Attacking The Phishing Problem With Technology: Options for Banks and Other Financial Institutions

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

American Bankers Association Conference Call
11AM Pacific, Tuesday, March 31st, 2009

http://www.uoregon.edu/~joe/aba/

Disclaimer: all opinions expressed in this presentation are those of the author and do not necessarily represent the opinion of any other entity.

This Briefing

- This talk is the result of an invitation from Peter Cassidy of the Anti-Phishing Working Group (APWG) and Jane Yao of the American Bankers Association. I’d like to thank them for the opportunity to share some thoughts with you today.
- While there are many different approaches one can take to counter phishing, this talk is intended to help you think about some technical options available to you. Even if <u>you</u> aren’t particularly technical, you should still be able to get the gist of what we’re covering (I’ve tried to tone down the technical level wherever I can), and it will at least give you something to talk about with your tech folks.
- 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 looking at this talk after the fact.

My Background and A Disclaimer

- I’m Security Programs Manager for Internet2 under contract through the University of Oregon, and I’m also involved with a variety of system and network security-related projects at the national/international level.
  For example, I’m one of half a dozen senior technical advisors for MAAWG (the carrier Messaging Anti-Abuse Working Group), the carrier anti-spam organization representing nearly a billion (yes, with a B) mailboxes worldwide. I’ve also been serving as an invited subject matter expert for the ICANN GNSO Fast Flux Working Group.
- ***However, let me emphasize that everything I say today is solely my own opinion.***
- That said, let’s start out by making sure we’re all working toward the same goals

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.)

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,” and insure that bank emails don’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

Where Might Technical Approaches to Dealing With Phishing Come From?

- Technical approaches to phishing need to come from all of us, but especially from those of you who are actually running banks, as well as folks like the APWG.

- I sincerely doubt that there’s anything new I can tell you today, but I would like to take a moment or two of your time to review some material you may already know, just on the off chance that you may now be able to implement some of these approaches when previously you might not have been able to do so.

- For those of you who are doing all the right things already, congratulations and keep up the good work!

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 well 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, Thunderbird, whatever) and change your name and email address to something else – 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 some 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 “128.223.142.89”).
- With SPF, a domain owner publishes a new record in the domain name 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 banks have a 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!”

Starting to Learn About SPF

- SPF and related protocols are formally documented in a series of Internet Engineering Task Force (IETF) drafts (RFC4405-RFC4408). To look at one of these, for example RFC4408, you'd go to:

  http://www.ietf.org/rfc/rfc4408.txt

  A more approachable starting point, however, is probably the SPF project white paper:

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

- Another nice way to learn about SPF is to check out an SPF record that's actually been published by a domain…

An Example SPF Record: Citibank

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

```
% host -t txt citibank.com
citibank.com descriptive text "v=spf1
a:mail.citigroup.com ip4:217.29.160.12 ~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 for their domain? yes, yes they have…
  -- that SPF txt record allows citibank.com mail from the mail server server mail.citigroup.com or from 217.29.160.12 (that happens to be an IP address at EFLUXA in Italy
  -- mail from all other locations should probably be rejected (~all = “soft failure”)

We Just Looked At An SPF Record Manually; Mail Systems Can Check SPF 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 just received mail purportedly from our bank checks the SPF records the bank has published, spoofed mail that claims to be “from” that domain can then be rejected outright, or filed in a junk folder with spam, etc.
- Many banks are already publishing SPF records, and many ISPs are already checking them.
- Examples of some banks and other entities that have published SPF records include…

```
% host –t txt usbank.com
usbank.com descriptive text "v=spf1 mx a:mail5.usbank.com
a:mail10.usbank.com a:mail14.usbank.com a:mail9.usbank.com
a:mail13.usbank.com -all"
% host -t txt bankofamerica.com
bankofamerica.com descriptive text "v=spf1
include:_sfspf.bankofamerica.com
include:_txspf.bankofamerica.com
include:_vaspf.bankofamerica.com ~all”
% host -t txt jpmorganchase.com
jpmorganchase.com descriptive text "v=spf ip4:170.148.48.0/24
ip4:159.53.36.0/24 ip4:159.53.46.0/24 ip4:159.53.110.0/24 -all"
% host -t txt visa.com
visa.com descriptive text "v=spf1 ip4:198.80.42.3
ip4:198.241.156.21 ip4:69.20.125.232 ip4:198.241.175.106
ip4:216.251.253.98 include:em.visa.com ~all”
% host -t txt americanexpress.com
americanexpress.com descriptive text "v=spf1 include:aexp.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]
```

Most Leading Financial Institutions Now Have Published SPF Records…

- I used to list leading banks that didn’t publish SPF records, but these days virtually EVERY leading bank *IS* publishing an SPF records for their domain.
- Actually, there *are* still a *few* banks who aren’t publishing SPF records, but they’re pretty rare these days. If you’re with one of those rare banks that hasn’t published an SPF record, you might ask yourself:

  > *“Who will the bad guys probably target for their next phishing attack? The domains that have published SPF records or those which haven’t?”*

- In fact, given industry uptake of SPF, publishing an SPF record might even be taken by some as a fundamental act of basic due dillegence, sort of like remembering to lock the vault when the brick-and-mortar bank is closed.

“OK, I Do Want to Publish An SPF Record…”

- Start by having technical staff review the SPF Whitepaper at 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 sending mail on the bank’s behalf)
- 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 should run the SPF Wizard to help them craft an initial SPF record: http://old.openspf.org/wizard.html
- Check it with http://www.kitterman.com/spf/validate.html or http://www.vamsoft.com/spfvalidator.asp
- Publish the SPF records
- Check/tweak them based on any issues you run into

When Your Bank Publishes SPF Records, Make Sure You Publish Them for ALL Your Domains

- Many banks are associated with more than one domain.

- At least at one time, it was common for a bank to ONLY publish an SPF record for their primary domain, forgetting to also publish SPF records for all their other domains, too.

- Phishers only need the ability to send mail as ONE of your domains to potentially “win” this game.

- Thus, please check to make sure you’ve published SPF records for ALL the domains associated with your bank.

Bad Guys Can Still Create "Look Alike" Domains and Even Define Their Own SPF Records for Them

- Assume you're joesexamplebank.com (a hypothetical/non-existent bank and domain).
- Also assume you've published SPF records "locking down" who can originate mail for joesexamplebank.com
- Will SPF completely protect joesexamplebank.com? No.
- For example, SPF cannot protect joesexamplebank.com from mail that's sent by someone who has registered joesexamp1ebank.com (note that the "el" you expect to see in that domain name has been replaced by the number one)
- The person who registers joesexamp1ebank.com may even publish an SPF record for it, protecting himself (as a bad guy!) against spoofed email.

Making Tea vs. Boiling the Ocean

- Publishing SPF records and checking SPF records on your local servers are fully independent activities.
  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 promoted an alternative protocol, SenderID, that tried hard to look at the sort of From: headers that users would normally see. See www.microsoft.com/mscorp/safety/technologies/ senderid/default.mspx (URL split due to length)
- SenderID received a rather luke-warm-to-hostile reception in some circles 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: SPF v1 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.

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 would 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 if/when that signature is tested.

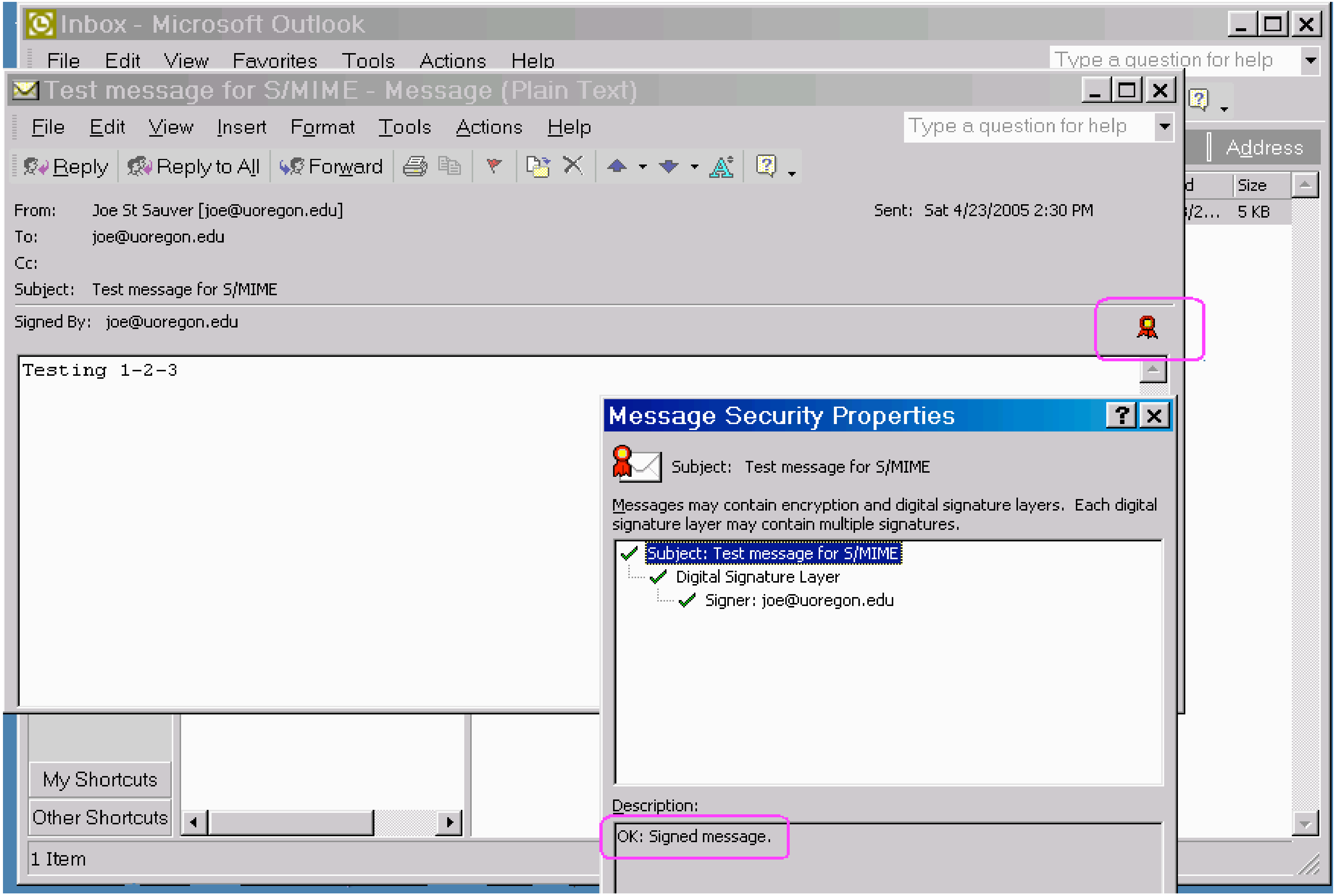
Digital Signing Is NOT Message Encryption

- 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



Inbox - Microsoft Outlook
File Edit View Favorites Tools Actions Help
Type a question for help
Test message for S/MIME - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Type a question for help
Reply
Reply to All
Forward
Address
Size
5 KB
My Shortcuts
Other Shortcuts
1 Item

From: Joe St Sauver [joe@uoregon.edu]

Sent: Sat 4/23/2005 2:30 PM

To: joe@uoregon.edu

Cc:

Subject: Test message for S/MIME

Signed By: joe@uoregon.edu

```
Testing 1-2-3
```

Message Security Properties

Subject: Test message for S/MIME

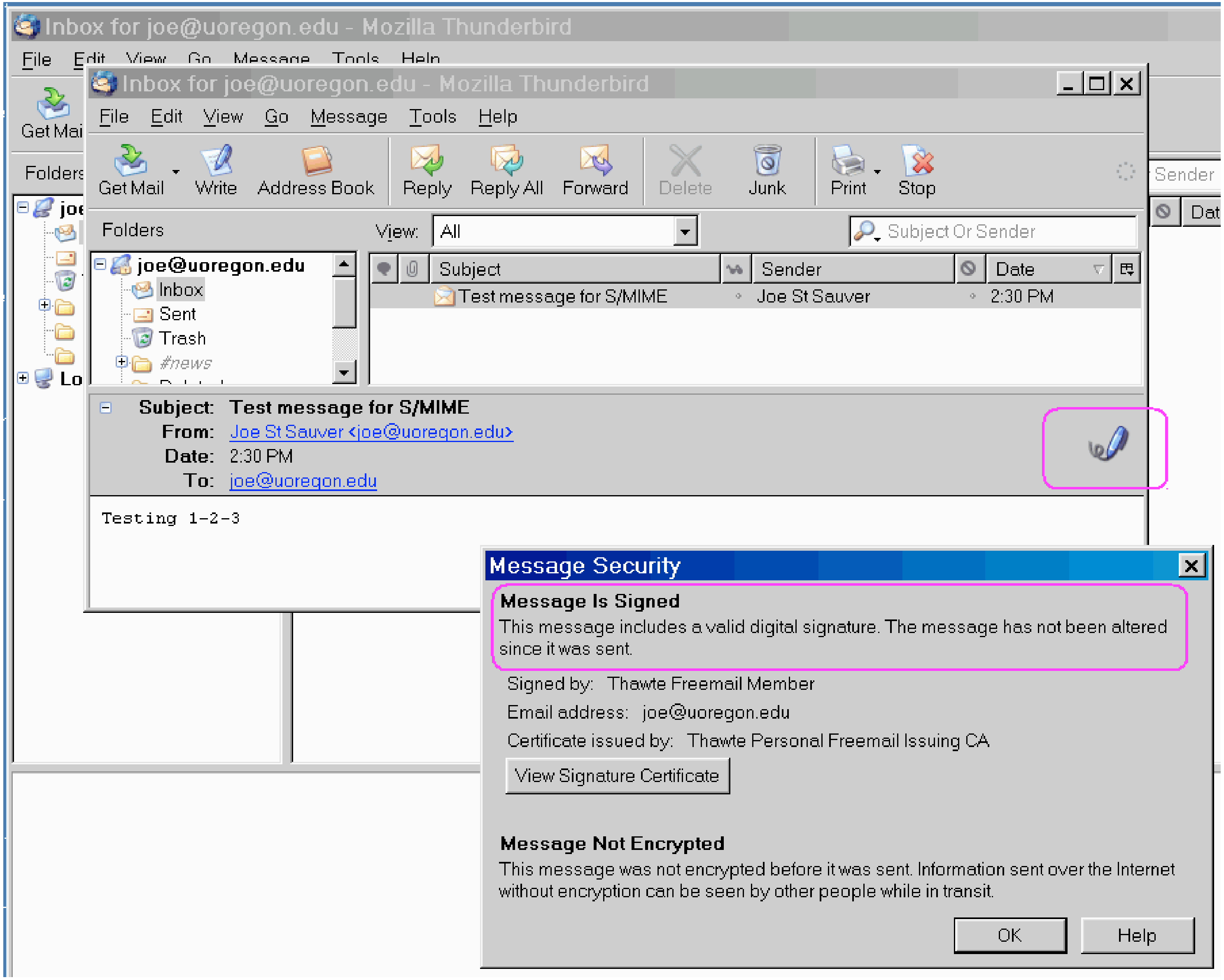
Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

- ✓ Subject: Test message for S/MIME
  - ✓ Digital Signature Layer
    - ✓ Signer: joe@uoregon.edu

Description:

OK: Signed message.

An S/MIME Digitally Signed Message In Thunderbird



Test message for S/MIME | Joe St Sauver | 2:30 PM

Subject: Test message for S/MIME
From: Joe St Sauver <joe@uoregon.edu>
Date: 2:30 PM
To: joe@uoregon.edu

```
Testing 1-2-3
```

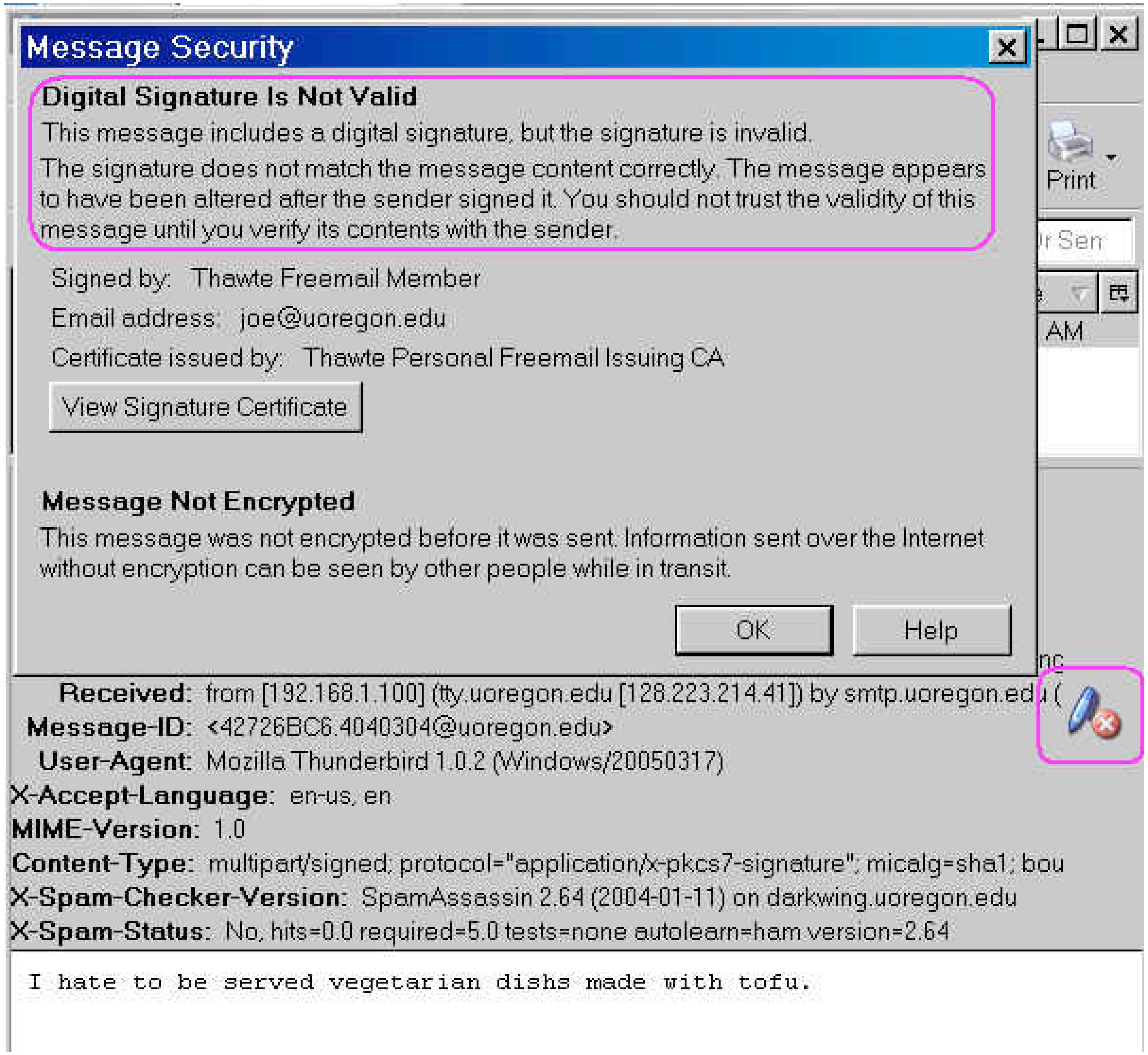
Message Security

Message Is Signed
This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: Thawte Freemail Member
Email address: joe@uoregon.edu
Certificate issued by: Thawte Personal Freemail Issuing CA

Message Not Encrypted
This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

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



Message Security

Digital Signature Is Not Valid

This message includes a digital signature, but the signature is invalid.

The signature does not match the message content correctly. The message appears to have been altered after the sender signed it. You should not trust the validity of this message until you verify its contents with the sender.

Signed by: Thawte Freemail Member

Email address: joe@uoregon.edu

Certificate issued by: Thawte Personal Freemail Issuing CA

Message Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

Received: from [192.168.1.100] (tty.uoregon.edu [128.223.214.41]) by smtp.uoregon.edu (

Message-ID: <42726BC6.4040304@uoregon.edu>

User-Agent: Mozilla Thunderbird 1.0.2 (Windows/20050317)

X-Accept-Language: en-us, en

MIME-Version: 1.0

Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; bou

X-Spam-Checker-Version: SpamAssassin 2.64 (2004-01-11) on darkwing.uoregon.edu

X-Spam-Status: No, hits=0.0 required=5.0 tests=none autolearn=ham version=2.64

```
I hate to be served vegetarian dishs made with tofu.
```

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):
  www.thawte.com/secure-email/personal-email-certificates/index.html

  -- Comodo (Yorkshire, UK):
  http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html

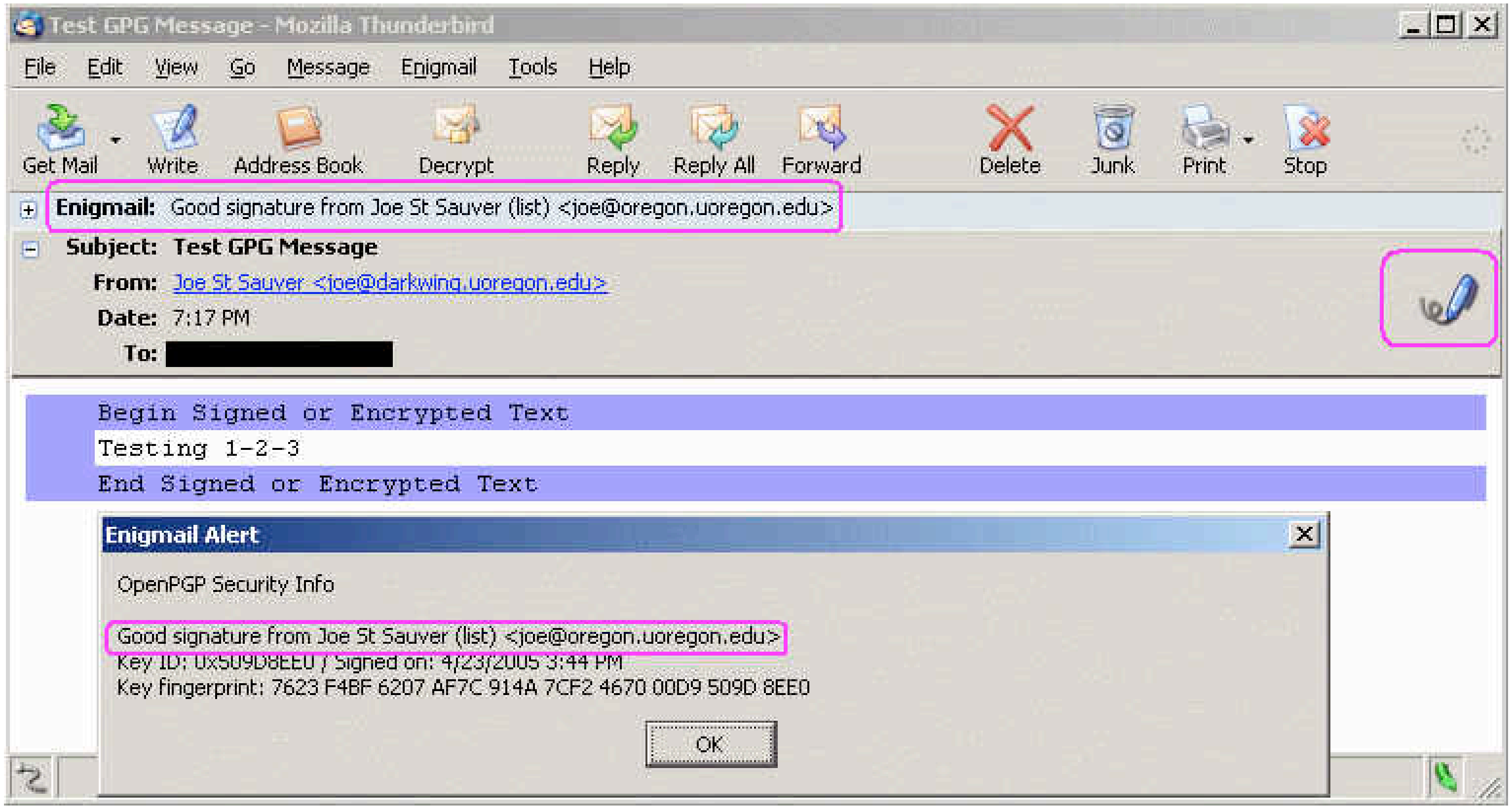
  -- ipsCA (Madrid, Spain):
  http://certs.ipsca.com/Products/SMIME.asp

  and there may be others…

Those Examples Used S/MIME, But You Could Also Use PGP

- PGP (and its free analog Gnu PrivacyGuard) can also be used to digitally sign emails.
- PGP/GPG is quite popular with technical audiences. 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 found 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 one-to-one.

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



Enigmail: Good signature from Joe St Sauver (list) <joe@oregon.uoregon.edu>

Subject: Test GPG Message
From: Joe St Sauver <joe@darkwing.uoregon.edu>
Date: 7:17 PM
To: [redacted]

```
Begin Signed or Encrypted Text
Testing 1-2-3
End Signed or Encrypted Text
```

OpenPGP Security Info

Good signature from Joe St Sauver (list) <joe@oregon.uoregon.edu>
Key ID: 0x509D8EE0 / Signed on: 4/23/2005 3:44 PM
Key fingerprint: 7623 F4BF 6207 AF7C 914A 7CF2 4670 00D9 509D 8EE0

- 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.

Why *Isn't* E-Mail Encryption Widely Used?

- At least in the old days, it was somewhat hard to get started with PGP/GPG (or even with S/MIME). Reseachers have done studies of what things seemed to cause problems for PGP/GPG. If you're interested, check out:
  Why Johnny Can't Encrypt
  www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf
  Why Johnny Still Can't Encrypt
  cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf
- At least some of the issues mentioned in that research have recently been eliminated through the development of simple interfaces for PGP/GPG such as Enigmail, see http://enigmail.mozdev.org/home/index.php
- That said, a technical orientation, and a friend who is already facile with PGP/GPG, are still quite helpful for those interested in independently using mail encryption.

Onesie-Twosie vs. Institutional Usage

- While individual users can employ S/MIME or GPG on a independent 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.
- If you need the bank president to host PGP key signing parties, you're not doing this right. :-)
- Fortunately, both S/MIME and PGP/GPG can be mechanically/automatically handled via commercial mail gateway hosts that will also handle the mechanics of key management creation and retrieval, etc.
- This is not a product spiel for any commercial vendor, however, so let me just suggest you discuss S/MIME or PGP/GPG signing with your current messaging vendor.

Digital Signatures Are *Not* A "Magic Bullet"

- For instance, 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 when issuing certificates, and depending on the vetting done, you may or may not really know the identify of the person who's "behind" a given cert.

  -- If you see the "message digitally signed" icon show up, try clicking on it and see what it tells 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?

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," 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 DKIM?

- DKIM is yet another cryptographic approach which is in use by Yahoo, Cisco, Google and others.
- DKIM is described in RFC 4871 and related documents; see http://www.dkim.org/ietf-dkim.htm
- There is something of a community perception that DKIM is “harder” than SPF (hey, DKIM is crypto-based, right?), but I **don’t** think it’s so hard that interested folks will find it to be impossible to deploy.
- DKIM historically focussed on mail which had been validly signed (e.g., DKIM sig is there & verifies as valid)
- But what if a message looks like it came from a domain that normally signs its mail, but that message isn’t signed? Folks are now working through this issue via http://tools.ietf.org/html/draft-ietf-dkim-ssp-09

Oh Yes: The Issue of Sheer Deliverability

- One more thing before we leave the topic of phishing and 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 ”this is probably spam” folders or otherwise not getting to where it should go.
- Pay attention to your bounce traffic or any complaints that your customers aren’t seeing mail that they expect to receive!
- Some vendors may offer deliverability management consulting services; again, you may want to talk with your current messaging vendor about this issue.

3. Review How You Use Domains

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 helps us by translating fully qualified domain names to IP addresses. For example:

  www.uoregon.edu ==> 128.223.142.89

  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 taken to your site; if things don’t work right, 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 coincidentally has a similar name, or to sites that have been intentionally set up to take advantage of common typos?

- 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. Bank, N.A., Cincinnati OH)

www.usbank.net ==> 170.135.216.181
  (U.S. Bank, N.A., Cincinnati OH)

www.usbank.org ==> 170.135.216.181
  (U.S. Bank, N.A., Cincinnati OH)

www.firstar.com ==> 170.135.216.181
  (U.S. Bank, N.A., Cincinnati OH)

www.usbancorp.com ==> 170.135.216.181
  (U.S. Bank, N.A., Cincinnati OH)

www.usbank.info ==> 170.135.216.181
  (U.S. Bank, N.A., Cincinnati OH)

www.usbank.cc ==> 170.135.216.181
  (U.S. Bank, N.A., Cincinnati OH)
```

Other Domain Variants May Be Expiring…

- Registrants may sometimes allow domains to expire…

```
Domain Name: USBANKSL.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS1.PENDINGRENEWALDELETION.COM
Name Server: NS2.PENDINGRENEWALDELETION.COM
Status: clientTransferProhibited
Updated Date: 09-mar-2009
Creation Date: 02-mar-1995
Expiration Date: 03-mar-2010
```

- This is not necessarily a sign that there is a problem (you do kind of find yourself worrying about who may re-register a domain like that one in the future, however)
- **Are any of YOUR domains about to expire?**

Other Times, Other Phenomena May Be Seen

- **Omit the first dot and you go to…**

```
wwwusbank.com ==> 82.98.86.173
  (domain whois: Mumbai Domains, Mumbai IN;
   IP whois: Sedo Domain Parking, c/o Plusline, Frankfurt, DE)
```

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

```
www.us-bank.com ==> 208.73.210.121
  (domain whois: private whois escrow via a Mumbai provider;
   IP whois: oversee.net, Los Angeles, California)
www.us.bank.com ==> 208.38.134.211
  (domain whois: First Place Internet, Clearwater, Florida;
   IP whois E Solutions Corporation, Tampa, Florida)
www.usbankcorp.com ==> 82.98.86.165
  (domain whois: S Pace, Boston Mass;
   IP whois: Sedo Domain Parking, c/o Plusline, Frankfurt, DE)
```

What (if anything), your bank wants to do about entities using what may appear to be “variants” of your company’s name or domain name is a good subject for a conversation with house legal counsel.

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 ==> 82.98.86.165
(domain whois: McCopin Creative, San Francisco, CA;
 IP whois: Sedo Domain Parking, c/o Plusline, Frankfurt, DE)

www.usbanknet.com ==> 216.188.26.235
(domain whois: Above.com Domain Privacy;
 IP whois: Trellian Limited, Beaumaris, Victoria, Australia)

www.firstarcom.com ==> 207.58.131.201
(domain whois: First Arcom, Jerusalem IL;
 IP whois: SMV, McLean, Virginia)
```

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, but perhaps there's still more work to be done…

Some usbank.<something> Domains…

-
  ```
  www.usbank.us ==> 208.73.210.50
    (domain whois: Gee Whiz Domains Privacy Service;
     IP whois, Oversee.net, Los Angeles CA)
  www.usbank.ca ==> 65.39.183.210
    (domain whois: [I'll let you draw your own conclusions here];
     IP whois: Barmetal.com, Inc, Victoria BC)
  www.usbank.co.uk ==>
    (domain whois: Amin Amor, Amsterdam NL;
     IP whois: ThePlanet/WebSiteWelcome, Boca Raton FL)
  www.usbank.cn ==> 61.156.40.100
    (domain whois information unavailable (whois.cnnic.net.cn
     doesn't answer); IP whois: CNCGROUP Shandong province)
  ```

Some other variants are also still unregistered or do not resolve; check your favorite generic TLDs and country codes (there are over 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 Domain Problem Is Not Specific To Any Single Bank

- While the preceding example looked at US Bank, this problem is NOT unique to them, so please don’t get the impression that I’m “picking on them” -- they’re actually doing far better than many banks on these issues, and I could just as easily have selected pretty much any other bank for similar results.

- This is a very difficult issue, particularly when you begin dealing with some of the more obscure TLDs.

Domain “Takeovers” or “Hijacking”

- Some of you may also know that some domains have been targeted for “take over” or hijacking by third parties.

  For example, ICANN and IANA themselves have had their domains hijacked (see “ICANN and IANA’s domains hijacked by Turkish Hacking Group,” June 26th, 2008, http://blogs.zdnet.com/security/?p=1356 and “Response to Recent Security Threats,” http://icann.com/en/announcements/ announcement-03jul08-en.htm (URL wrapped due to length).

  Can you imagine if **your bank** had been targeted for this sort of treatment instead of ICANN or IANA?

Talk With Your Registrar About How Your Domain Info Might Be Able to Be "Updated"

- While your domain names are critical online assets, you may be shocked to learn how easy it is to change or update your domain names (at least at some registrars).
- If I'm able to change your point of contact information (or your name servers), I can completely control your domain names, at least until any unauthorized changes are discovered and rolled back.
- When investigating this potential issue, be sure to look at both online and offline change mechanism (such as faxed "change authorizations" sent on letterhead).
- Look for strong cryptographic protection for your domains, or confirmation that the registrar requires out of band approval for changes from bank IT management.

You Also Need to Avoid Cache Poisoning

- Cyber criminals can also attack the resolution of your domains using a technique known as “cache poisoning.” (see for example, http://www.kb.cert.org/vuls/id/800113)
- When DNS cache poisoning takes place, a user can enter a 100% valid address for your bank, only to be magically taken to some other destination unrelated to your site.
- Individual ISPs can make it harder for cyber criminals to successfully engage in cache poisoning attacks, but not all ISPs have taken even the most minimal steps to harden their recursive resolvers against cache poisoning (You can test the ISPs you yourself may use with https://www.dns-oarc.net/oarc/services/porttest)
- Fortunately, just as SPF has materially reduced your risk of spoofed email, DNSSEC has the potential to eventually reduce the risks you face from cache poisoning.

How DNSSEC Works

- Sites (such as your bank) can cryptographically sign their DNS records.
- When customers attempt to access your bank’s website (at least from an ISP that is DNSSEC enabled), those customers will then be transparently protected from a number of DNS-based attacks (such as cache poisoning).
- The DNSSEC validation process is unnoticeable to users, but in order to protect DNS resolution, **two** things **must** occur: (a) sites (like your bank) must sign their DNS records, AND (b) your customer’s ISPs must verify the validity of those signatures.
- Obviously you can’t control what ISPs do all over the world, but **you CAN at least insure that you’ve signed your bank’s DNS records.**

Signing Your DNS Records

- The first step when it comes to deploying DNSSEC is talking to the people who do authoritative DNS for your domain. Let them know you'd like to use DNSSEC to secure your bank's domain name.
- Sometimes authoritative DNS service for your domain may be done in-house by your IT department, other times it may have been outsourced to a third party DNS service provider -- either way, tell them you'd like them to look into what would be required for you to begin signing your DNS.
- At least one registry (Afilias) is now offering a "one click" DNSSEC solution trial for selected dot org, dot info and dot gov domains (see http://www.afilias.info/1-click-dnssec). Regretably the registry that supports dot com domains isn't able to do "one click DNSSEC," but you can still use DNSSEC for dot com domains, it's just a little more work.

Malware That Changes Customer DNS Servers

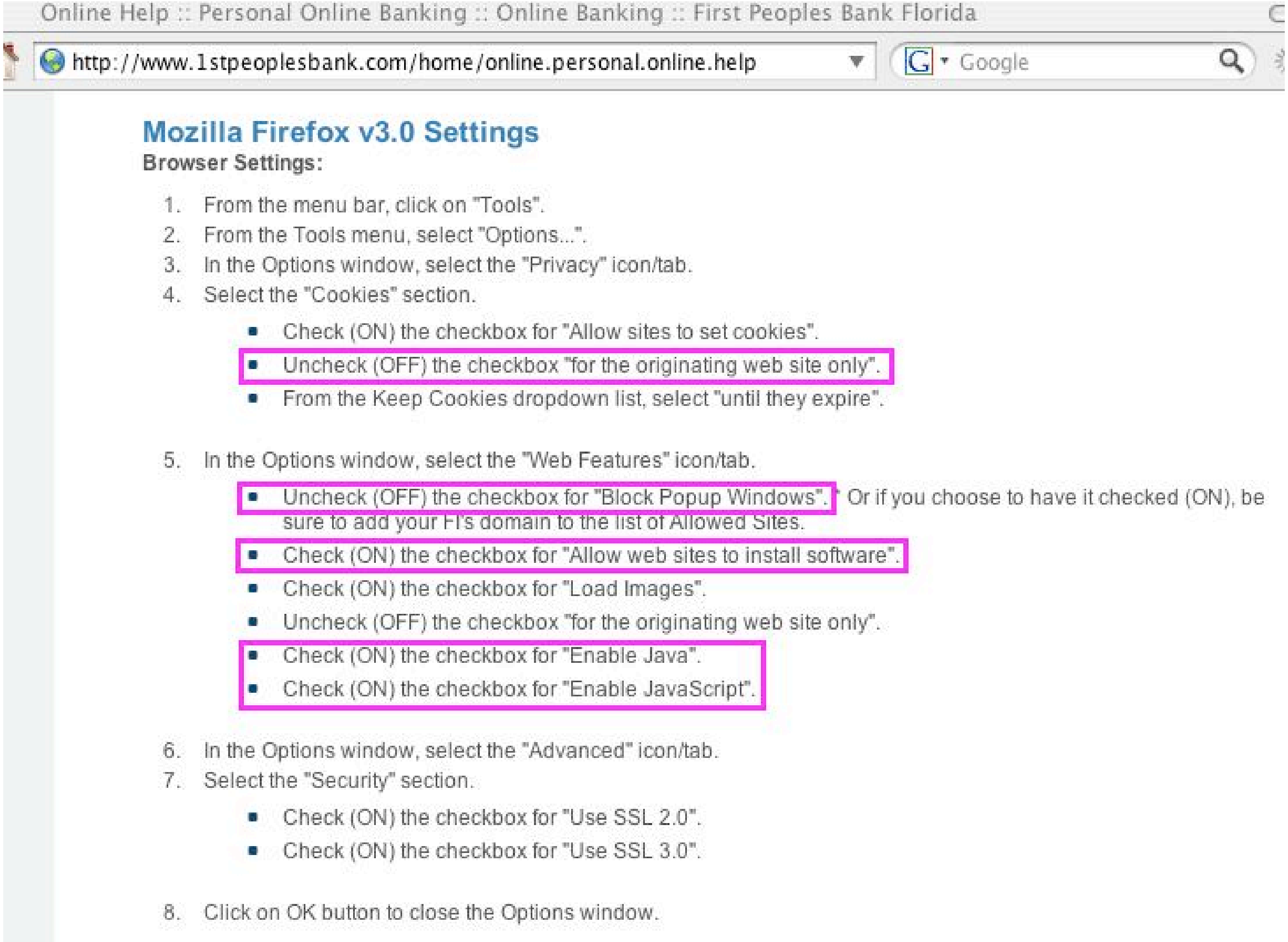
- A final DNS-related threat to keep in mind: some malware actually goes in and changes the recursive DNS servers that your customers' systems are configured to use.
- When this happens, instead of asking the normal ISP's DNS servers how to resolve domain names, the malware causes your customer's system to use rogue name servers under someone else's control. See for example the writeup at "DNSChanger.f", http://vil.nai.com/vil/content/v_141841.htm
- This is a potentially very difficult threat to counter (some ISPs have begun managing customer DNS traffic going to DNS servers other than the ISP's own, but attempting to do that can raise problems of its own.

4. Your World Wide Web Site

Let’s Move On To Your Website

- When users interact with your bank online, they likely do it via your web site. What’s their online experience like? Is your page fast, clean, and uncluttered, like Google’s? Or is your page cluttered with a lot of extraneous “features” that users really don’t use?
- Have you thoroughly scrutinized your website to insure that it doesn’t have any of the web application errors flagged by the OWASP project? (see http://www.owasp.org/index.php/Top_10_2007)
- Where relevant, are you running a web application firewall, such as modsecurity? (www.modsecurity.org)
- Do you require your customers to enable potentially risky technologies, such as Javascript, or to enable web sites to install software? You shouldn’t! And similarly, don’t allow users to continue to use antique OS’s & browsers!

Some Settings That One Bank Recommends



Online Help :: Personal Online Banking :: Online Banking :: First Peoples Bank Florida
http://www.1stpeoplesbank.com/home/online.personal.online.help
Google

Mozilla Firefox v3.0 Settings

Browser Settings:

1. From the menu bar, click on "Tools".
2. From the Tools menu, select "Options...".
3. In the Options window, select the "Privacy" icon/tab.
4. Select the "Cookies" section.
   - Check (ON) the checkbox for "Allow sites to set cookies".
   - Uncheck (OFF) the checkbox "for the originating web site only".
   - From the Keep Cookies dropdown list, select "until they expire".
5. In the Options window, select the "Web Features" icon/tab.
   - Uncheck (OFF) the checkbox for "Block Popup Windows". Or if you choose to have it checked (ON), be sure to add your FI's domain to the list of Allowed Sites.
   - Check (ON) the checkbox for "Allow web sites to install software".
   - Check (ON) the checkbox for "Load Images".
   - Uncheck (OFF) the checkbox "for the originating web site only".
   - Check (ON) the checkbox for "Enable Java".
   - Check (ON) the checkbox for "Enable JavaScript".
6. In the Options window, select the "Advanced" icon/tab.
7. Select the "Security" section.
   - Check (ON) the checkbox for "Use SSL 2.0".
   - Check (ON) the checkbox for "Use SSL 3.0".
8. Click on OK button to close the Options window.

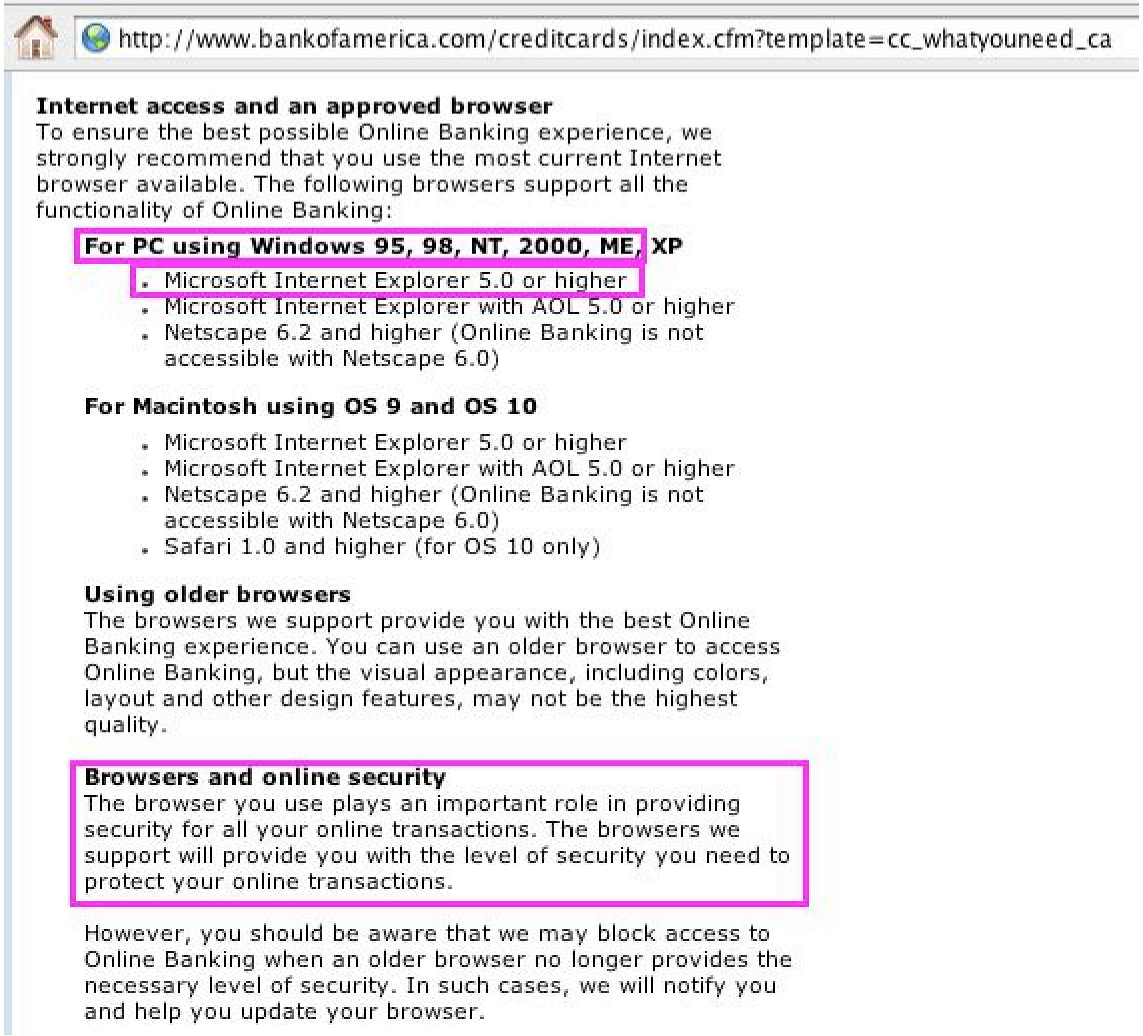
Remember, Users Use ALL Sorts of Websites, Not Just Your Bank's Website!

- Even if some browser settings are arguably safe to use on your bank's web site, if you recommend risky browser configurations, you run the risk of your customers getting compromised when they visit other web sites.

- Once they're compromised, wherever they get compromised it will be bad news for you if they then do online banking from that system.

- Work to make sure that your web site encourages your customers to harden their configuration, don't casually require them to undercut critical security features and settings.

For Example: Should We *Really* Still Be Telling Users It's Okay to Use W/95 or NT?



http://www.bankofamerica.com/creditcards/index.cfm?template=cc_whatyouneed_ca

Internet access and an approved browser
To ensure the best possible Online Banking experience, we strongly recommend that you use the most current Internet browser available. The following browsers support all the functionality of Online Banking:

For PC using Windows 95, 98, NT, 2000, ME, XP

- Microsoft Internet Explorer 5.0 or higher
- Microsoft Internet Explorer with AOL 5.0 or higher
- Netscape 6.2 and higher (Online Banking is not accessible with Netscape 6.0)

For Macintosh using OS 9 and OS 10

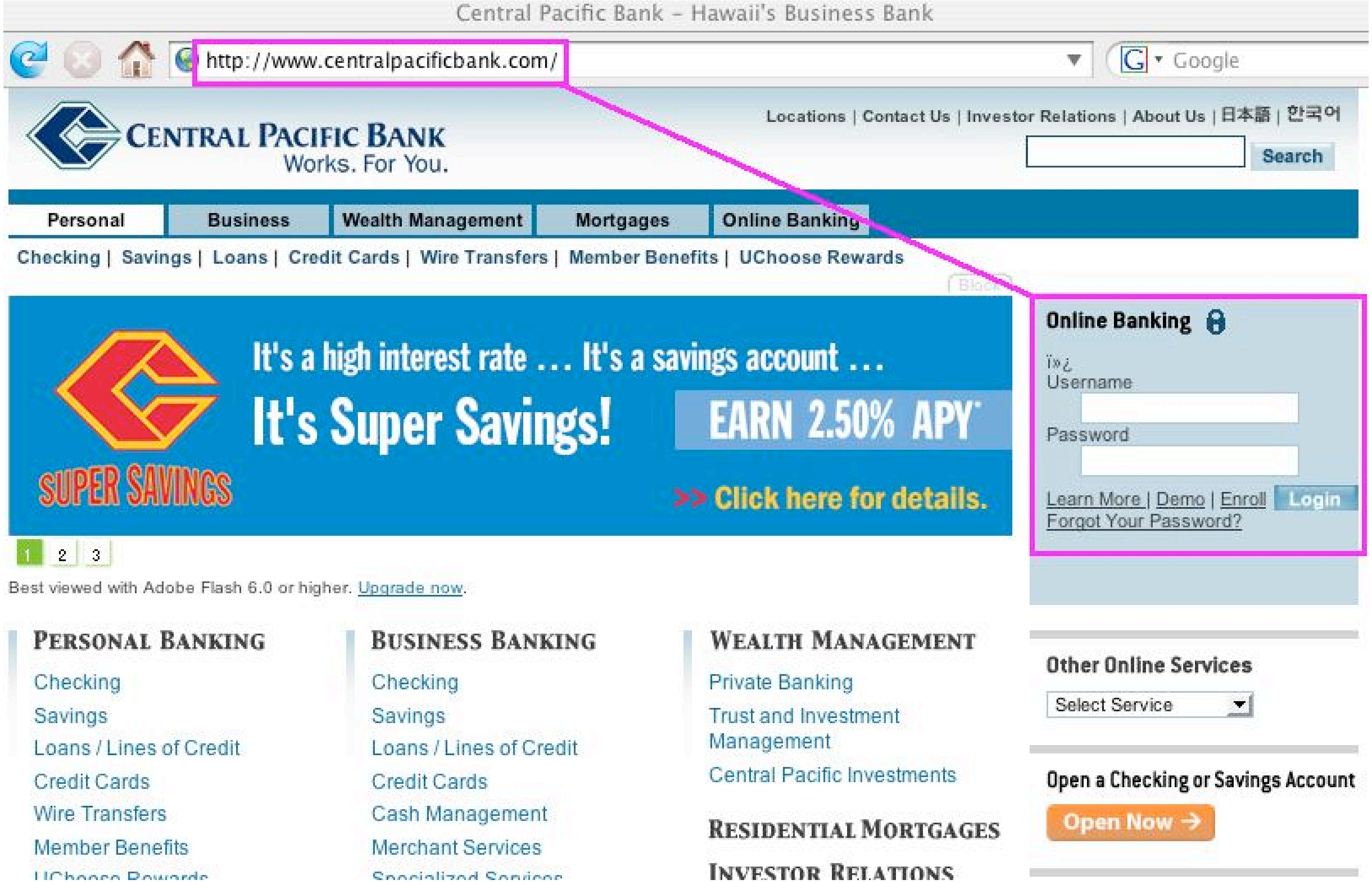
- Microsoft Internet Explorer 5.0 or higher
- Microsoft Internet Explorer with AOL 5.0 or higher
- Netscape 6.2 and higher (Online Banking is not accessible with Netscape 6.0)
- Safari 1.0 and higher (for OS 10 only)

Using older browsers
The browsers we support provide you with the best Online Banking experience. You can use an older browser to access Online Banking, but the visual appearance, including colors, layout and other design features, may not be the highest quality.

Browsers and online security
The browser you use plays an important role in providing security for all your online transactions. The browsers we support will provide you with the level of security you need to protect your online transactions.

However, you should be aware that we may block access to Online Banking when an older browser no longer provides the necessary level of security. In such cases, we will notify you and help you update your browser.

OK. Let’s Move On! Another Bank Web Page



Central Pacific Bank – Hawaii's Business Bank

http://www.centralpacificbank.com/

CENTRAL PACIFIC BANK
Works. For You.

Locations | Contact Us | Investor Relations | About Us | 日本語 | 한국어

Personal | Business | Wealth Management | Mortgages | Online Banking

Checking | Savings | Loans | Credit Cards | Wire Transfers | Member Benefits | UChoose Rewards

It's a high interest rate … It's a savings account …
It's Super Savings!
EARN 2.50% APY*
SUPER SAVINGS
>> Click here for details.

Best viewed with Adobe Flash 6.0 or higher. Upgrade now.

Online Banking

ï»¿
Username
Password

Learn More | Demo | Enroll

Forgot Your Password?

PERSONAL BANKING
- Checking
- Savings
- Loans / Lines of Credit
- Credit Cards
- Wire Transfers
- Member Benefits
- UChoose Rewards

BUSINESS BANKING
- Checking
- Savings
- Loans / Lines of Credit
- Credit Cards
- Cash Management
- Merchant Services
- Specialized Services

WEALTH MANAGEMENT
- Private Banking
- Trust and Investment Management
- Central Pacific Investments

RESIDENTIAL MORTGAGES

INVESTOR RELATIONS

Other Online Services

Select Service

Open a Checking or Savings Account

A Quick Question About The Bank Web Page You Just Saw…

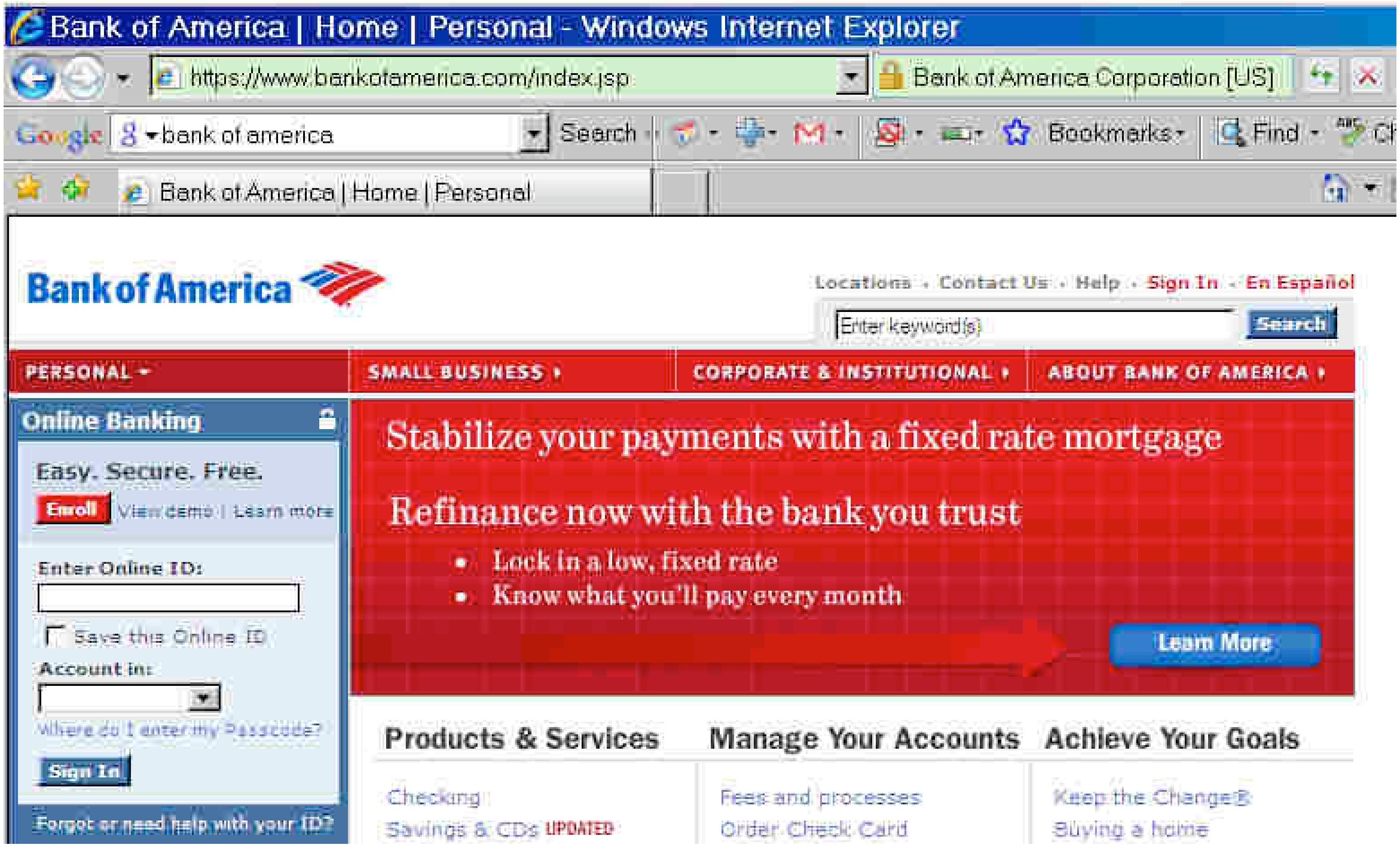
- If that's a secure login page, to avoid confusion why isn't the page URL "https" prefixed? (and no, the little padlock doesn’t show up where it should on the status bar either)
- Yes, I do understand that parts of an insecure page can still be transmitted securely, but using that sort of approach potentially confuses users and makes it easier for the bad guys and bad gals to get away with bad things.
- A growing number of major banks now routinely have their **entire home page** delivered via an https page, and that’s a very good practice in my opinion.

- ***What does your bank do?***

Extended Validation Certificates

- All SSL certificates are not the same.
- At one time, in the “good old days,” certificates were issued only after painfully extensive validation procedures, these days obtaining a web certificate may only require the ability to be able to receive an email message sent by the cert issuer to a point of contact address associated with your domain. That doesn’t provide very much in the way of “identity verification.”
- Extended validation certificates (so-called “green bar” certificates) are meant to reverse some of that errosion of trust. In exchange for paying an additional (substantial!) fee and going through fairly rigorous validation procedures, your site can be issued an EV cert that will cause the address bar of your customer’s browser to “turn green” when they visit you. E.G., …

Here's What BOA's "Green Bar" Extended Validation Cert Looks Like…



Bank of America | Home | Personal - Windows Internet Explorer

https://www.bankofamerica.com/index.jsp

Bank of America Corporation [US]

Easy. Secure. Free.

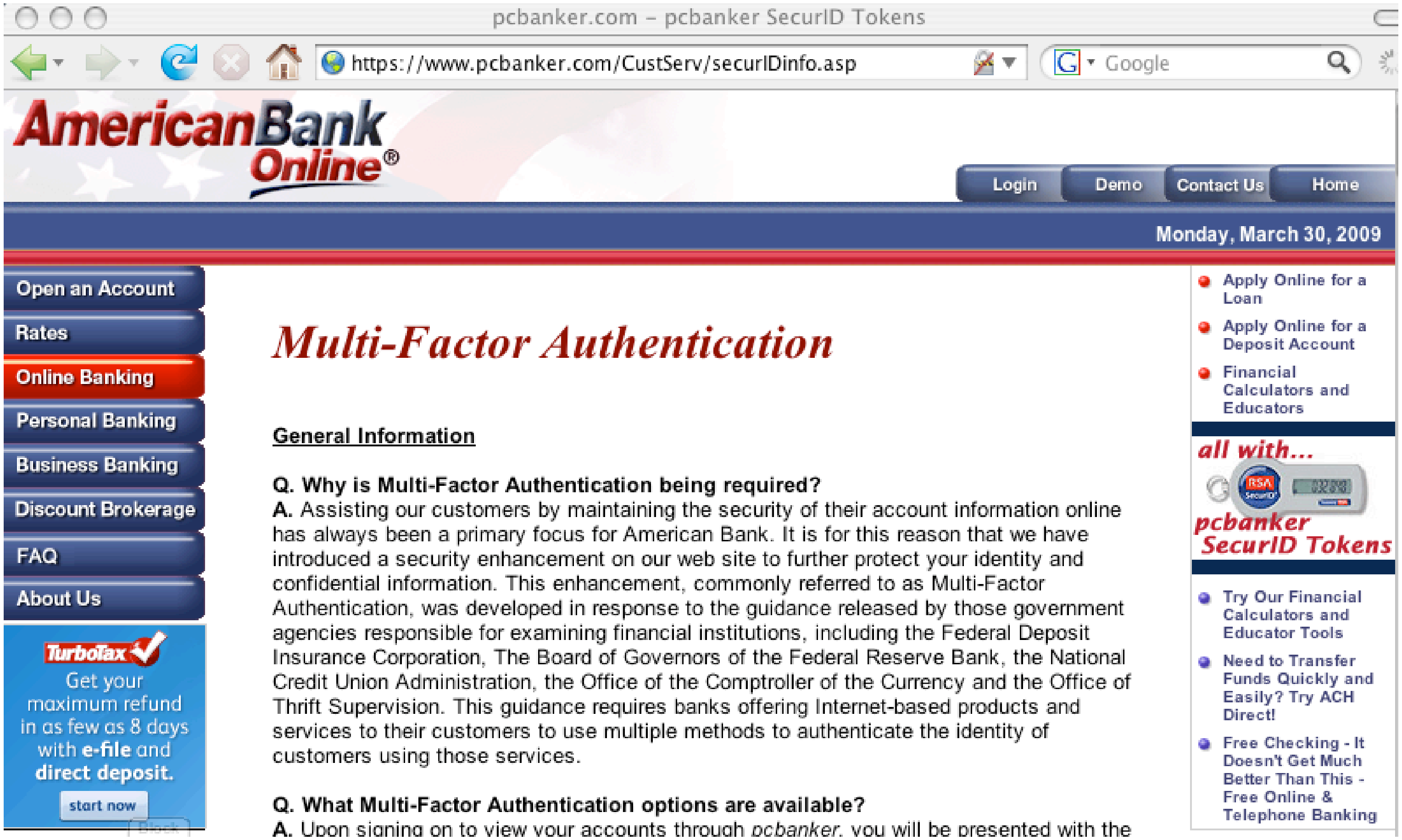
Stabilize your payments with a fixed rate mortgage

Refinance now with the bank you trust

- Lock in a low, fixed rate
- Know what you'll pay every month

The Next Step in Securing Bank Websites

- The next step that a growing number of banks will likely find themselves considering will likely be cryptographic hardware tokens; some banks are already deploying ‘em



pcbanker.com – pcbanker SecurID Tokens
https://www.pcbanker.com/CustServ/securIDinfo.asp
Google
AmericanBank Online®
Login
Demo
Contact Us
Home
Monday, March 30, 2009
Open an Account
Rates
Online Banking
Personal Banking
Business Banking
Discount Brokerage
FAQ
About Us
TurboTax
Get your maximum refund in as few as 8 days with e-file and direct deposit.
start now
Apply Online for a Loan
Apply Online for a Deposit Account
Financial Calculators and Educators
all with...
RSA SecurID
pcbanker SecurID Tokens
Try Our Financial Calculators and Educator Tools
Need to Transfer Funds Quickly and Easily? Try ACH Direct!
Free Checking - It Doesn't Get Much Better Than This - Free Online & Telephone Banking

Multi-Factor Authentication

General Information

Q. Why is Multi-Factor Authentication being required?
A. Assisting our customers by maintaining the security of their account information online has always been a primary focus for American Bank. It is for this reason that we have introduced a security enhancement on our web site to further protect your identity and confidential information. This enhancement, commonly referred to as Multi-Factor Authentication, was developed in response to the guidance released by those government agencies responsible for examining financial institutions, including the Federal Deposit Insurance Corporation, The Board of Governors of the Federal Reserve Bank, the National Credit Union Administration, the Office of the Comptroller of the Currency and the Office of Thrift Supervision. This guidance requires banks offering Internet-based products and services to their customers to use multiple methods to authenticate the identity of customers using those services.

Q. What Multi-Factor Authentication options are available?
A. Upon signing on to view your accounts through *pcbanker*, you will be presented with the

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 online 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 a worthwhile objective to pursue?

John's Going to Go Into Multifactor Authentication In More Detail, So…

- I won't belabor the issue here, but it is critical for you to be thinking about true multifactor authentication for your customers.

- Even if it can't protect against all attacks, it certainly make a successful attack against your bank FAR more difficult than if you're just using plain passwords, or other simple expedients that try to improve on plain passwords.

- Plain old passwords are dead, let's all move on.

Blocking Access to Online Banking From Some Places Abroad

- If banks allow access to customer online banking web sites from anywhere in the world, they may want to reconsider that decision given the fact that the vast majority of their customers probably do **<u>not</u>** travel internationally.

- 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.

- Of course, in some cases it may be hard to determine the true geolocation of a given Internet user due to abuse of open proxy servers and criminal VPN services, but many of those can also be readily identified and blocked today.

Banks Should Also Be Monitoring Their Web Servers 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 phish 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 their "graphical intellectual property" without permission.
- Not surprisingly, solutions have been developed.

Anti-Leach

- 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 servers’ logs!

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 provid, 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), low-dollar attacks may not.
- Thus, a 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 Need To Communicate With Their Customers; For Some Reason Customers May Not Trust Stuff Emailed 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 a KEY element 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 contact
  actually go through as RFC2142 (and common sense) say it should?

- Check www.rfc-ignorant.org for your domain!

Leverage Phish Reporting Sites

- Are you taking full advantage of free phish reporting sites such as PhishTank (see http://www.phishtank.org/)?

- If not, maybe that would be worth considering?

6. What’s Next?

There Are Many Trains Coming Down the Track

- We've already talked about some of them, such as DNS-based attacks and the importance of moving to true multifactor authentication.

- However, let's just talk about two others before concluding today:

  -- Fast flux hosting of phishvertised sites, and

  -- VoIP-based phishing

Fast Flux Hosting of Phish Sites

- Most real web sites are hosted on conventional web servers. A domain name such as www.example.com points at a single machine, or small set of machines sitting behind a load balancer.
- These days, however, a growing number of phishing sites (and other illegal content) is hosted on fast flux web sites.
- When fast flux hosting is used, cyber criminals take advantage of compromised consumer PCs, pointing a phishvertised web site at a small pool of those compromised PCs. Rather than copy all their content onto each compromised PC, they just transparently tunnel connections made to the compromised back to a “mothership” system hosted somewhere else. If one PC goes down or gets cleaned up, another one replaces it.

Cleaning Up Fast Flux Hosting

- Ultimately, cleaning up fast flux hosting will likely require the cooperation of registrars and registries.
- ICANN GNSO established a fast flux working group to try to begin tackling this issue, a working group I participated in, but quite frankly, most banks (all banks?) didn’t really pay much attention to this issue, even though fast flux approaches enable and sustain many of the phishing attacks being perpetrated against banks worldwide.
- If you haven’t heard of fast flux before, but you’d like to learn more, you may want to see the initial report of thde ICANN GNSO Fast Flux Working Group, see http://gnso.icann.org/issues/fast-flux-hosting/ fast-flux-initial-report-26jan09.pdf (URL split due to length)

Phone-Based Phishing

- While most phishing is taking place via email right now, phone-based phishing is also a growing problem

- 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…

- Hugely popular with legitimate users (Skype, for example, has had a ***billion*** downloads now, see http://share.skype.com/sites/en/2008/09/celebrating_1_billion_download.html)
- VoIP can be gatewayed to and from the plain old telephone system
- VoIP routinely supports 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 can be very difficult to trace when it gets abused

We Need Effort Focussed on VoIP Abuse

- A lot of the cybercrime that leverages VoIP is poorly reported and erratically worked by law enforcement because it is so hard to do so. One only needs to Google for VoIP numbers seen in fraudulent or otherwise abusive emails to run into examples of numbers that have been live for months if not years.
- There has been great progress when it comes to dealing with email and web abuse on the Internet as a result of efforts by groups such as Spamhaus (see www.spamhaus.org), but to the best of my knowledge, there's nothing currently like Spamhaus for VoIP.
- We desperately need the equivalent of Spamhaus for VoIP.
- We also need law enforcement officers focussed on phone related issues, even if it isn't as "cool" as "network" crimes.

Thanks For The Chance to Talk Today!

- Are there any questions?