

Phishing: Technical Approaches to Combating The Threat

Economic Fraud and Digital Evidence
September 22nd, 2005

Valley River Inn, Eugene OR

Joe St Sauver, Ph.D. (joe@uoregon.edu)

University of Oregon Computing Center

<http://www.uoregon.edu/~joe/eug-fraud-phishing/>

This Talk

- This talk came about following a phishing talk I did for the Valley Fraud Group in Eugene; Sean invited me to adapt and share some material from that talk with a wider audience here today.
- This talk is intended to help you understand technical approaches to dealing with the phishing threat.
- To help me stay on track, I've laid this talk out in some detail; doing so will also hopefully make it easier for folks to follow what I'm trying to say if they end up looking at this talk after the fact.

My Background

- I've been at UO for going on 18 years now, and work for the UO Computing Center as Director, User Services and Network Applications; my Ph.D. is in Production and Operations Management.
- Part of what I do for UO involves a variety of security-related projects both at the campus and national level. For example, I'm one of three senior technical advisors for MAAWG (the carrier Messaging Anti-Abuse Working Group), I'm also co-chair for the Educause Security Effective Practices Group, and I sit on the Internet2 Security at Line Speed (SALSA) working group.
- Security-related topics I'm interested in include host security, network traffic analysis, email spam, open proxies/spam zombies, SCADA (process control) security, denial of service attacks... and phishing.

What Are Some Potential Bank Goals with Respect to The Phishing Problem?

- The obvious: control direct out-of-pocket losses, and
- Criminally prosecute phishers (just like armed robbers, embezzlers, people kiting checks, etc.)

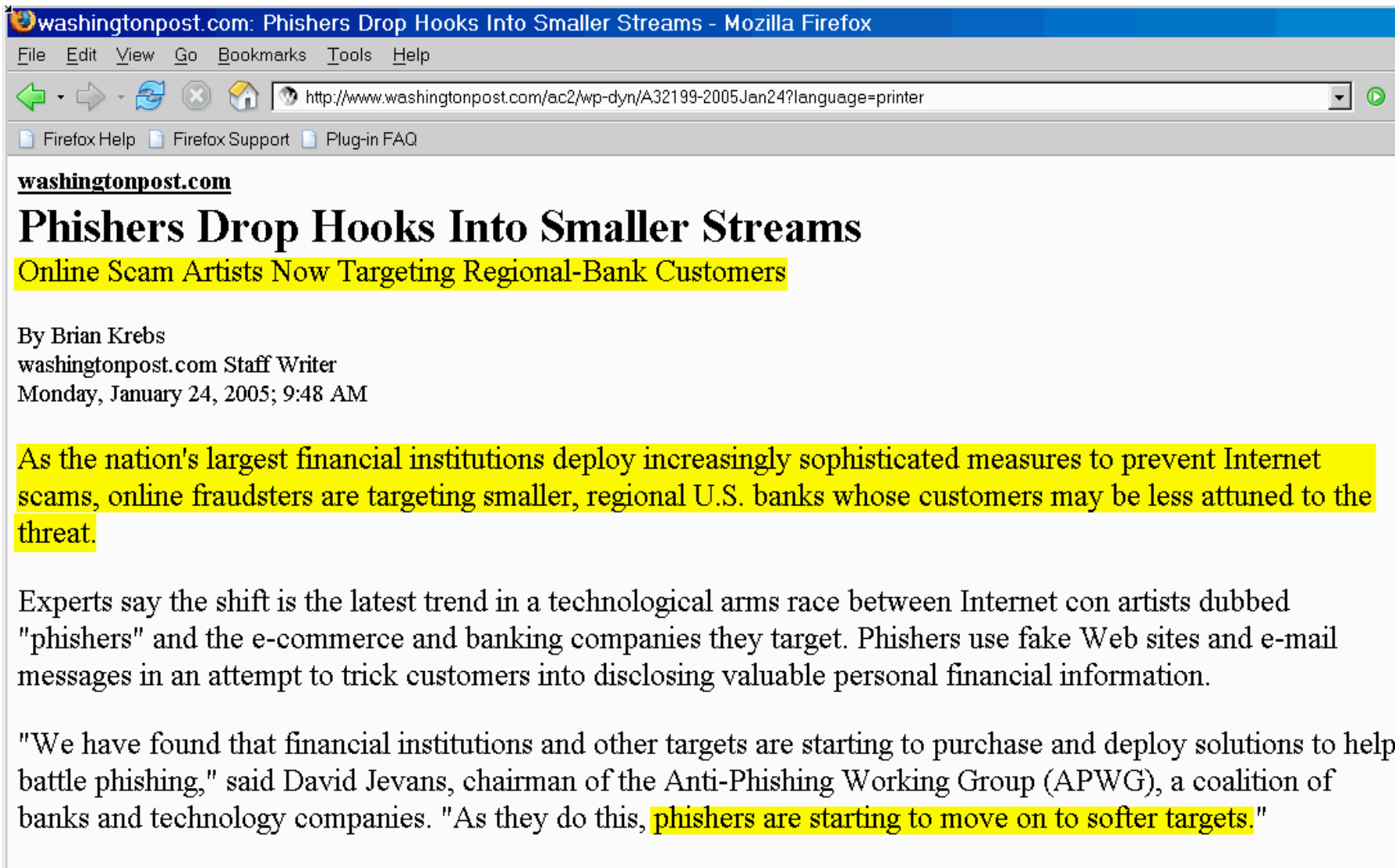
Institutional goals **SHOULD** probably also include...

- Preserve institutional reputation/avoid brand dilution
- Limit customer churn/retain market share
- Protect nascent online operational venues, e.g., insure that customers don't turn their back on online banking as being "too risky;" insure that bank emails doesn't start getting routinely ignored (or blocked outright as a result of phishing attacks), etc.
- Demonstrate due diligence in confronting emerging security threats; be responsive to regulatory mandates

Begin To Take Action NOW: Phishing IS a Problem For Banks in the Northwest, Today.

- There is an exceedingly dangerous trend I've noticed, which is the assumption by some entities that phishing is a problem for the "other guy," but not for them:
 - "We're too small to bother with" or "the phishers are only going after banks with a national footprint -- we're 'just' a regional" or even
 - "I'm a credit union (or brokerage, or ...) and they're only going after banks"
 - "We'll wait until we see widescale attacks, and deal with it then. No point worrying about vague rumors."
- That's flawed thinking. International or national, regional or local; bank, credit union, brokerage, card company, online merchants -- phishers are interested in Pacific Northwest banks right NOW.

Smaller Banks == "Softer Targets?"



The screenshot shows a Mozilla Firefox browser window with the title bar "washingtonpost.com: Phishers Drop Hooks Into Smaller Streams - Mozilla Firefox". The address bar contains the URL "http://www.washingtonpost.com/ac2/wp-dyn/A32199-2005Jan24?language=printer". The page content includes the Washington Post logo, the article title "Phishers Drop Hooks Into Smaller Streams", a subtitle "Online Scam Artists Now Targeting Regional-Bank Customers", the author "By Brian Krebs", and the date "Monday, January 24, 2005; 9:48 AM". The main text discusses how online fraudsters are targeting smaller, regional U.S. banks as larger financial institutions deploy more sophisticated anti-phishing measures.

washingtonpost.com

Phishers Drop Hooks Into Smaller Streams

Online Scam Artists Now Targeting Regional-Bank Customers

By Brian Krebs
washingtonpost.com Staff Writer
Monday, January 24, 2005; 9:48 AM

As the nation's largest financial institutions deploy increasingly sophisticated measures to prevent Internet scams, online fraudsters are targeting smaller, regional U.S. banks whose customers may be less attuned to the threat.

Experts say the shift is the latest trend in a technological arms race between Internet con artists dubbed "phishers" and the e-commerce and banking companies they target. Phishers use fake Web sites and e-mail messages in an attempt to trick customers into disclosing valuable personal financial information.

"We have found that financial institutions and other targets are starting to purchase and deploy solutions to help battle phishing," said David Jevans, chairman of the Anti-Phishing Working Group (APWG), a coalition of banks and technology companies. "As they do this, phishers are starting to move on to softer targets."

An Example Small CU That Was Targeted

<http://www.oaoa.com/news/nw041205g.htm>

‘Phishers’ target Odessa financial institution

Scam uses e-mail to get personal information

*By Julie Breaux
Odessa American*

Identity thieves targeted Complex Community Federal Credit Union in Odessa, casting bogus electronic e-mails to some of its customers over the weekend in a scam known as “phishing.”

The culprits victimized members and non-members, who unwittingly complied with requests for personal information from an e-mail that appeared to be from the credit union, said Lisa Wyman, director of marketing for CCECU.

Some Highly Targeted Institutions Are Located Here in the Pacific Northwest

- E.G., we've seen a few Washington Mutual phishing attempts (this is for one system with roughly 15K accounts, for 24 hours in each case; data shown is count, connecting host, plus envelope sender address)

Friday, January 21st, 2005:

```
680 vds-324155.amen-pro.com [62.193.212.177], account@wamu.com
666 vds-324155.amen-pro.com [62.193.212.177], service@wamu.com
655 vds-324155.amen-pro.com [62.193.212.177], support@wamu.com
647 vds-324155.amen-pro.com [62.193.212.177], confirm@wamu.com
630 vds-324155.amen-pro.com [62.193.212.177], security@wamu.com
```

Saturday, January 22nd, 2005

```
607 host166.hostcentric.com [66.40.38.166], confirm@wamu.com
579 host166.hostcentric.com [66.40.38.166], support@wamu.com
548 host166.hostcentric.com [66.40.38.166], service@wamu.com
542 host166.hostcentric.com [66.40.38.166], account@wamu.com
538 host166.hostcentric.com [66.40.38.166], security@wamu.com
```


Some Sense Of The Scale of What Folks Are Facing...


http://www.scmagazine.com/features/index.cfm?fuseaction=featureDe
ox Support Plug-in FAQ

Features

Washington has a new champion

by Illena Armstrong

Dave Cullinane, SC's CSO of the Year, tells Illena Armstrong why infosec professionals need to be at the center of decision-making – and the best way to kill phishing sites



As CISO of Washington Mutual, Dave Cullinane has shut down around 930 phishing sites since last October. Dealing with phishing attacks and overall identity theft issues has been one of the biggest challenges for this year's winner of *SC Magazine's* CSO of the Year award.

However, you wouldn't know it after reviewing the WaMu website, where consumers can gather tips on avoiding online scams, learn all about recent phishing emails, and report any suspicious activity directly to the Fortune 100 company. "It's becoming a much more pervasive problem than we ever anticipated, both in terms of the number of attacks going on [and] also in terms of the ramifications and the impact it is having," he says.

Or also see also http://antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf

Where Will Technical Approaches to Dealing With Phishing Come From?

- Banks and other financial institutions will naturally turn to you for online security advice much in the same way they look to you for advice about dealing with physical security or responding to crimes.
- When they do, what are some of the measures you could suggest?
- Well, let's begin by focusing on the most common way that phishing messages get delivered: email.

1. Publish SPF Records to Reduce Opportunities for Email Spoofing

Email: The Fundamental Internet User Application

- We have all come to rely on email, as imperfect as it may be.
- Email is the most common expression of individual identity (and thus reputation) – many people I've never met face-to-face "know me" by email address, and vice versa.
- Even though users shouldn't rely on email, they do:
 - even though email isn't an assured delivery service, email would usually go through (at least prior to content based/non-deterministic spam filtering)
 - historically email has (usually) been from whom it appeared to be from
 - users WANT to trust email
 - there's a lack of superior cost-effective alternatives

The Problem of SMTP Spoofing

- In technical circles it is understood that regular email has effectively zero protection against address spoofing
Trivial example of this: go into the options/settings/preferences for your favorite email client (Outlook, Eudora, whatever) and change your name and email address – bang, now you’re S. Claus, <santa@northpole.int>
- Phishers rely on email’s lack of protection from spoofing to be able to send email purporting to be from a target bank to users who **want** to trust that email.
- Historically, spoofed email could be sourced from anywhere – a rogue network in eastern Europe, a compromised broadband host in Missouri, or a cybercafé in Beijing all worked just fine.
- “The bank” could have been sending email from anywhere.

But Now We Have SPF!

- In a nutshell, SPF allows a domain owner to (finally!) say where mail from their domain should be coming from.
- Domain owners publish SPF records via the domain name system (the same Internet infrastructure that allows applications to resolve domain names like “www.uoregon.edu” to IP addresses “128.223.142.13”).
- Under the SPF draft standard, a domain owner publishes a new record in the domain system, a “TXT” (text) record, specifying where email for a particular domain should be “coming from” (implicitly, of course, this also defines where email should not be coming from). Finally a bank has the chance to say, “NO! Do not accept email that claims to be from my domain if it is coming from an a rogue network in eastern Europe, a compromised broadband host in Missouri, or a cybercafé in Beijing!”

Beginning to Learn About SPF

- The SPF protocol (“Sender Policy Framework”) is formally documented in an Internet Engineering Task Force draft:

[http://www.ietf.org/internet-drafts/
draft-schlitt-spf-classic-00.txt](http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-00.txt)

but a better starting point is the SPF project white paper:

<http://spf.pobox.com/whitepaper.pdf>

- One of the easiest ways to learn about SPF, however, is to check out an SPF record that’s actually been published by a domain...

An SPF Record Example: Citibank

- For example, consider citibank.com's SPF record:

```
% host -t txt citibank.com
citibank.com text "v=spf1 a:mail.citigroup.com
ip4:192.193.195.0/24 ip4:192.193.210.0/24 ~all"
```

- Decoding that cryptic blurb just a little:
 - we used the Unix “host” command to manually ask the domain name system: has citibank.com published a txt record? yes, they have...
 - that SPF txt record allows citibank.com mail from mail.citigroup.com or from hosts in the numerical IP address ranges 192.193.195.0 - 192.193.195.255 and 192.193.210.0 - 192.193.210.255
 - mail from all other locations should be treated as probably spoofed (~all = “soft failure”)

We Just Looked At An SPF Record Manually, But Mail Systems Can Check Automatically

- While we just checked for the presence of an SPF record manually, most popular mail systems can be configured to automatically check all received mail for congruence with published SPF records.
- Thus, IF a bank publishes an SPF record, and IF the ISP that received “the bank’s” mail checks the SPF records they’ve published, spoofed mail that claims to be “from” their domain can then be rejected outright, or filed in a junk folder with spam and other unwanted content.
- While SPF is new, many banks are already publishing SPF records, and many ISPs are already checking them.
- Examples of some entities that have published SPF records include...

% host -t txt usbank.com

usbank.com text "v=spf1 mx a:mail5.usbank.com a:mail6.usbank.com
mx:mail1.usbank.com mx:mail2.usbank.com mx:mail3.usbank.com
mx:mail4.usbank.com ~all"

% host -t txt therightbank.com

therightbank.com text "v=spf1 mx mx:therightbank.com
ip4:206.107.78.0/24 ip4:208.2.188.0/23 ip4:208.35.184.0/21
ip4:208.29.163.0/24 ip4:209.195.52.0/24 ip4:207.1.168.0/24
ip4:63.172.232.0/21 ip4:208.147.64.0/24 ip4:65.205.252.0/24
ip4:207.1.168.0/24 ?all"

% host -t txt bankofamerica.com

bankofamerica.com text "v=spf1 a:sfm02.bankofamerica.com
a:sfm04.bankofamerica.com a:vamx04.bankofamerica.com
a:vamx02.bankofamerica.com a:txmx02.bankofamerica.com
a:txmx04.bankofamerica.com a:cr-mailgw.bankofamerica.com
a:cw-mailgw.bankofamerica.com ?all"

% host -t txt americanexpress.com

americanexpress.com text "v=spf1 include:aexp.com ~all"

% host -t txt smithbarney.com

smithbarney.com text "v=spf1 a:mail.citigroup.com ~all"

% host -t txt ebay.com

ebay.com text "v=spf1 mx include:s._spf.ebay.com
include:m._spf.ebay.com include:p._spf.ebay.com
include:c._spf.ebay.com ~all"

[etc]

Regretably, Many Institutions Have Still NOT Yet Published SPF Records...

- An unfortunately long list of folks have NOT yet published SPF records. Guess who the bad guys will target for their next phishing attack? The domains that have published SPF records or those who haven't?

bankofny.com
bankone.com
bbandt.com
centennialbank.com
chase.com
comerica.com
firstunion.com
jpmorgan.com
key.com
lasallebank.com
mastercard.com
etc., etc., etc.

nationalcity.com
oregoncommunitycu.org
pncbank.com

selco.org
suntrust.com
visa.com
wachovia.com

wellsfargo.com
worldsavings.com

- This list grows smaller each time I give this talk. :-)

When A Bank Publishes SPF Records, Make Sure They Publish for ALL Their Domains

- ```
% host -t txt citizensbank.com
citizensbank.com text "v=spf1 mx mx:12.46.106.20
mx:12.154.167.140 mx:12.154.167.156 mx:12.46.106.21
a:mailgw02.citizensbank.com ~all"
```

**BUT (at least on April 21st, 2005):**

```
% host -t txt citizensbankonline.com
[nothing]
```

Both of those domains are registered to:

```
Citizens Bank
1 Citizens Plaza
Providence, RI 02903
```

Guess which one we saw used in an actual phish?

# Publishing An SPF Record...

- Have bank staff review the SPF Whitepaper (really, *please*, RTFM :-))...<http://spf.pobox.com/whitepaper.pdf>
- Make sure they get managerial/institutional “buy-in”
- They should then figure out where their mail will legitimately be coming from (including any authorized business partners)
- They then need to decide what should happen to mail that’s coming from a “wrong place” – hard fail? Soft fail? Just note/log its existence, starting gently at first?
- Next they then run the SPF Wizard to help them craft an initial SPF record: <http://spf.pobox.com/wizard.html>
- Check it with <http://freshmeat.net/projects/spfval/> or <http://www.vamsoft.com/orf/spfvalidator.asp>
- Their DNS people then publish their SPF records and refine them based on any issues they run into

# Making Tea vs. Boiling the Ocean

- **Note:** publishing SPF records and checking SPF records on your local servers are fully independent activities and a bank or ISP can do one without having to do the other.
- **Also Note:** a bank can publish very broadly inclusive and very soft and gentle SPF records initially. There is much to be said for an incremental strategy that "gets a foot in the door" and provides experience with the protocol and sets a precedent; records can always be tightened down, or made less inclusive over time.

# One Caution: SPF May Not Actually Be Doing What You Think It 'Should' Be Doing

- Often casual email users may not understand that email really has three (3) “from” addresses of one sort or another:
  - the IP address (and potentially a domain name) associated with the connecting host that’s handing you the mail message (think “Received:” headers here)
  - the MAIL FROM (“envelope”) address, as is usually shown in the even-more-obscure/usually-unseen-and-ignored Return-path: header of a message), and
  - the message body “From:” address (the one that casual users commonly see associated with each mail message)
- SPF potentially checks **2** of those **3** addresses. Guess which one of the three it **DOESN’T** check? Correct, it does **NOT** check the message body “From:” address you normally see in your email reading program.

# Obligatory Slide: SPF vs. SenderID

- Because SPF looks at the "wrong" header from the point of view of a casual email user, Microsoft tried to promote an alternative, SenderID, that tried hard to look at the sort of From: headers that users would normally see. See <http://www.microsoft.com/mscorp/twc/privacy/spam/senderid/default.msp>
- It received a rather luke-warm-to-hostile reception in some circles, probably due to a variety of factors:
  - knee-jerk reaction to anything that comes from MS,
  - intellectual property/patent/licensing issues involved (see for example <http://www.apache.org/foundation/docs/sender-id-position.html> ), and
  - some legitimate technical concerns.
- Bottom line: classic SPF is what's getting deployed



# Remember: SPF is Meant for Mail Servers

- In spite of SPF looking at what end users may think of as the "wrong" source information, it **can be** QUITE helpful.
- SPF is designed to be used by MTA's (e.g., the mail software that runs on mail servers, such as sendmail, postfix, exim, qmail, etc.) at the time the remote mail sending host is connected to the local mail server. It is not really designed for MUA's (e.g., the mail software that runs on your desktop PC, such as a web email client, Eudora, Outlook, Thunderbird, etc.)
- Verifying where mail comes from at connection time is radically different from verifying the CONTENTS of the message, including the message's headers (including those pesky message body From: addresses that people see in their mail programs). Cryptographic approaches are more appropriate for this; we'll talk about them next.<sup>25</sup>

## **2. Encourage Digital Signing of the Messages That Are Sent to Customers**

# Making Sure That Real Email Remains Credible

- While publishing SPF records will help to reduce the amount of spoofed phishing email users receive, what about the legitimate mail that businesses would like to send to their customers? Does the phishing problem mean that they need to abandon use of email as a communication channel?
- No... However, they SHOULD be moving toward digitally signing all business email.
- Digital signatures allow bank customers to cryptographically verify that the message they received was really created by the party who signed it. Other mail will either be unsigned, signed with a key belonging to a different party, or fail to pass cryptographic checks when the signature is tested.

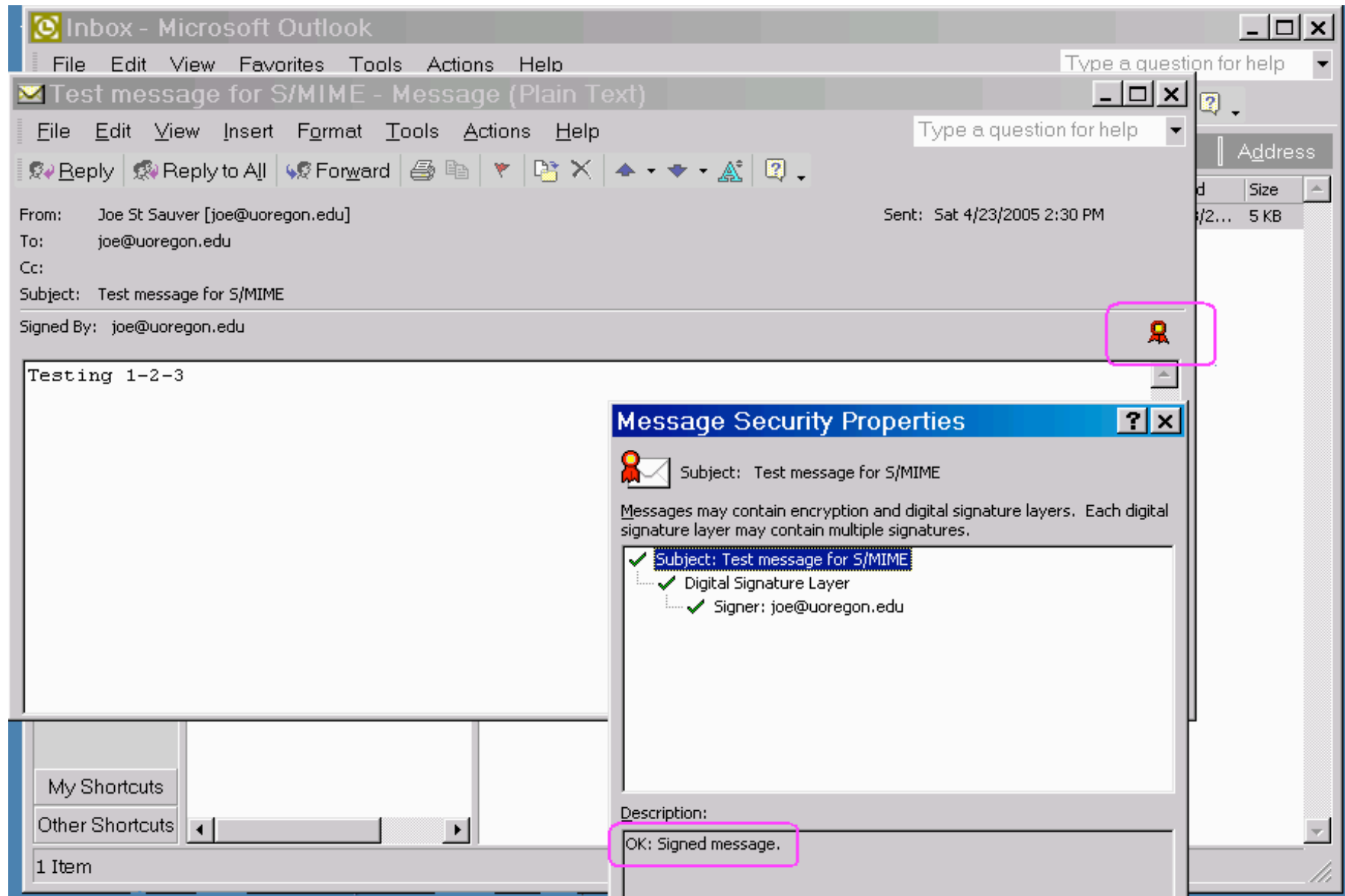
# Digital Signing Is NOT Message Encryption

- Sometimes there's confusion about the difference between digitally signed mail and encrypted mail.
- Mail that's been digitally signed can be read by anyone, without doing any sort of cryptography on the message. Yes, there will be additional (literally cryptic!) "stuff" delivered as part of the message (namely, the digital signature), but the underlying message will still be readable by anyone who gets the message whether the signature gets verified or not.
- Mail that's been encrypted, on the other hand, can ONLY be read after it has been decrypted using a secret key.
- The vast majority of "push" communications from a bank to its customer need NOT need be encrypted, but ALL bank email should be digitally signed.

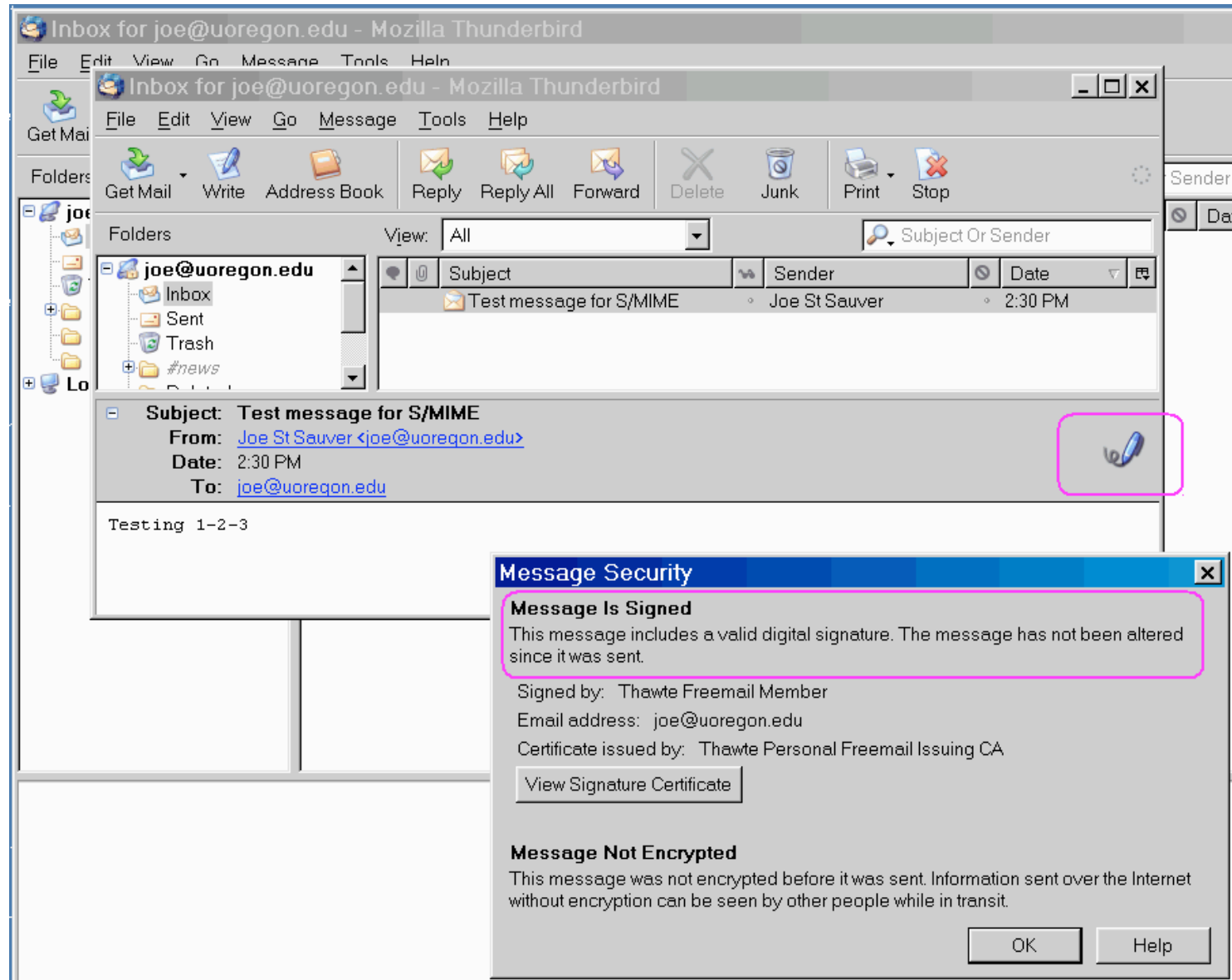
# Will Customers Even *Know* or CARE What a Digital Signature Is?

- We know/agree that many customers won't have the slightest idea what a digitally signed message is (at least right now).
- Over time, however, more users WILL begin to expect to see important messages signed, including messages from their bank (or other financial institutions), just as consumers now routinely expect to see e-commerce web sites use SSL to secure online purchases.
- Think of digital signatures for email as being the email equivalent of the "little padlock" icon on secure web sites
- For example, if you receive an S/MIME signed email in Outlook or Thunderbird today, it automatically "does the right thing"... here's what that would look like...

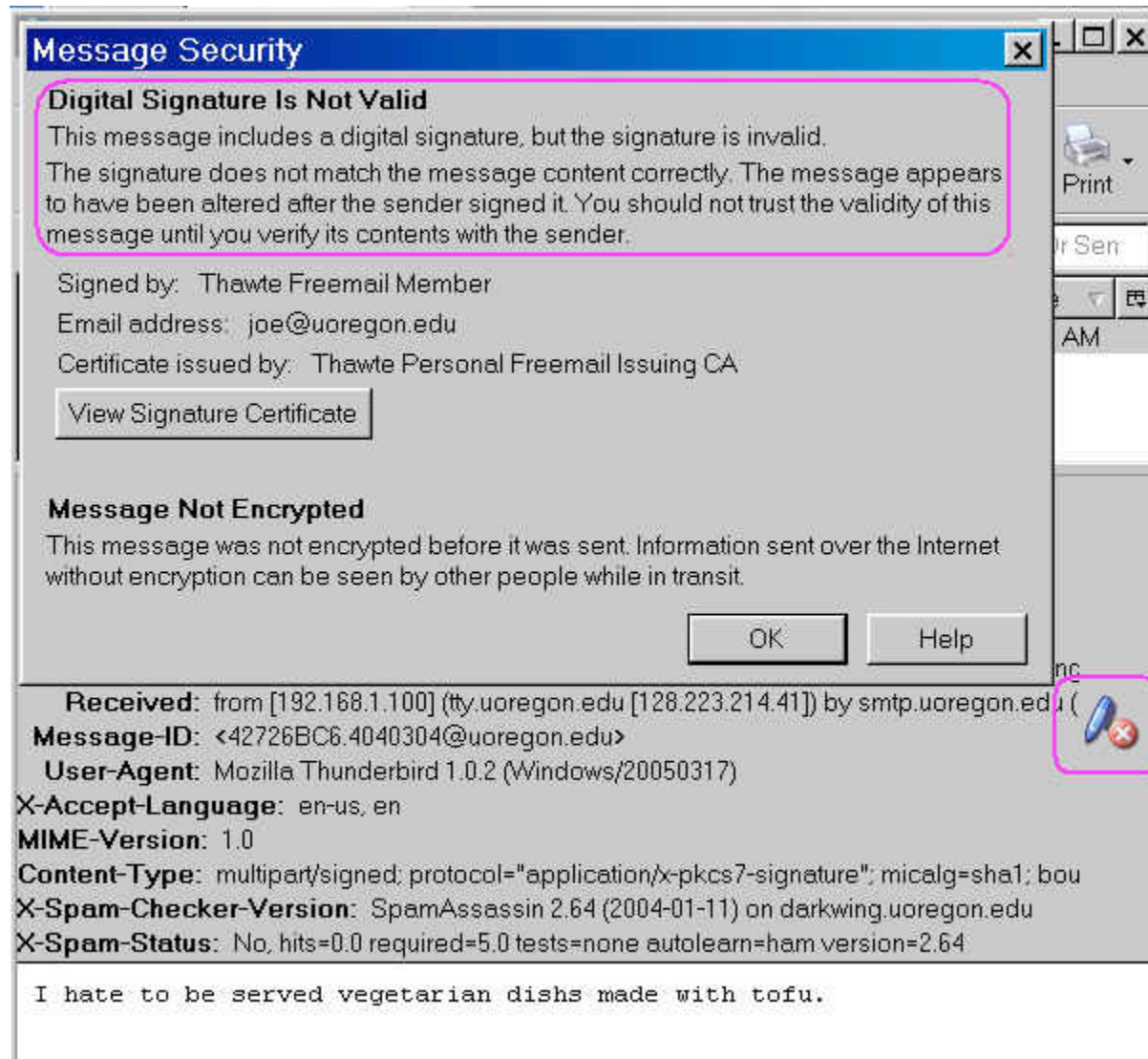
# An S/MIME Signed Message in Microsoft Outlook



# An S/MIME Digitally Signed Message In Thunderbird



# What Do Users See When A Signed Message Has Been Tampered With?





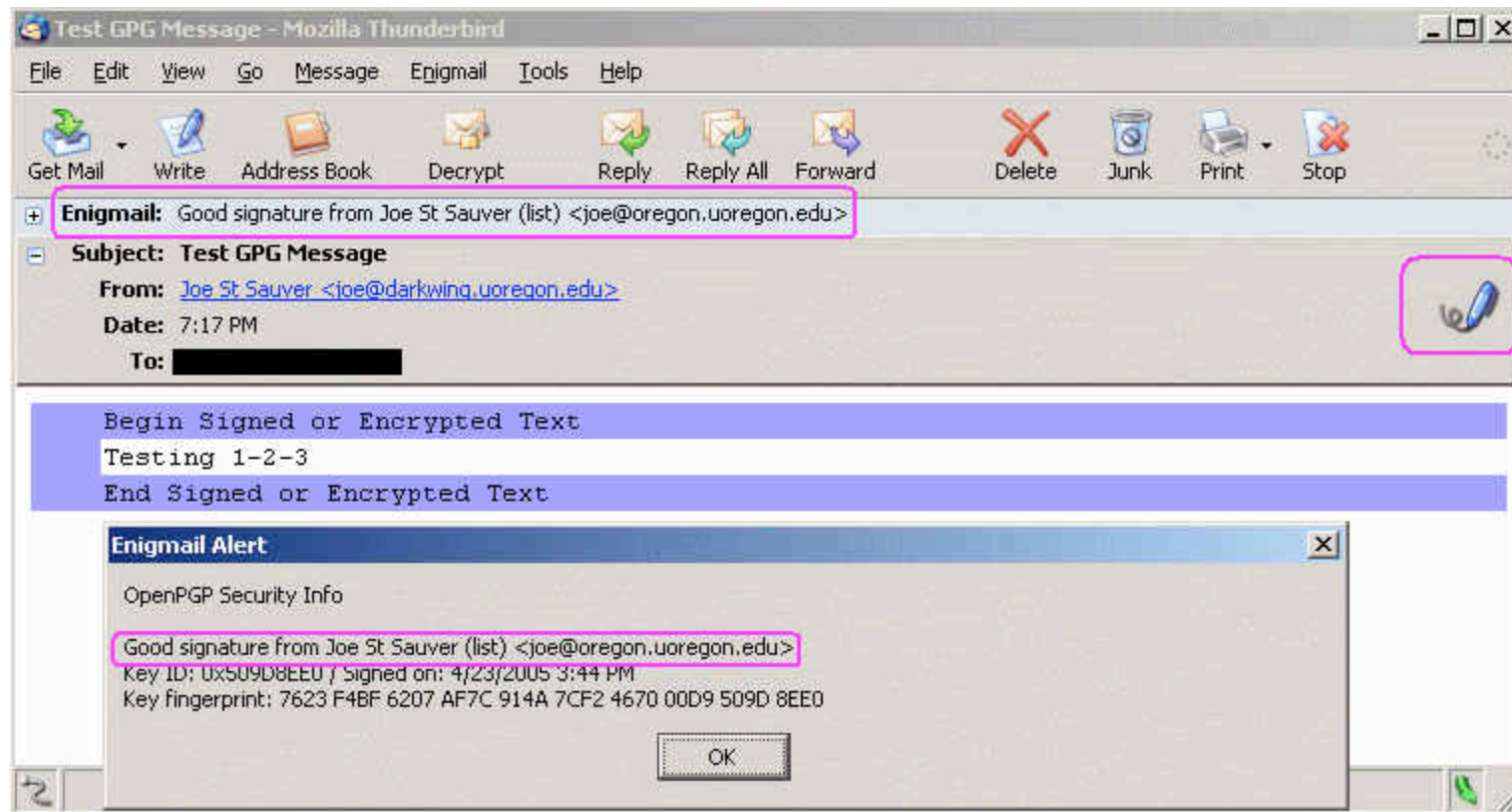
# Trying S/MIME Yourself

- If you'd like to experiment with S/MIME signing, you need a certificate. You can obtain a free personal email certificate from:
  - Thawte (Verisign, Mountain View, CA, USA):  
<http://www.thawte.com/email/>
  - Comodo (Yorkshire, UK):  
<http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>
  - ipsCA (Madrid, Spain):  
<http://certs.ipsca.com/Products/SMIME.asp>

## **Those Examples Were Using S/MIME, But You Could Also Use PGP**

- PGP (and its free analog Gnu Privacy Guard) can also be used to digitally sign emails.
- PGP/GPG is quite popular with technical audiences, and rather than using a hierarchical certificate authority-focused model, PGP/GPG users share their public keys via Internet-connected PGP/GPG key servers.
- The trustworthiness of any freely available individual public key on one of those key servers is recursively a function of the trustworthiness of the keys (if any) that have cryptographically signed the key of interest. This is known as the PGP/GPG "web of trust."
- Alternatively, if you have direct contact with a PGP/GPG user, they may simply confirm the fingerprint of their public key to you person-to-person..

# Example of a GPG Signed Message Being Read in Thunderbird with Enigmail



- It may be worth noting that the disconnect between the message "From:" address and the address in the PGP signature of the payload did not cause any alerts/issues.

# Onesie-Twosie vs. Institutional Usage

- While individual users employ S/MIME or PGP/GPG on a onesie-two message basis, the trick to broadly deploying digital signatures for email is to scale signing to corporate volumes, insuring that usage is consistent, key management is handled cleanly and non-intrusively, etc. The bank president should not have to be holding GPG key signing parties. :-)
- Fortunately, both S/MIME and PGP/GPG can be mechanically/automatically applied to outbound email via a specially configured mail gateway host that will also handle key management.
- For example...

# An S/MIME Email Gateway Appliance



**MailGate Email Firewall** includes an Email Authentication Engine that allows you to automatically apply S/MIME digital signatures to outbound email at the gateway, based on policies you define. Digital signatures are based on S/MIME, the industry standard for email security, which is supported in Microsoft Outlook, Microsoft Outlook Express, Lotus Notes, and Novell GroupWise. Together these email programs have an installed base of more than 350 million email clients throughout the world, making Tumbleweed's solution easily and ubiquitously deployable.

- In case you can't read that URL, it is [http://www.tumbleweed.com/solutions/email\\_authentication.html](http://www.tumbleweed.com/solutions/email_authentication.html) or see [http://www.opengroup.org/smg/cert/cert\\_prodlist.tpl](http://www.opengroup.org/smg/cert/cert_prodlist.tpl) for a full list of OpenGroup-certified commercial S/MIME gateway products

# A PGP Email Gateway Product

## PGP Universal Server

PGP Universal Server provides automatic generation and management of keys/certificates, automatic encryption/decryption/digital signatures, as well as two-way policy enforcement. Email can be secured on internal servers (End-to-End) or just from the Gateway to external recipients. It interoperates with PGP Desktop, all PGP keys, and X.509 certificates.

### **PGP Universal Server – Gateway**

PGP Universal Server sits between your email server and the Internet or corporate SMTP gateway, automatically securing and enforcing policy for all outgoing and incoming messages. According to defined policy, PGP Universal Server proxies traffic between the DMZ and the outside world, automatically creating keys as needed; encrypting, decrypting, and signing messages as required; and finding recipient keys and locating other PGP Universal Servers.

## Note: Digital Signatures Are Not A "Magic Bullet"

- Digital signatures are NOT a magic bullet.
- For example, users need to be trained to interpret the presence of the "digitally signed" icon intelligently...
  - Certificates are NOT all alike when it comes to the amount of due diligence applied by the certificate authority prior to a cert being issued, and depending on the vetting done, you may or may not really know the identity of the person who's "behind" a given cert.
  - If you see the "message digitally signed" icon show up, click on it and see just what it can tell you!
  - Bad people can use digital signatures just like good people; carefully evaluate your signer's reputation & role.
  - Pay attention to what's been signed. Message payload? Message headers including the subject? The whole thing?
  - When was the signature applied? Recently? Long ago?<sup>9</sup>

# Learning More About S/MIME and PGP/GPG

- PGP: Pretty Good Privacy, Simson Garfinkel,  
<http://www.oreilly.com/catalog/pgp/>
- Rolf Opplinger, Secure Messaging with PGP and S/MIME, Artech, 2000, (ISBN 158053161X)
- Introduction to Cryptography (full text document on PGP)  
<http://www.pgpi.org/doc/guide/6.5/en/intro/>
- Brenno de Winter et. al., "GnuPrivacyGuard Mini Howto,"  
[http://webber.dewinter.com/gnupg\\_howto/english/GPGMiniHowto.html](http://webber.dewinter.com/gnupg_howto/english/GPGMiniHowto.html)
- Bruce Schneier, "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure"  
<http://www.schneier.com/paper-pki.html>
- Bruce Schneier, "Risks of PKI: Secure E-Mail"  
<http://www.schneier.com/essay-022.html>



## Obligatory Slide: What About DomainKeys?

- Yet another cryptographic approach, in use by Yahoo, Google, Earthlink, and others.
- DomainKeys is described at <http://antispam.yahoo.com/domainkeys> and is available as an under-development Internet draft: <http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-02.txt> (note that over time the dash 02 may increment to dash 03, etc.) and implementations are available from <http://domainkeys.sourceforge.net/>
- Only your institution can decide what approach will work best for you...

# Oh Yes: The Issue of Sheer Deliverability

- One more thing before we leave the topic of email: because of the number of phishing emails sent out in the name of some banks, banks that are particularly popular phishing targets may find that real mail from their domain is getting rejected outright; in other cases real mail may *appear* to be getting delivered, but may be getting silently filed in "probably spam folders" or otherwise not get to where it should go.
- Pay attention to your bounces!

# Programs Such as Bonded Sender

- If banks do develop problems with being blocked by some sites, one possible way of proving their real email is trustworthy may be participation in a program such as Bonded Sender (see <http://www.bondedsender.com/> ) or seeking Institute for Spam and Internet Public Policy accreditation (see <http://www.isipp.com/index.php> )
- Another possibility is the Spamhaus-proposed new .mail domain (see: <http://www.spamhaus.org/faq/answers.lasso?section=The%20.mail%20TLD> )  
[obligatory disclaimer – I've been asked to sit on the board as the higher ed rep for .mail if it is approved, so please feel free to factor that into any assessment]
- Best of all, however, by FAR, is to take steps to insure you're domain is NEVER an attractive target for phishers

### **3. Review How You Use Domains And Your World Wide Web Site**

# DNS: Another Fundamental Service

- Banks, along with just about everything else on the Internet, relies on the Domain Name System to connect users to Internet resources such as web sites.
- The Domain Name System does this by translating fully qualified domain names to IP addresses. For example:

`www.uoregon.edu ==> 128.223.142.13`

DNS can also be used to translate IP addresses to domain names, but for now, let's just focus on the name to address translation...

- DNS service is key: done right, users get to your site; if mistakes happen, well, maybe they don't...

# **Are You On Guard Against Opportunities For User Confusion and Accidental Web Redirection?**

- Are users who are trying to access bank web sites being accidentally misdirected elsewhere, either to another site that just coincidentally has a similar name, or to sites that have been set up to take advantage of common errors as a way of obtaining a large source of eyeballs for web advertising or for more nefarious purposes (like phishing)?
- What happens if a user makes a trivial error, like misspelling/mistyping a domain name or accidentally omitting punctuation, such as a period?

# One Example: US Bank

- **As expected (I think)...**

```
www.usbank.com ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.usbank.net ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.usbank.org ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.firstar.com ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.fbs.com ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.usbancorp.com ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.starbank.com ==> 170.135.216.181
 (U.S. Bancorp Licensing, Inc., St Paul MN)
```

**Different (but okay, I suppose)...**

```
www.usbank.info ==> SERVFAIL
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.usbank.cc ==> SERVFAIL
 (U.S. Bancorp Licensing, Inc., St Paul MN)
www.usbanks1.com ==> SERVFAIL
 (U.S. Bancorp Licensing, Inc., St Paul MN)
```

# One Example (continued)

- **Maybe NOT quite as expected... omit the first dot and you go to...**

wwwusbank.com ==> 64.15.205.155 (and multiple others)  
(Howard Hoffman, Palo Alto CA)

wwwfirststar.com ==> 208.38.61.228  
(PopularEnterprises LLC, Knoxville TN)

wwwfbs.com ==> 64.235.246.143  
(LaPorte Holdings, Los Angeles CA)

- **Add punctuation or "correct" some spelling and you go to...**

www.us-bank.com ==> 209.123.16.2  
(Cayman Trademark Trust, Georgetown, Grand Cayman)

www.us.bank.com ==> 66.240.173.8  
(VerandaGlobal.com, Inc., Clearwater FL)

www.usbankcorp.com ==> 204.251.15.173  
(DragonAsia, Manama FPO AE BH)



# What Happens If A User Omits The Second Dot In A Domain Name?

- In most browsers, if a URL doesn't directly resolve, the browser will attempt to add a .com extension by default. Thus, if you meant to enter `www.usbank.com` but accidentally enter `www.usbankcom` instead (missing the dot before the "com"), you'll go to `www.usbankcom.com` instead of `www.usbank.com`

`www.usbankcom.com ==> 212.227.34.3`  
(Csonaki Enterprises, Sammamish WA)

`www.usbanknet.com ==> 66.118.136.67`  
(Manila Industries, Bangkok TH)

`www.fbscom.com ==> 216.180.251.228`  
(First Business Solutions, Westmont IL)

# What About TLD-Related Issues?

- You've all probably heard about the unexpected "content" that one will get if one accidentally confuses whitehouse.gov with some other "whitehouse dot something-else" domains.

So what happens if a customer make a mistake with respect to a bank's domain extension?

In the case of our sample bank domain, they've covered many of the more common possibilities (.com, .net, .org, etc.), but perhaps there's still more work to be done...

# Some usbank.<something> Domains...

- `www.usbank.biz ==> 64.202.167.192`  
(Arshad Chhipa, Karachi Pakistan)  
`www.usbank.name ==> 64.202.167.129`  
(EOS-1, Inc., Los Angeles California, client hold status)  
`www.usbank.bz ==> 216.168.224.63`  
(David Levin, Fenton MO)  
`www.usbank.us ==> 206.207.85.33`  
(Yakov Yukhananov, Rego Park NY)  
`www.usbank.ca ==> 66.150.161.34` (and two others)  
(Scott Whiteford, Myrtle Beach SC)  
`www.usbank.co.uk ==> 62.59.29.59`  
(Jacques Veltman, Amsterdam NL)  
`www.usbank.museum ==> 195.7.77.20`  
(but the domain is "available")

Some other variants are also still unregistered or do not resolve; check your favorite generic TLDs and country codes (there are 240+ two letter ccTLDs listed at <http://www.iana.org/cctld/cctld.htm> ). Don't forget about internationalized domain names (with umlauts, etc.), too.

# This Problem Is Not Specific To A Single Bank

- For example, BankOne uses `http://online.firstusa.com/` for its online banking web site...  
`online.firstusa.com ==> 159.53.0.18 ==> NXDOMAIN`  
`firstusa.com` is registered to a a Wilmington DE address
- What happens if we accidentally omit that first dot and go to `http://onlinefirstusa.com/` instead?  
`Onlinefirstusa.com ==> 64.235.246.143 ==> NXDOMAIN`  
`onlinefirstusa.com` is registered to a Singapore address
- This coincidental similarity in names is no doubt simply an incidental/accidental/unintentional thing, but it still should make one go “hmm...”

Cardmember Services - Home - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://online.firstusa.com/

Log in | Help Center | Contact Us | Privacy Policy | Terms of Use

# CardMember services

January 24, 2005


Home Your Accounts Explore CardMember Services

Log In [Login Help](#)  
User ID: [Forgot User ID?](#)  
Password: [Forgot Password?](#)  
User IDs and Passwords are case-sensitive  
**LOG IN**

**Security at Login**  
Your login is secured using Secure Sockets Layer (SSL) technology. [Learn More](#)

**NEW USERS**  
Our site is easy to use and gives you FREE access to your accounts. See for yourself. [View a Demo](#).  
**GET A USER ID**

[UPDATED: Security notice on e-mail fraud.](#)  
[Apply for a Credit Card](#)  
[Apply for a Business Credit](#)




## CardMember services

Online account management is **fast, free and secure**.  
[Enroll in CardMember Services](#) today and start thinking about how you'll spend all the time you're going to save.

Get back to life.

|                                                                                                        |                                                                                                               |                                                                                                                                |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Visa Deals</b><br>Shopping made simple. <a href="#">View special offers from top web merchants.</a> | <b>Running Late...</b><br>No problem. Save the stamp and <a href="#">Make your payments online right now.</a> | <b>Why Pay More?</b><br>Don't be stuck with high interest rates. Transfer a balance today and save! <a href="#">Learn More</a> |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|



**Children in Asia  
Need Help Now**



**Save the Children®  
USA**

## Some Quick Questions About This Real FirstUSA Page That You Just Saw...

- What bank is that page *really* for? Where's the bank branding and logo usage that you'd normally expect?
- If that's a secure login page, to avoid confusion, why isn't the page URL "https" prefixed? (and no, the little padlock does NOT show at the bottom of the page where it should be) [Yes, I understand that parts of an insecure page can still be transmitted securely, but it still confuses users and makes it easier for the bad guys to do bad things.]
- So what does the "I accidentally forgot a dot" version of the FirstUSA page look like?

onlinefirstusa.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://onlinefirstusa.com/ Go

onlinefirstusa.com January 24th, 2005

*What you need, when you need it* [Bookmark this page](#) | [Make this your homepage](#)

Bank One Credit Card Pay Bill First Usa Online Services Credit Card Payment Bankone.com Credit Card Payments

| Popular Links        |
|----------------------|
| Bank One Credit Card |
| Pay Bill             |
| First Usa            |
| Online Services      |
| Credit Card Payment  |
| Bankone.com          |
| Credit Card Payments |
| Visa                 |
| Bank One             |
| Bill Pay             |

**Popular Categories**

|                                      |                                     |                                |
|--------------------------------------|-------------------------------------|--------------------------------|
| <a href="#">Bank one credit card</a> | <a href="#">Pay bill</a>            | <a href="#">First usa</a>      |
| <a href="#">Online services</a>      | <a href="#">Credit card payment</a> | <a href="#">Bankone.com</a>    |
| <a href="#">Credit card payments</a> | <a href="#">Visa</a>                | <a href="#">Bank one</a>       |
| <a href="#">Bill pay</a>             | <a href="#">Statements</a>          | <a href="#">Online banking</a> |
| <a href="#">Car rental</a>           | <a href="#">British air</a>         | <a href="#">United airline</a> |
| <a href="#">Sony</a>                 | <a href="#">Marriott</a>            | <a href="#">United</a>         |

**Favorite Categories**

|                                        |                                    |                                      |
|----------------------------------------|------------------------------------|--------------------------------------|
| Travel                                 | Money Savers                       | Gambling                             |
| <a href="#">Airline Tickets</a>        | <a href="#">Online Banking</a>     | <a href="#">Free Casino Games</a>    |
| <a href="#">Hotels</a>                 | <a href="#">Online Payment</a>     | <a href="#">Poker</a>                |
| <a href="#">Car Rental</a>             | <a href="#">Debt Consolidation</a> | <a href="#">Texas Holdem</a>         |
| <a href="#">Air Charter</a>            | <a href="#">Foreclosures</a>       | <a href="#">Blackjack</a>            |
| <a href="#">South Beach Hotels</a>     | <a href="#">Free Credit Report</a> | <a href="#">Casino</a>               |
| Services                               | Leisure                            | Learn More                           |
| <a href="#">Car Insurance</a>          | <a href="#">Music</a>              | <a href="#">Real Estate Training</a> |
| <a href="#">Mortgage</a>               | <a href="#">Dating</a>             | <a href="#">College</a>              |
| <a href="#">Business Opportunities</a> | <a href="#">Christian Singles</a>  | <a href="#">Weight Loss</a>          |
| <a href="#">Life Insurance</a>         | <a href="#">Cell Phones</a>        | <a href="#">Alcohol Treatment</a>    |
| <a href="#">Work From Home</a>         | <a href="#">Jewish Singles</a>     | <a href="#">MCSE Certification</a>   |

Search:  Search

Bank One Credit Card | Pay Bill | First Usa | Online Services | Credit Card Payment | Bankone.com | Credit Card Payments |

## Once You've Gone Down the Wrong Path...

- There are opportunities for persistent errors, once the user has erred once ("bookmark this page," "make this your homepage" links as listed on the page you just saw).
- Banks should consider: is it that easy for users to bookmark real online banking sites? What is your expectation for your users' home page? Is there a home page that you recommend they use, perhaps something like an "institutionally tweaked" version of a popular start page, prominently featuring a convenient link to the bank's real web site? (Regretably, most default bank home pages would make poor generic start pages for users, I'm afraid).



# What About Non-Institutional Content?

- Look at the off-by-a-dot sample page again.

About the point that someone notices "Christian Singles" and "Jewish Singles" and "Free Casino Games" and "Alcohol Treatment" links they will hopefully be getting suspicious, but there are real bank web sites which also include non-institutional links.

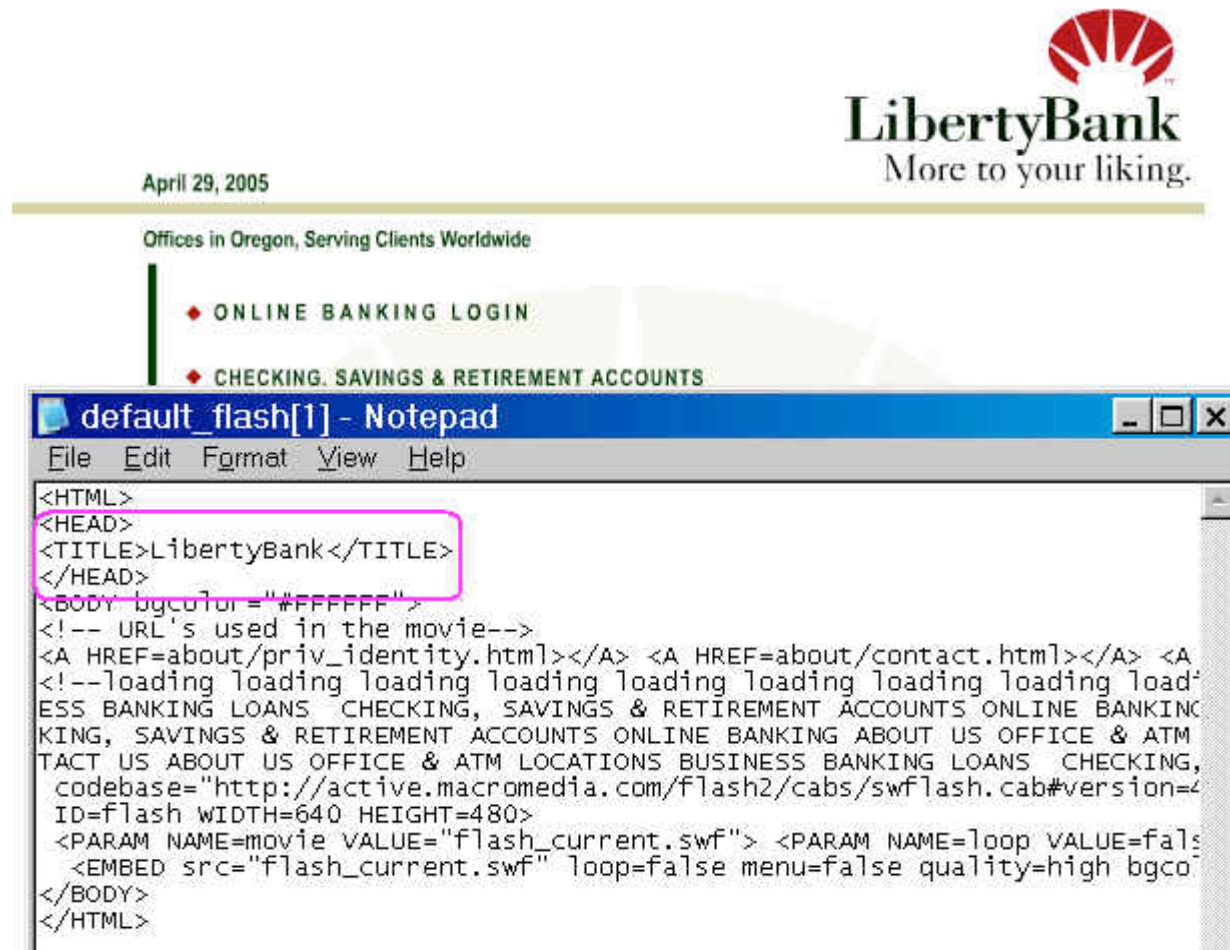
If you scroll back to the real bank page in this example, you'll see it links to "Save The Children" – unquestionably a worthy cause, but a dilution of the banks' web site's organic purpose and identity...

Sites should be conservative about anything that distracts from user assessment of a web site's identity.

# Search Engines and Meta Tags

- The content in the "blue bar" of the off-by-a-dot page indicates that the creator of this page is paying attention to the keywords people are searching for – institutional web sites should include keyword data "meta tags" in web page headers.
- You REALLY want to do EVERYTHING you can to make sure that your web site is easily indexed, and optimized to come up in the top spot on every search engine out there...

**Real site with no meta tags (and a homepage that redirects to a Flash interface that some search engines may index poorly if at all)**



# Result? 4th Place in Google

Address <http://www.google.com/search?hl=en&q=liberty+bank>

Google  Search Web PageRank 4 blocked AutoFill Options liberty

Google Web Images Groups News Froogle Local <sup>New!</sup> more »

Search [Advanced Search](#) [Preferences](#)

**Web**

**[Liberty Bank](#)**  
One of Connecticut's strongest independent community **banks** with 28 branches in the Hartford, New Haven and New London regions.  
[www.liberty-bank.com/](http://www.liberty-bank.com/) - 11k - [Cached](#) - [Similar pages](#)

**[Liberty Bank & Trust](#)**  
... \*Insurance products are offered by **Liberty** Insurance, Inc., a wholly owned subsidiary of **Liberty Bank & Trust Company** ...  
[www.libertybank.net/](http://www.libertybank.net/) - 21k - [Cached](#) - [Similar pages](#)

**[It's Your Bank ... Liberty Bank for Savings, Chicago, IL USA](#)**  
A locally owned, community oriented **bank**.  
[www.libertybank.com/](http://www.libertybank.com/) - 1k - [Cached](#) - [Similar pages](#)

**[LibertyBank](#)**  
... Online **Banking** Login Checking, Savings, and Retirement Accounts Loans Business **Banking** Office & ATM Locations About Us Contact Us Privacy ...  
[www.elibertybank.com/](http://www.elibertybank.com/) - 9k - [Cached](#) - [Similar pages](#)

**[Liberty Bank](#)**  
**Liberty Bank** has branches in Boulder Creek, Ben Lomond, and Felton.  
[www.libertybk.com/](http://www.libertybk.com/) - 3k - [Cached](#) - [Similar pages](#)

# 2nd Page/18th Spot on MSN Search, etc.

MSN Search: liberty bank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <http://search.msn.com/results.aspx?q=liberty+bank&first=11&count=10&FORM=PERE> Go Norton AntiVirus

Google Domain Keys Search Web PageRank 4 blocked AutoFill Options Domain Keys

[www.libertysb.com](#) [Cached page](#)

**LibertyBank**

... 2005 LibertyBank. All Rights Reserved. Unauthorized use of this website is strictly forbidden. ...

[www.elibertybank.com](#) [Cached page](#) 4/29/2005

**First Liberty National Bank - Home - Liberty, Texas, Dayton Financial ...**

... or Stolen , Please Call 800/554-8969! Thank you for visiting the Home Page of First **Liberty** National Bank . Please visit About Us to learn about the history of First **Liberty** National Bank. First ...

[www.flnb.com](#) [Cached page](#)

**Welcome to Northfield Savings Bank and Liberty Bank**

Northfield and **Liberty** represent two strong financial institutions joining together to give our mutual customers the benefits of financial strength, community commitment ...

[www.enorthfield.com](#) [Cached page](#)

**Liberty Bank Mortgages - Free Quotes** - [www.wizardofloan.com](#) SPONSORED SITES

Overview of Liberty Bank and their mortgage services. Review of their website plus a free link to an online loan quoting...

**Liberty Bank** - [www.mortgage-reviews.com](#)

Find out more about Liberty Bank, and get up to four free mortgage quotes from some of the nation's leading banks and lenders...

**Liberty Bank: In-depth Company Info** - [www.hoovers.com](#)

Go to Hoover's Online for in-depth, first-hand, company coverage provided by business experts. Get an overview, key executive...

Didn't get the results you expected? [Help us improve.](#) [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [Next](#)

# Who's Bidding For Institutional Identity/Key Related Search Terms?

- Even if a bank does a great job of getting its web site to the top of the regular search engine listings, what about people who are willing to pay to show up as a sponsored link? If you check for a bank's name, who (if anyone) shows up as a sponsored listing?
- In most cases the folks who show up will simply be competing institutions, brokers, etc., but what if a phisher advertised for phishing victims that way?
- Are banks even tracking what their identity is going for on a per-click basis? How about related terms? See:  
<http://uv.bidtool.overture.com/d/search/tools/bidtool/>  
<http://inventory.overture.com/d/searchinventory/suggestion/>  
<https://adwords.google.com/select/KeywordSandbox>



**YAHOO! SEARCH**

Web Images Video Directory Local News Products

"wells fargo"

Search

My Web BETA

Shortcuts Advanced Search Preferences

Search Results:

Results 1 - 10 of about 3,260,000 for "wells fargo" - 0.11 sec. (About this page)

Also try: [wells fargo bank](#), [wells fargo online](#), [wells fargo mortgage](#) [More...](#)

SPONSOR RESULTS

- [Compare Wells Fargo's Rates to E-LOAN's](#) Compare our rates and costs to **Wells Fargo**. Get low rates on mortgages for new home purchases or refinancing in all 50 states. Simple application process. No hidden fees. Bad credit okay.  
[www.eloan.com](http://www.eloan.com)
- [Wells Fargo Mortgage - Compare Rates](#) Quickly apply online for a refinance, bill consolidation, home purchase and cash out mortgages. Compare **Wells Fargo** Mortgage rates with our network of over 2,000 banks and lenders.  
[www.the-homeloan-center.com](http://www.the-homeloan-center.com)

Yahoo! Local: [Wells Fargo](#) near you  
[Yahoo! Shortcut](#) - [About](#)

1. [Wells Fargo](#) <sup>Ⓜ</sup> (NYSE: [WFC](#))  
diversified financial services company providing banking, insurance, investments, mortgages, and consumer finance across North America.  
Category: [Financial Services > Banks](#)  
[www.wellsfargo.com](http://www.wellsfargo.com) - 17k - [Cached](#) - [More from this site](#)
2. [Wells Fargo Financial](#) <sup>Ⓜ</sup>  
offers consumer debt consolidation, home equity and automobile loans, private label credit cards, and equipment lease financing.  
[financial.wellsfargo.com/index.html](http://financial.wellsfargo.com/index.html) - 36k - [Cached](#) - [More from this site](#)
3. [Wells Fargo Employment](#) <sup>Ⓜ</sup>  
Learn about employment opportunities at **Wells Fargo**.  
[www.wfjobs.com](http://www.wfjobs.com) - 10k - [Cached](#) - [More from this site](#)
4. [Wells Fargo Home Equity](#) <sup>Ⓜ</sup>  
offers a product fit calculator and online application.  
Category: [Real Estate Financing](#)  
[www.wellsfargo.com/per/accounts/equity](http://www.wellsfargo.com/per/accounts/equity) - 18k - [Cached](#) - [More from this site](#)
5. [Wells Fargo Education Success Loans](#) <sup>Ⓜ</sup>  
information on student loans, assistance with financial aid, including education consolidation loans, college planning, and scholarship searches.

SPONSOR RESULTS

[Wells Fargo Mortgages - Review, Quotes](#)

Overview of **Wells Fargo** and its mortgage options. Review of their Web site plus a...  
[www.wizardofloan.com](http://www.wizardofloan.com)

[Wells Fargo Home Loans Online](#)

LendingLeaders.com will attempt to match you with a **Wells Fargo** broker. If not...  
[www.lendingleaders.com](http://www.lendingleaders.com)

[Wells Fargo Mortgage Loans and Quotes](#)

Compare and shop **Wells Fargo** mortgage loans and get up to four free quotes...  
[www.usaquickloans.com](http://www.usaquickloans.com)

[Wells Fargo Mortgage - Free Quotes](#)

Get important **Wells Fargo** information. Includes a free service to compare mortgage...  
[www.4mortgagehelp.org](http://www.4mortgagehelp.org)

[Wells Fargo Mortgage Comparison](#)

Complete online comparison of national lenders, including **Wells Fargo**. Free online...  
[www.allpurposemortgage.com](http://www.allpurposemortgage.com)

[Wells Fargo Mortgages - Info and Quotes](#)

Find out more about **Wells Fargo** home loans and get up to four free

# "Oopsie" Search Engines and Banks

- Watch out for attacks targeting user misspellings/typing errors made when trying to visit common search engine names. E.G., having made a minor typing error, the user may think they're going to their favorite search engine or web "portal" but in reality they're not... they then have an untrustworthy guide steering their subsequent travels.
  - Now make the mistake of searching for a bank? You may get sent to a phishing site instead of the real thing...
  - Trying to log in to read your web email? Trying to do some online shopping? Maybe there's now a man-in-the-middle, evesdropping on that transaction...
  - Nothing immediately financially exploitable? That's okay, they can always "just" drop malware on your system that will redirect all future traffic or sniff all future passwords.



# Obviously PLEASE DO NOT GO TO The Google-look-alike Site Described on this Page



## F-Secure Virus Descriptions : Google

[\[Summary\]](#) | [\[Detailed Description\]](#) | [\[Detection\]](#)

NAME: **Google**

ALIAS: Google.com

### Summary

F-Secure staff has found a malicious website that utilizes a spelling error when typing the name of the popular search engine - 'Google.com'. If a user opens a malicious website, his/her computer gets hijacked - a lot of different malware gets automatically downloaded and installed: trojan droppers, trojan downloaders, backdoors, a proxy trojan and a spying trojan. Also a few adware-related files are installed.



# What If We're a Visually Impaired User Running Lynx (Instead of IE With Flash)?

- Users with disabilities get phishing messages just like users who don't have disabilities, but their web experience may look radically different...
- Don't forget about parallel "text only" versions of your web site (e.g., note the expired cert)

```
LibertyBank <p1 of 2>
[shim.gif] [shim.gif] [shim.gif] [shim.gif] [shim.gif] [shim.gif]
[shim.gif]
 [in2_r01_c5.gif] [in2_r01_c6.gif] [shim.gif]
[in2_r02_c1.gif] [shim.gif]
[in2_r03_c1.gif] [in2_r03_c3.gif] Now Available! LibertyBillPay
 [in2_r03_c6.gif] [shim.gif]
[in2_r04_c1.gif] [shim.gif]
Online Banking Login
Checking, Savings, and Retirement Accounts
Loans
Business Banking
Office & ATM Locations
About Us
Contact Us
Privacy
[in2_fdic_winter.gif] [shim.gif]
[shim.gif]
[shim.gif]
[shim.gif]
SSL error:certificate has expired-Continue? <y>
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)help O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

# Here's The Mainstream Version...

## The Cert For This Version Looks Fine...

The screenshot shows a web browser window with the address bar displaying `https://www.elibertybankonline.com/engine/login/login.asp`. The browser's toolbar includes a Google search bar, a search button, and various utility icons like PageRank, 4 blocked, AutoFill, and Options. The LibertyBank website header features the bank's logo and a navigation menu with links: HOME, ONLINE BANKING, CHECKING, SAVINGS & RETIREMENT, LOANS, BUSINESS BANKING, OFFICE & ATM LOCATIONS, ABOUT US, CONTACT US, and PRIVACY.

The main content area of the website includes a "Login" section with links for "APPLY NOW", "COMMERCIAL SIGN IN", and "LibertyBillPay FAQ". It also features a "Try our DEMO" button and a section titled "LibertyOnline will allow you to:" with a list of services: Access your accounts and transaction history online, Transfer funds between accounts, Customize and change your account descriptions, and Place stop payments on checks you have written.

Overlaid on the right side of the browser window is a "Certificate" dialog box. The dialog has tabs for "General", "Details", and "Certification Path". The "General" tab is selected, showing "Certificate Information". The text in the dialog states: "This certificate is intended for the following purpose(s): Ensures the identity of a remote computer". It also includes a note: "\* Refer to the certification authority's statement for details." The "Issued to:" field shows "www.elibertybankonline.com" and the "Issued by:" field shows "www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(c)97 VeriSign". The "Valid from" field is highlighted with a pink box and shows "1/17/2005 to 2/12/2006". At the bottom of the dialog are buttons for "Install Certificate...", "Issuer Statement", and "OK".

## **One Final DNS-Related Note: Beware of “New” DNS-Based Attacks**

- While traditional phishing attacks have focused on luring users into clicking on links that appear to be legitimate (but which actually go to bogus sites), you should be aware that a new/emerging approach to doing phishing attacks has emerged which relies on changing the actual mapping of domain names to IP addresses.
- This has come to be called by some "pharming" (although frankly I could personally live without another new term for DNS-based online attacks).

# MessageLabs Monthly Report Nov. 2004

- “MessageLabs has recently intercepted a number of phishing emails, targeting several Brazilian banks. These demonstrate a sinister new technique, designed to plant malware surreptitiously on users’ PCs. When the spam email is opened, it silently runs a script that rewrites the “hosts” file of the target machine. In effect, this replaces the genuine address for the target organisation with the bogus one, without even querying its DNS record.

“So the next time the user attempts to access online banking, they are automatically redirected to a fraudulent web site where their log-in details can be stolen.

“Planting bogus IP addresses in the hosts file, which will override the DNS file, is a technique that has been exploited by virus writers in the past. The objective here is usually to fool the PC user into thinking he has updated his anti-virus signatures, but in fact he has been redirected unknowingly to a spoof address.”

<http://www.messagelabs.com/emailthreats/intelligence/reports/monthlies/November04/>

## Beware of “New” DNS-Based Attacks (cont.)

- A nice discussion of DNS cache poisoning by Joe Stewart of LURHQ is available at <http://www.lurhq.com/cache poisoning.html>
- For other disturbing DNS-related attack examples, see:
  - “Vulnerability Note VU#458659: Microsoft Windows domain name resolver service accepts responses from non-queried DNS servers by default,”  
<http://www.kb.cert.org/vuls/id/458659>
  - “Vulnerability Note VU#109475: Microsoft Windows NT and 2000 Domain Name Servers allow non-authoritative RRs to be cached by default,”  
<http://www.kb.cert.org/vuls/id/109475>
- And then there’s always attacks on domain registrations themselves (ala panix.com’s 1/16/2005 incident, [http://news.com.com/2100-1025\\_3-5538227.html](http://news.com.com/2100-1025_3-5538227.html) )

## Financial Cryptography

Where the crypto rubber meets the Road of Finance...

« Sarbanes-Oxley - what the insiders already know | Main | Financial Cryptography v. The Enterprise »

September 03, 2004

### DNS SPOOFING - SPOKE TOO SOON?

Just the other day, in discussing [VeriSign's conflict of interest](#), I noted that absence of actual theft-inspired attacks on DNS. I spoke too soon - [The Register](#) now reports that the German eBay site was captured via DNS spoofing.

What makes this unusual is that DNS spoofing is not really a useful attack for professional thieves. The reason for this is cost: attacking the DNS roots and causing domains to switch across is technically easy, but it also brings the wrath of many [BOFHs](#) down on the heads of the thieves. This doesn't mean they'll be caught but it sure raises the odds.

In contrast, if a mail header is spoofed, who's gonna care? The user is too busy being a victim, and the bank is too busy dealing with support calls and trying to skip out on liability. The spam mail could have come from anywhere, and in many cases did. It's just not reasonable for the victims to go after the spoofers in this case.

It will be interesting to see who it is. One thing could be read from this attack - phishers are getting more brazen. Whether that means they are increasingly secure in their crime or whether the field is being crowded out by wannabe crooks remains to be seen.

Addendum 20040918: The Register reports that [the Ebay domain hijacker was arrested](#) and admitted to doing the DNS spoof. Reason:

"The 19 year-old says he didn't intend to do any harm and that it was 'just for fun'. He didn't believe the ploy was possible.

So, back to the *status quo* we go, and DNS attacks are not a theft-inspired attack. In celebration of the false alert to a potential change to the threats model, I've added a '?' to the title of this blog.

Posted by iang at September 3, 2004 01:15 PM | [TrackBack](#)

## **4. Bank Web Sites And User's Browsers**



# Internet Explorer vs Other Browsers

- Yes, we know that IE still has a 90% market share.
- However, please note that IE has been specifically flagged as one of the top 10 Windows security vulnerabilities by SANS (See <http://www.sans.org/top20/#w6> ), and US CERT has specifically recommended that users use a browser other than IE ( <http://www.kb.cert.org/vuls/id/713878> ).
- Make sure that Firefox, Safari, Opera and other alternative browsers work with your web site, too.

# Old, Vulnerable Browser Versions

- Do the banks you work with knowingly allow customers to do online banking from ancient versions of browsers, versions well known to have security issues? Do you think those customers are likely to be working from a safe and secure platform if they're routinely surfing an increasingly hostile Internet with an insecure browser?
- Banks are not doing their customers any favors in the long run if they enable them to engage in risky behaviors, so be a force for positive change by encouraging web sites to require use of a current browser if they want to do online banking.

# Design Bank Websites So They Can Be Used Without Needing Risky Browser "Features"

- There are a whole slew of different browser settings that can harden or weaken the security of a bank customer's system.
- Responsible web sites can use virtually any feature in a responsible way, and those features may improve the customer's experience – on the bank's web site.
- However, if a bank requires customers to configure their browsers to permit risky actions, other malicious web sites may take advantage of those now-default risky configurations to harm those customer (users will NOT bother changing settings back and forth depending on whether they're using a bank's web site or some other random/risky web site).

## For Example: Scripting, and Cookies

- Does a bank's website require customers to use Javascript or other scripting technology to use its site? If so, please understand that doing so substantially increases the bank customers' overall exposure to a host of web-related vulnerabilities (see [http://www.cert.org/tech\\_tips/malicious\\_code\\_FAQ.html](http://www.cert.org/tech_tips/malicious_code_FAQ.html) ) Javascript/other scripting -- if used at all -- should only be used in a way that breaks cleanly if scripting is disabled.
- Cookies are used by some sites to track customers, often for advertising-related purposes. Does the bank require customers to accept cookies? Why? Are they really needed if they have an SSL-secured connection established? If they do use cookies, do they clean them up at the end of the session? Again, help users to protect themselves by not mandating use of cookies.

Key - Technical - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.key.com/templates/t-ob2.jhtml?nodeID=E-1

Access My Accounts | Apply for Loans and Accounts | Site Map | Search | Contact Us

## Frequently Asked Questions

### Online Banking and Investing

#### Browser Requirements

- ◆ We require Internet Explorer 5.0 or higher or Netscape 5.0 or higher
- ◆ Determine your browser version by clicking Help and About (browser name)
- ◆ 128-bit encryption
- ◆ Browser set to accept cookies
- ◆ Recommended cache settings
- ◆ Javascript should be enabled

#### Cache Settings Requirements

PERSONAL

SMALL BUSINESS

CORPORATE

ABOUT KEY

ONLINE BANKING

Online Banking and Investing

FAQs


► Technical

128-bit encryption

Service Comparison

Helpful Resources

Personal Financial Managers



# Your Website And Popups...

- Does your site require users to permit popup windows?
- Remember that Windows XP SP2 now routinely blocks popup Windows. Should banks be using that sort of feature on their web sites?
- See also: “Pop-up Loophole Opens Browsers to Phishing Attacks,” December 8th 2004,  
<http://www.eweek.com/article2/0,1759,1737588,00.asp>

# From the sccu.com Credit Union Site:

5. Under the **Privacy & Security** category click **Popup Windows**. On the right side of the window, uncheck "Block unrequested pop up windows".



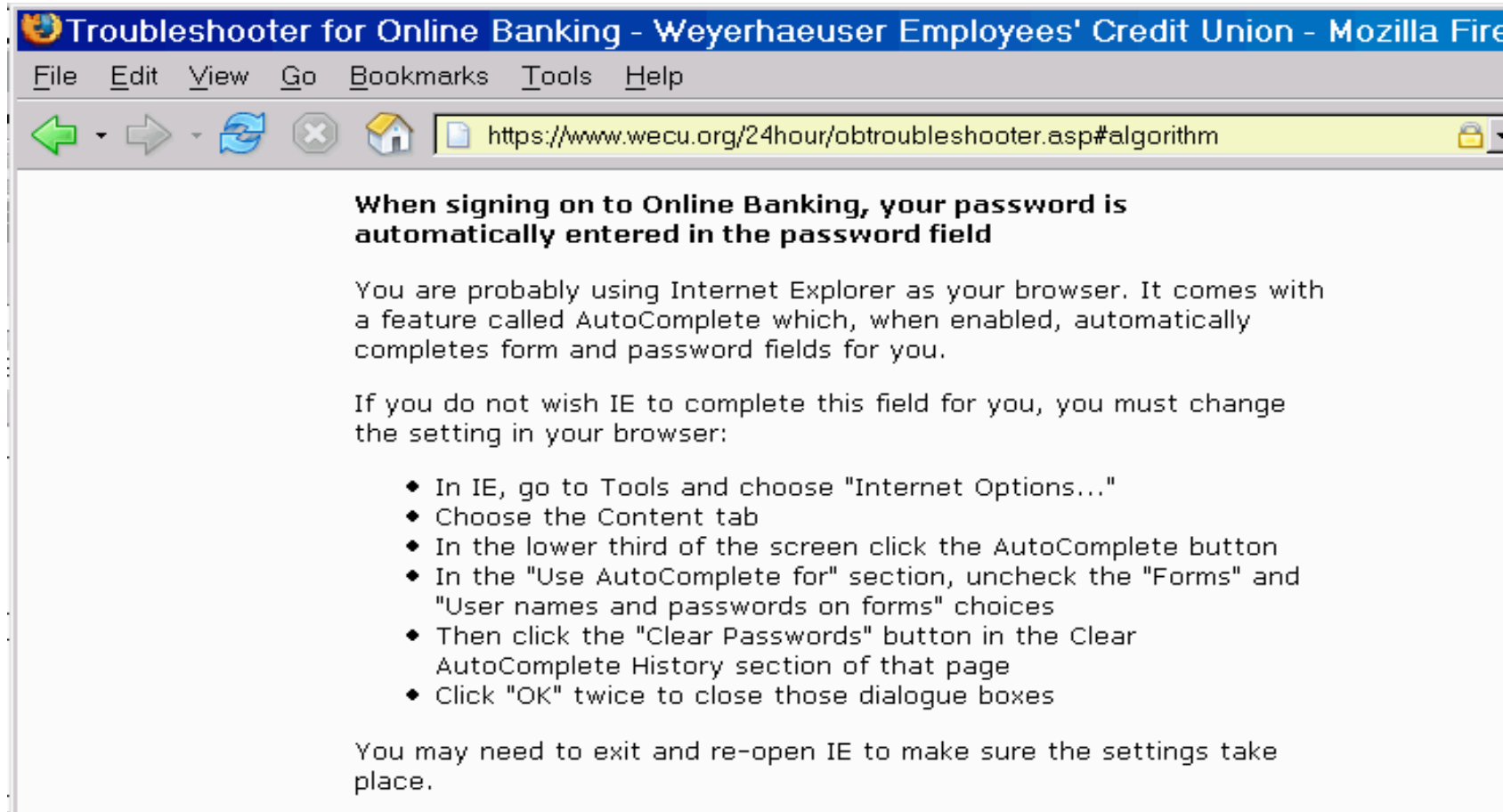
(Note: If you prefer to block popups except for the SCCU Online Banking site, keep the box checked but include SCCU's Online Banking web site in the list of your "Allowed Sites".

# Is *Too Much* Getting Saved?

- Caching, in the web sense of the word, is the notion that you can speed things up by retrieving and saving a copy of an unchanging image or web page, delivering it the next time it is needed from that local copy (rather than re-retrieving them from a remote site time after time). Are your web pages cacheable? Normally it is wonderful if they are, but if you're running a bank web site, they probably shouldn't be...
- As a convenience feature, do you allow users to save their username and password as a persistent cookie on their system? Don't!
- Is browser form auto-completion *\*automatically\** saving sensitive user account information and passwords?

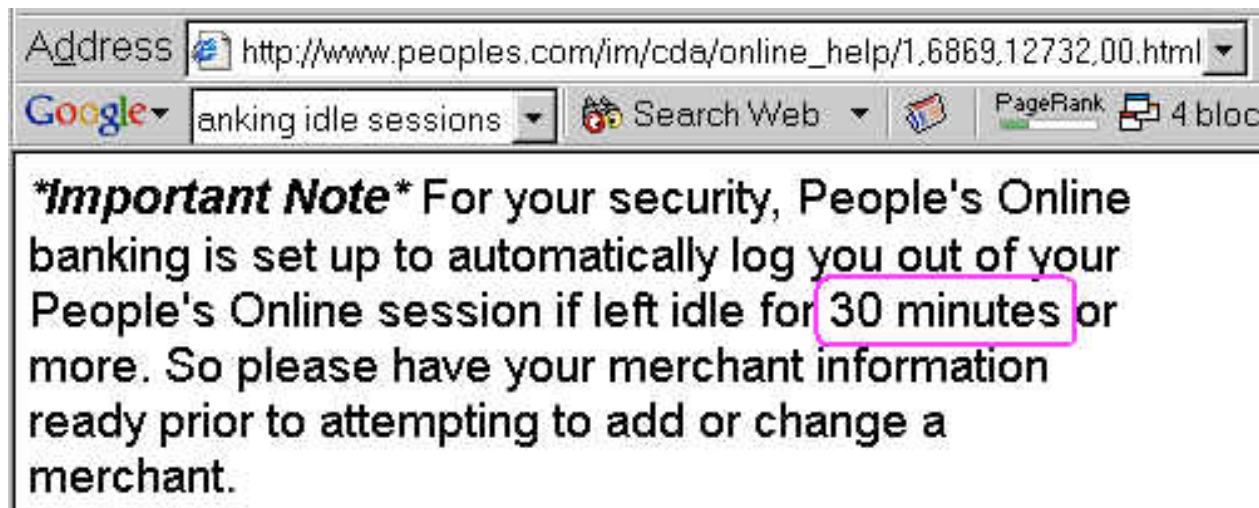


# Autocompletion Symptomology



# What About Idle/Abandoned Sessions?

- Do idle or abandoned secure sessions time out?  
How soon? How was that value selected? 30 minutes, for example, can be a long, long time in a cybercafe or other shared system environment...




# How About Browser Anti-phishing Toolbars?







- While some people really like browser anti-phishing toolbars, others have presented examples of phishing attacks where they haven't worked so hot, e.g., see: "Phishing Toolbars – The One That Works," [http://loosewire.typepad.com/blog/2005/04/phishing\\_toolba.html](http://loosewire.typepad.com/blog/2005/04/phishing_toolba.html) and the followup day's piece, "The Antiphishing Toolbars That Didn't," [http://loosewire.typepad.com/blog/2005/04/the\\_antiphishin.html](http://loosewire.typepad.com/blog/2005/04/the_antiphishin.html)
- Some browser anti-phishing toolbars work with IE only
- Some anti-phishing toolbars may include advertising or collect statistics or do other things besides just working to combat phishing (maybe that's a problem for you, maybe not).

# Blocking Access to Online Banking (Some Places)

- If banks allow access to customer online banking web sites from anywhere in the world, they may want to reconsider that given the fact that the vast majority of their customers probably do not travel internationally. An analogy from the long distance phone card world: some phone company calling cards are "domestic use only"
- Some countries are known to have particularly high levels of fraud-related activity; banks should consider the possibility that there may not be a business case for allowing access to online banking from those countries whatsoever. (Be aware that in some cases it may be hard to determine the true geolocation of a given Internet user due to abuse of open proxy servers)

 Americart FAQ - Credit Card Fraud - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

      <http://www.cartserver.com/americart/faq-fr.html>

---

### Geographical Tips:

The vast majority of orders from the following countries are FRAUDULENT:

- Romania
- Indonesia
- Singapore (see note below)
- Ghana (a rising star of fraud!)
- Ukraine
- Uganda
- Nigeria
- Hungary
- Belarus
- Estonia
- Latvia
- Lithuania
- Slovak Republic
- Russia
- Yugoslavia
- Macedonia
- Phillipines
- Thailand
- Malaysia (see note below)

Note on Singapore & Maylasia: People in Indonesia use Singapore or Maylasia as the destination Country name, and still get the package because Singapore/Maylasia Postal Service figures out where to send it.

Our advice is to just not ship to any of these countries. In the long haul, you will lose money.

## **Banks Need To Be Monitoring Their Web Server for Phishing That Use The Bank's Images, Logos, Etc.**

- Scam artists love to use graphics directly from the bank's institutional web site; the URLs in their email help lull users into a false sense of security, and using hyperlinks instead of attached graphics helps reduce the size of each mail they send.
- Banks, obviously, should try to prevent this.
- This problem is, in many ways, quite analogous to what "adult hosting" companies face when competitors try to include/reuse "graphical content" without permission.
- Not surprisingly, solutions have been developed.

# Anti-Leach

- Solutions have been developed to eliminate or reduce reuse of web images or other content without permission. Try googling for

anti-leach .htaccess

or see <http://httpd.apache.org/docs/misc/rewriteguide.html> under “Blocked Inline-Images”

- Even simple expedients can help: change the location of web images over time; if phishers are hitting images the bank itself is no longer using, consider "helping" them by making creative adjustments to the images which are being used without your permission.
- At a minimum, banks should watch their server's logs!

## **Let Users Help You Monitor Access That Originates From “Unusual” Locations**

- Banks should enlist customers to help them keep watch on their accounts. Most banks do NOT routinely tell customers the last place(s) where “they” accessed their online banking account, but they should! Build it right into their normal account display once they've logged in. [“What do you mean I last accessed my account six days ago from a high school in Sao Paulo Brazil???”]
- This is the web analog of "last login" reporting feature that's common on some traditional mainframe systems for shell users.



## **5. Training And Communicating With Users**

# **Banks Should Help Customers Use The Financial Statements They Provide**

- Many customers likely never look at the financial statements banks provide, and that may be in part because the (necessary) amount of detail may sometimes overwhelm the key "big picture" issues.
- While most phishing will get easily caught before routine statements get issued (e.g., the user's account gets completely zero'd), more subtle low-dollar attacks may not.
- One thought: banks should prioritize and highlight the salient bits of what they tell their users. Odd transactions, relative to their norm? High dollar transactions? Other oddities? Highlight them so they stand out and can receive extra scrutiny by bank customers.

# **Banks Really Need To Be Communicating With Their Customers; For Some Reason Customers May Not Trust Stuff Emailed to Them :-)**

- Do bank customers know what to do (and what NOT to do) if they receive phishing email? As a matter of due diligence/CYA, banks should officially notify their customers about phishing problems and what they should do if they receive phishing email.
- Bank web sites should have information about phishing.
- Are policies in place if a customer reports a phishing event to a customer service person or other bank staff member in person? By phone?
- Remember: proactive customer education is KEY to killing phishing as a viable attack strategy.

## **Banks Should Make Sure Customers Can Communicate With Them**

- Users want to tell banks about phishing that's going on -- be sure you're open to those reports!
- Does mail sent to:
  - abuse@<the bank's domain>
  - postmaster@<the bank's domain>
  - the bank's domain whois points of contact
  - the bank's netblock whois points of contact
  - your autonomous system whois points of contactactually go through as RFC2142 (and common sense) say it should?
- Be particularly careful that you're accepting spamcop.net reports; they're generally remarkably timely and of good quality.

# Sample Output from RFC-Ignorant.Org

Lookup results - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.rfc-ignorant.org/tools/lookup.php?domain=chase.com

**RFC-Ignorant.Org**

How to Use:

- [Domain Based Zones](#)

[Mailing List](#)

Submit to:

- [DSN \( <> \)](#)
- [postmaster](#)
- [abuse](#)
- [whois](#)
- [bogusmx](#)

**Current Results for chase.com lookup**

| blacklist_zone | domain                    | status | Submitted              | Added                 | Rejected | Removed |
|----------------|---------------------------|--------|------------------------|-----------------------|----------|---------|
| whois          | <a href="#">chase.com</a> | Listed | Jun 11, 2004 19:35 EDT | Jun 12, 2004 4:13 EDT | Never    | Never   |
| postmaster     | <a href="#">chase.com</a> | Listed | May 6, 2003 16:40 EDT  | May 7, 2003 5:05 EDT  | Never    | Never   |

(Click [here](#) to include Rejected/Removed listings.)

# Make Sure Bank Customers Know How To Share Phishing Samples With Full Headers

- Potential scenario: 20,000 (or 200,000!) customers calling the bank to tell you that they've -- <gasp!> -- received a message that is claiming to be from the bank, but which looks mighty suspicious to them, yes siree, Bob... Knew you'd want to know about that! [fifteen minutes per call, no tangible/usable information, hard to avoid customer ending up feeling disappointed when an immediate nuclear strike on the unidentifiably spamming phisher isn't immediately launched]
- Alternative scenario: a few hundred customers report phishing to you via email with FULL HEADERS within a day of the time the phishing was sent to them. With full headers and full message body, you actually have a chance to go after the bad guys in a timely fashion.

## Per-Email Client Full Header Reporting Info

- We have information about how to get full headers from most popular email programs at <http://micro.uoregon.edu/fullheaders/> however note that there are some email programs (like MS Outlook/Outlook Express) that make getting full headers a real PITA.
- You guys have a lot more clout than I do – encourage Microsoft to make getting full headers easy and painless, both on a message-by-message basis, and as a default setting.

## **6. The Importance of Card Encoding Algorithms**



# Translating Phished Data Into Cash

- Just recently, an incredibly important paper was publicly released:

“The economy of phishing: A survey of the operations of the phishing market,” by Christopher Abad  
[www.firstmonday.org/issues/issue10\\_9/abad/](http://www.firstmonday.org/issues/issue10_9/abad/)

If you read only one paper about phishing, make it that one...

## Brief Quote from Abad's Paper:

- “The main difficulty with tracking is the encoding of bank data to the ATM card. The preferred hardware used to encode information onto magnetic stripe cards is the MSR-206. Although the MSR-206 hardware most preferred by cashiers can be easily obtained, each bank uses a specific encoding algorithm to translate the credentials into the encoded data written to an ATM card. The tracking algorithm may be as simple as appending the expiration date and cvv2 code along with a fixed numeric value to the end of a check card number, or as complex as encrypting the information with a secret key and then encoding the encrypted block to the card.

“It is no surprise that Washington Mutual, Key Bank, and various other institutions are at the top of phishers’ lists. The tracking algorithms for these financial institutions are easily obtained from within the phishing economy, while Bank of America, a huge financial institution, is nearly off phishers’ radar because their encoding algorithm is very hard to obtain or crack.”

## **7. What's Next?**

# **1. Banks Really Need To Be Thinking About Something Other Than Account Numbers Plus Passwords to Secure Online Access**

- “Financial institutions and government should consider a number of steps to reduce online fraud, including:  
1. Upgrading existing password-based single-factor customer authentication systems to two-factor authentication...”

“Putting an End to Account-Hijacking Identity Theft”

<http://www.fdic.gov/consumers/consumer/idtheftstudy/>

- Two factor authentication ==>  
something you have, plus something you know.  
Classic financial industry example: ATM card and PIN.  
In the computer world, typical example is a hardware token (e.g., keychain fob that generates a periodically changing unguessable number) and a password.

# AOL is Doing Two Factor These Days

RSA Security - Press Release - America Online and RSA Security Launch AOL PassCode Premium Service

File Edit View Go Bookmarks Tools Help

http://www.rsasecurity.com/press\_release.asp?doc\_id=5033&id=1034

**SERVICES**

**PARTNERS**

**LEADERSHIP**

**NEWS & EVENTS**

- Press Releases
- RSA Security In the News
- Web Seminars
- Events
- Customer Success Stories
- Awards
- Corporate Press Kit

## America Online and RSA Security Launch AOL PassCode Premium Service

AOL Is First Online Service to Offer Optional State-of-the-Art Two-Factor Authentication to Consumers

Keychain-Sized Device Provides Second Level of Account Protection Through Automatically-Generated Supplemental Password


**Dulles, VA and Bedford, MA, Tuesday, September 21, 2004 —**

America Online, Inc., the world's leading interactive services company, and RSA Security Inc. (NASDAQ: RSAS), a leading provider of solutions that secure and manage online identities, today announced the launch of AOL PassCode, a new premium service that offers members a second level of AOL account protection through the use of a keychain-sized device that generates and displays a unique six-digit numeric code every 60 seconds.

**Related Solution**

By delivering the strongest online consumer security possible, companies can increase customer loyalty.

[Consumer Identity Protection](#)



AOL PassCode is a new premium service for AOL members.

"AOL PassCode is like adding a deadbolt to your AOL account by automatically creating a new secondary password every 60 seconds," said Ned Brody, AOL's Senior Vice President for Premium Services. "Many of our members use their accounts for business purposes, financial transactions or other sensitive activities. AOL Passcode offers a higher standard of protection through the same state-of-the-art two-factor authentication system used by many financial institutions, technology companies, and other major businesses. We're proud to be the first online service to offer this extraordinary supplementary level of security protection to our users."

# So Is E\*TRADE...

**E\*TRADE FINANCIAL - Home - Mozilla Firefox**

File Edit View Go Bookmarks Tools Help

https://us.etrade.com/e/t/microsite/custsecurity?SC=NPNL67G&traxui=F\_HV

**3. Complete Security Protection, unauthorized access to your account is virtually impossible.**

**1. Model New Cash Allocations** **2. View Results & Suggested Action** **3. Complete Security Protection**

**COMPLETE SECURITY PROTECTION**

- We utilize 128-bit encryption, the highest level of web site security available
- Individual RSA SecurID - An optional keychain-sized token which displays a unique 6-digit number that changes every 60 seconds<sup>2</sup>
- SmartAlerts - configure to inform you of your account activity
- Security specialists monitor your account for unusual activity

**Exclusive, Free,<sup>1</sup> Easy & Optional for E\*TRADE Customers**

**Trading**  
5 star quality  
100% satisfaction

**Investing**  
Open your 2004 tax-qualified IRA  
No fees, no minimum

**Banking**  
Get higher yields on CDs  
Free E\*TRADE Bank

**User ID:**  **Password:**

**Start In:**

**Secured by RSA**

**Markets**

<sup>1</sup> The Digital Security ID will be provided at no cost to Power E\*TRADE and Priority E\*TRADE customers. A \$25 charge may be imposed for each additional or replacement Digital Security ID. E\*TRADE FINANCIAL at its sole discretion may impose a fee for this service in the future or may discontinue the service.

<sup>2</sup> RSA, RSA logo and SecurID are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. RSA Security Inc. is not affiliated with E\*TRADE FINANCIAL Corp. or any of its affiliates and is not a sponsor

# The Process Need Not Be High Tech

- Consider, for example, the European PIN/TAN system, whereby online transactions need not only a secret password or PIN, but also a one-time-use-only transaction authorization number (e.g., the user's bank provides the customer with a printed list of TANs, and each time the user wants to do an online banking session, the user needs to supply their next TAN from the list...)
- As long as the miscreant doesn't get the user's account number, and their PIN, and their list of TANs, they should be safe...
- Well, maybe. See: "Outflanking and Securely Using the PIN/TAN-System," A. Wiesmaier, et. al., 6 Jan 2005, [http://arxiv.org/PS\\_cache/cs/pdf/0410/0410025.pdf](http://arxiv.org/PS_cache/cs/pdf/0410/0410025.pdf)

# Another Comparatively Simple Approach

Two Factor Authentication - Entrust IdentityGuard for Strong User Authentication

File Edit View Go Bookmarks Tools Help

http://www.entrust.com/identityguard/index.htm

With Entrust IdentityGuard, users continue to employ their current user name and password, but are also provided with a second physical form of authentication based on an assortment of characters in a row/column format printed on a card. A user must successfully complete a coordinate challenge to demonstrate that they are in possession of the appropriate card:

Welcome to Any Bank

User Name: John Smith

Password: xxxxxxxx

IdentityGuard: A2 C4 F3

Submit

ANY BANK

Entrust

|   | A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 7 | 1 | 9 | 3 | 5 | 5 | 4 | 9 |   |   |
| 2 | 9 | 2 | 5 | 3 | 6 | 8 | 4 | 1 | 3 |   |
| 3 | 4 | 6 | 1 | 4 | 6 | 2 | 8 | 0 | 7 |   |
| 4 | 5 | 2 | 4 | 8 | 5 | 0 | 1 | 7 | 2 |   |
| 5 | 6 | 8 | 6 | 8 | 1 | 7 | 4 | 0 | 8 | 0 |

Serial #1234567



# Please, Don't Make My Pants Fall Down

- If I have:
  - a two factor auth token for my workstation at work
  - another two factor auth token for my online bank
  - another two factor auth token for my broker
  - another two factor auth token for ...
  - etc., etc.

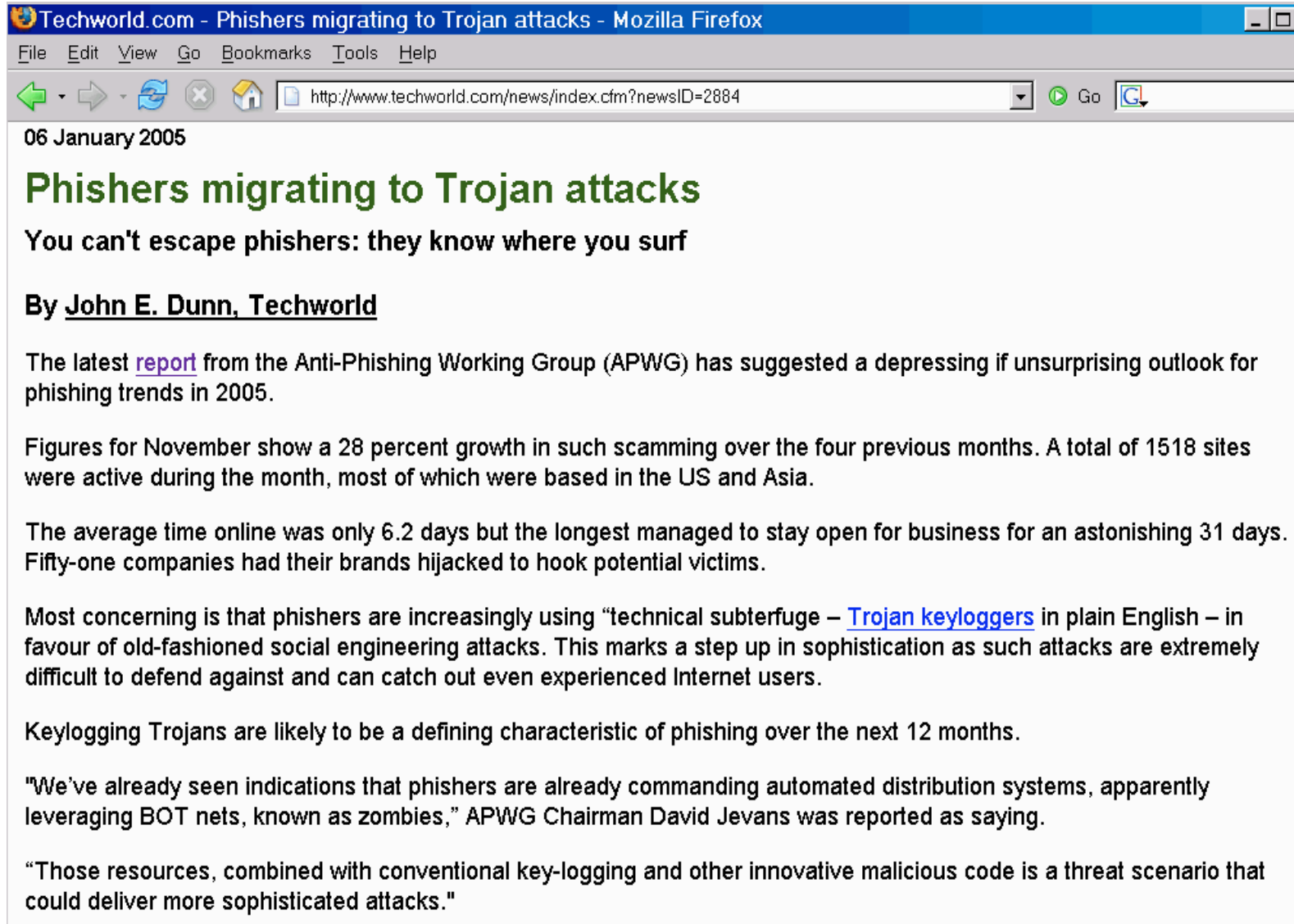
pretty soon things are going to start getting silly: think "janitor sized key rings," only this time full of two factor authentication tokens rather than traditional room keys.

- Perhaps coordination and interoperability or a shared nationally issued two factor solution would be worthwhile?

## Some Are Skeptical of Two Factor Auth

- See Bruce Schneier's "The Failure of Two Factor Authentication," Cryptogram, March 15th, 2005, <http://www.schneier.com/crypto-gram-0503.html#2> and see his followup at:
- "More On Two Factor Authentication," Cryptogram, April 15th, 2005, <http://www.schneier.com/crypto-gram-0504.html#1>
- The Anti-Phishing Working Group is already reporting that folks are deploying trojan keylogging software, precisely one of the sort of attacks that Schneier was worried about...

## 2. Trojan Keyloggers



The screenshot shows a Mozilla Firefox browser window with the title bar "Techworld.com - Phishers migrating to Trojan attacks - Mozilla Firefox". The address bar displays the URL "http://www.techworld.com/news/index.cfm?newsID=2884". The page content includes a date "06 January 2005", a main headline "Phishers migrating to Trojan attacks" in green, a sub-headline "You can't escape phishers: they know where you surf", and an author line "By John E. Dunn, Techworld". The article text discusses a report from the Anti-Phishing Working Group (APWG) about phishing trends in 2005, mentioning a 28 percent growth in scamming, 1518 active sites, and the use of Trojan keyloggers.

Techworld.com - Phishers migrating to Trojan attacks - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.techworld.com/news/index.cfm?newsID=2884

06 January 2005

### Phishers migrating to Trojan attacks

**You can't escape phishers: they know where you surf**

**By John E. Dunn, Techworld**

The latest [report](#) from the Anti-Phishing Working Group (APWG) has suggested a depressing if unsurprising outlook for phishing trends in 2005.

Figures for November show a 28 percent growth in such scamming over the four previous months. A total of 1518 sites were active during the month, most of which were based in the US and Asia.

The average time online was only 6.2 days but the longest managed to stay open for business for an astonishing 31 days. Fifty-one companies had their brands hijacked to hook potential victims.

Most concerning is that phishers are increasingly using "technical subterfuge – [Trojan keyloggers](#) in plain English – in favour of old-fashioned social engineering attacks. This marks a step up in sophistication as such attacks are extremely difficult to defend against and can catch out even experienced Internet users.

Keylogging Trojans are likely to be a defining characteristic of phishing over the next 12 months.

"We've already seen indications that phishers are already commanding automated distribution systems, apparently leveraging BOT nets, known as zombies," APWG Chairman David Jevans was reported as saying.

"Those resources, combined with conventional key-logging and other innovative malicious code is a threat scenario that could deliver more sophisticated attacks."

### 3. Phone-Based Phishing

- While most phishing is taking place via email right now, there's no reason why phone-based phishing could not occur (and frankly, it already is occurring)
- Contributing/enabling factors:
  - Voice Over IP (VoIP)
  - Caller ID spoofing
  - with email untrustworthy, folks want to be able to fall back to something they "know" they can "trust"
- What would that be? Why the phone, of course...

## Voice Over IP Is...

- VoIP is hugely popular with legitimate users (Skype, for example, has had a hundred million downloads, see <http://www.skype.com> )
- VoIP can be gatewayed to the plain old telephone system (in to Skype or out from Skype)
- VoIP can support voicemail
- VoIP is available on a virtually ubiquitous basis (to the dismay of legacy PTT operators)
- VoIP is free (or very cheap)
- VoIP has amazingly high audio quality
- VoIP is mobile -- got Internet? you've also got VoIP
- VoIP is potentially difficult to trace when it gets abused

# Scammers Snag Money on Net Phones

Reuters

Page 1 of 1

12:36 PM Mar. 20, 2005 PT

WASHINGTON -- Internet phone services have drawn millions of users looking for rock-bottom rates. Now they're attracting identity thieves who want to turn stolen credit cards into cash.

Some internet phone services allow scam artists to make it appear that they are calling from another phone number -- a useful trick that enables them to drain credit accounts and pose as banks or other trusted authorities, online fraud experts say.

Wireless Hot Spot  
Directory

**Find hot spots**

"It's like you've handed people an entire phone network," said Lance James, chief

## 4. Last Idea: Small Dollar Amount Fraud

- Small dollar amount fraud is the future... Why?
  - small dollar charges get less scrutiny at purchase time than big ticket purchases (you typically have less margin to plow into investigating the potential purchaser)
  - small dollar charges are less likely to be noticed/reported by the user when they check their bills
  - the fraudster knows that the cost of investigating a small-dollar unexpected charge (in staff time, inconvenience, etc.), may result in small disputed charges being written off by the victim/merchant/bank
  - he/she knows that even if small dollar amount frauds do get investigated, small dollar amount frauds are much less likely to be prosecuted than large dollar amount frauds

## Small Dollar Amount Fraud (cont.)

- -- he/she knows that even if a small dollar fraud is prosecuted, punishment for such a “petty” crime is likely to be negligible  
-- HOWEVER enough small distributed fraudulent charges may aggregate to a material amount from the point of view of the perpetrator
- 32% of all incidents reported to the FBI Internet Crime Complaint Center in 2004 were for less than a hundred dollars (I believe many many more simply went completely unreported).
- Americans as a culture are great when it comes to dealing with clearly presented scary threats, like a head on charging bear; as a society we're less good at dealing with being nibbled to death by a million fleas.



# **Thanks For The Chance to Talk Today!**

- Are there any questions?