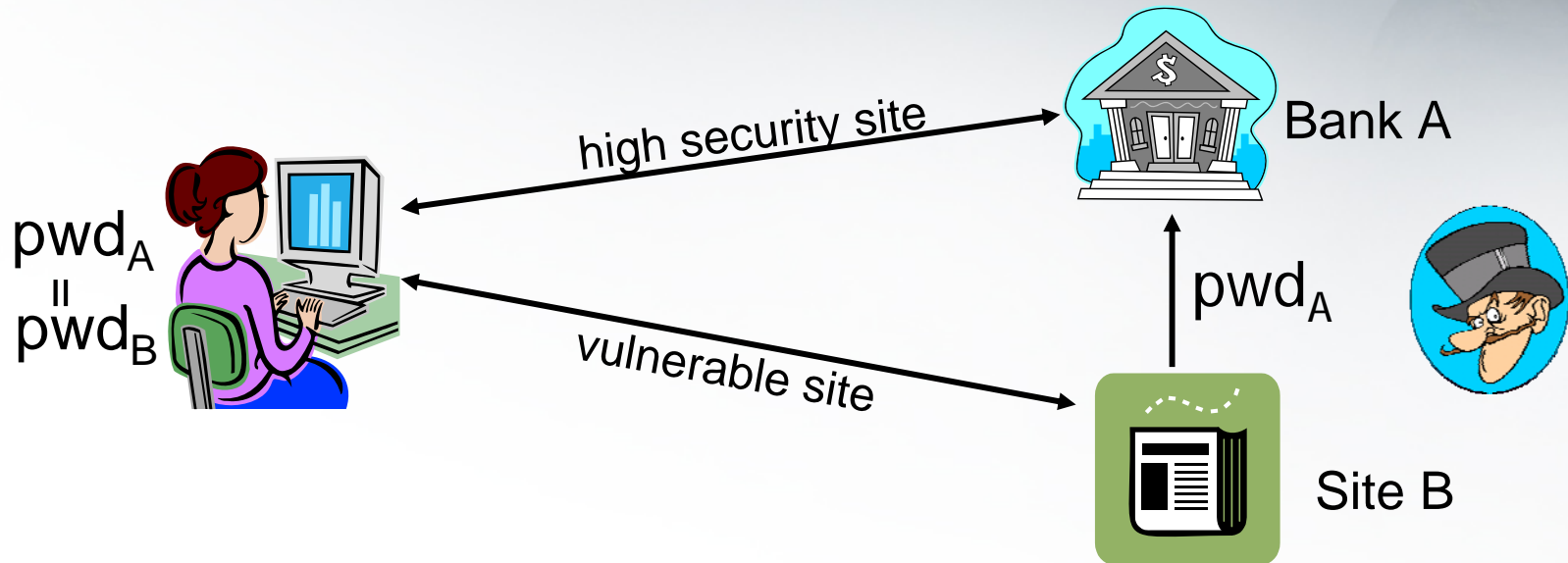


Password Phishing Problem



- User cannot reliably identify fake sites
- Captured password can be used at target site

Common Password Problem



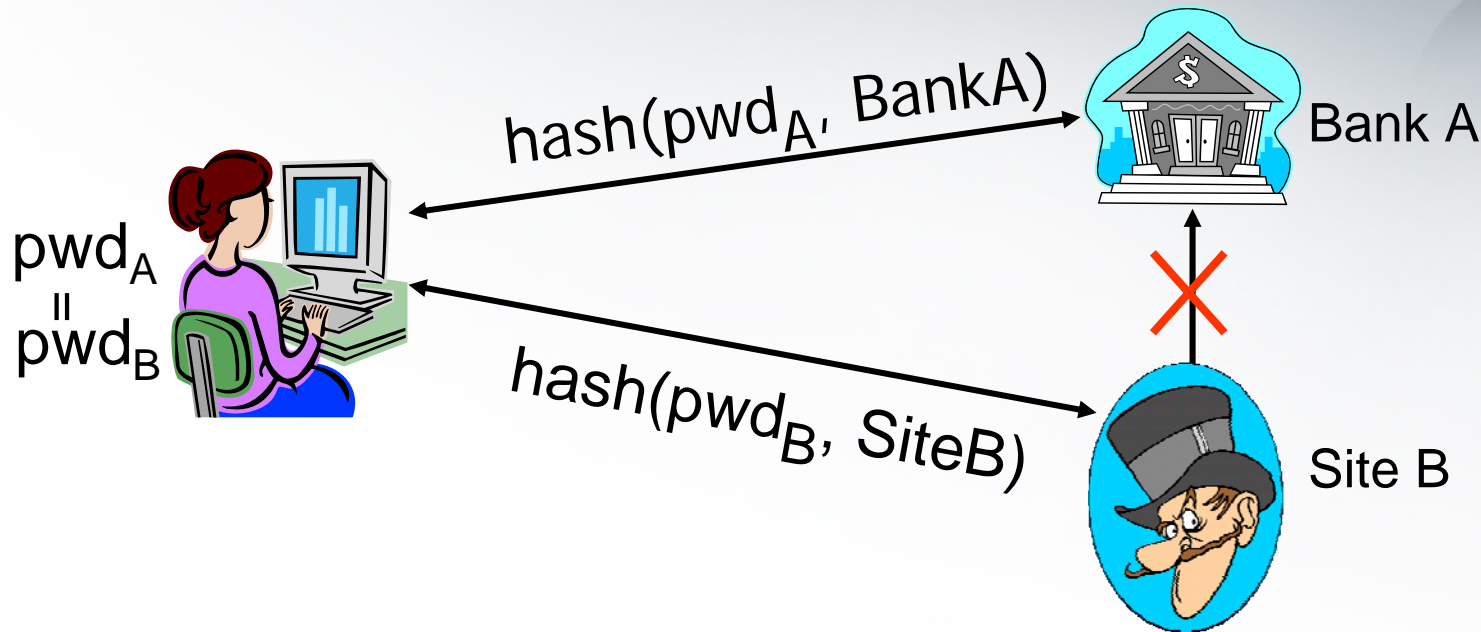
- ◆ Phishing attack or break-in at site B reveals pwd at A
 - Server-side solutions will not keep pwd safe
 - Solution: Strengthen with client-side support

Our Solution: PwdHash



- Lightweight browser extension
- Impedes password theft
- Invisible to server \Rightarrow Pwd Hashing
- Invisible to user \Rightarrow Pwd Prefix

Password Hashing



- Generate a unique password per site
 - $\text{HMAC}_{\text{fido:123}}(\text{banka.com}) \Rightarrow \text{Q7a+0ekEXb}$
 - $\text{HMAC}_{\text{fido:123}}(\text{siteb.com}) \Rightarrow \text{OzX2+1Cjac}$

The Spoofing Problem



- JavaScript can display password fields or dialogs:



Unhashed password sent
to attacker in clear

eBay User ID

joe_user

[Forgot](#) your User ID?

Password

...

[Forgot](#) your password?

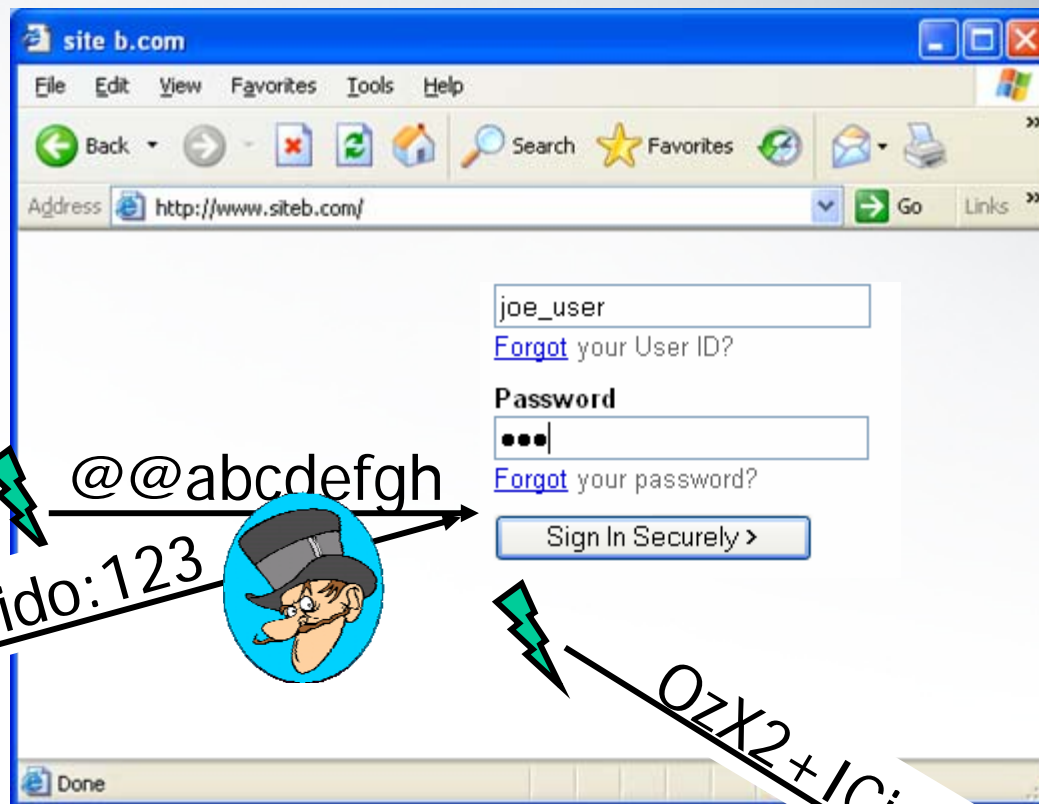
[Sign In Securely >](#)

LEADER, HONG KONG 2007

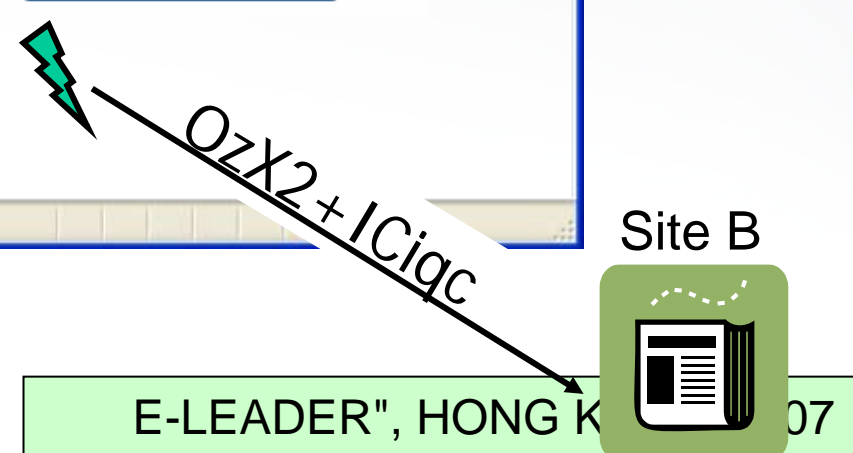
Password Prefix



- Original pwd should never be visible to web page



2/8/20



Site B



Password Prefix: How it works



- Normal operation: Prefix in password field

@@fido:123 \Rightarrow @@abcdefgh \Rightarrow *****

abcdefgh \Rightarrow fido:123

$\text{HMAC}_{\text{fido:123}}(\text{siteb.com}) \Rightarrow \text{Q7a+0ekEXb}$

- Abnormal operation: Prefix in non-password field

- Can just ignore the prefix and not hash
- Remind user not to enter password

Why use Password Prefix?



- Protection mechanism “built in” to password
- Does not rely on user to make a decision
- Same prefix works for everyone
- Distinguishes secure passwords from
 - normal passwords
 - social security numbers
 - PINs
- Only use it when you want to

Other Trusted Pwd Interfaces



- Password prefix
 - Passmark
 - DSS
- Secure attention sequence
- Trusted image or phrase:
 - Passmark
 - DSS




Starts with @@



LARGE **Log In**

Username:

PassMark:  **Maui Trip**
◀ Don't enter your password, until you see your PassMark.

Password:

E-LEADER", HONG KONG 2007

Other Challenges



- Password Reset
- Internet Cafes
- Dictionary Attacks
- Spyware, DNS poisoning (no protection)
- Other issues (described in the paper)
 - Choosing salt for hash
 - Encoding hashed password
 - Additional attacks and defenses

Password Reset



- After install, PwdHash can't protect existing pwds
 - Only passwords starting with @@ are secure
 - User can choose where to use PwdHash
 - User must enter old password unhashed into password reset page
- Pwd Prefix makes it easy
 - Old passwords won't be accidentally hashed
 - New, secure passwords are automatically hashed

Old password: [.....]

New password: [.....]

Re-enter password: [.....]

[Save Changes](#)

Starts with @@

Internet Cafes



- Users cannot install software at Internet Cafes.
- Would not be a problem if PwdHash were universally available
- Interim solution: A secure web site for remote hashing, e.g.

<https://www.pwdhash.com>

- Hash is computed using JavaScript
 - Server never sees password
 - Resulting hash is copied into clipboard
 - Can also be used as a standalone password generator

Site Domain
example.com

Site Password

Hashed Password
lc/FDyT1

Generate

[Switch to Advanced View](#)

Firefox

Site Domain
example.com

Site Password

Hashed Password

Copy to clipboard

Clear clipboard

[Switch to Advanced View](#)

Internet Explorer

Dictionary attacks



aardvark, aback,
abacus, abandon...

- After phishing attack or break-in to low security site, attacker can repeatedly guess password and check hash.
 - Succeeds on $\approx 15\%$ of passwords (unlike 100% today)
 - Less effective on longer, stronger passwords
- Solution: better authentication protocol (SPEKE, SRP, etc.)
 - Requires server-side changes
- Defense: user specifies a global pwd to strengthen all pwd hashes
 - Creates a new pwd management problem for shared machines
- Defense: slow hash function (Halderman, Waters, Felten '05)
 - Increases time of dictionary attack

PwdHash: Try it out



- Prototype for Internet Explorer and Mozilla Firefox
- Defends against spoofing
- Invisible to user
- Invisible to server
- Complementary to other anti-phishing solutions
- Only use it when you want to

www.pwdhash.com

Thank You



- Questions?