

Phishing: Some Technical Suggestions for Banks and Other Financial Institutions

2005 Quad State Security Conference

9:45-10:45 AM May 5th, 2005

The Resort at the Mountain, Welches OR

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

University of Oregon Computing Center

<http://darkwing.uoregon.edu/~joe/quadstate/>

This Talk

- This talk came about following a phishing talk I did for the Valley Fraud Group in Eugene; I'm delighted to have the chance to share some material from that talk plus some additional items with a wider audience here today.
- By prior arrangement with Sean, he's provided you with an introduction to the phishing problem and a legal perspective; this talk will be more oriented toward what banks and other financial institutions can do on a technical basis plus some investigative tools and approaches you may find useful and appropriate.
- 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.

The Audience for Today's Talk

- I know that many of you have probably been working on phishing and cybercrime-related issues far longer than I have; if you're not using some of the practices I'm going to mention, it is probably for managerial or financial reasons, or simply because you're busy putting out other more pressing fires first, or maybe because they're bad ideas. :-)
- I've been told to expect an audience comprised of financial institution security folks, law enforcement people, and some managerial/operational IT/networking folks... I've attempted to tailor my coverage accordingly.
- I will do my best to keep this from being a "how-to-phish more successfully" tutorial for the bad guys" and only share information that is already available from public sources.

Being Pragmatic

- While your customers' concerns are always important, our focus for this talk, today, will primarily be on your institution's interests, and we're going to focus on what's "practically doable."
- We recognize that if a proposal doesn't make business sense, it probably won't happen – the numbers need to work, and it needs to work with your business processes. We understand that the lawyers need to be happy, too.
- Solutions need to scale to Internet scale audiences.
- We recognize that every institution's circumstances will differ, and we don't expect universal adoption of everything (or anything) proposed during this talk.
- Even if you do everything mentioned/suggested today, you can still get hit by phishing; there is no magic bullet.

[Potential] Financial Institution 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 YOUR Financial Institution, 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 widespread 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 your customers right NOW.

Don't You Just Love It When They Refer To You As A "Softer Target?"

washingtonpost.com: Phishers Drop Hooks Into Smaller Streams - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.washingtonpost.com/ac2/wp-dyn/A32199-2005Jan24?language=printer

Firefox Help Firefox Support Plug-in FAQ

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 Wyrman, director of marketing for CCFCU.

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...

The screenshot shows a web browser window with the URL <http://www.scmagazine.com/features/index.cfm?fuseaction=featureDetail&id=1000000000000000000>. The page title is "Features". The main headline is "Washington has a new champion" by Illena Armstrong. Below the headline, there is a paragraph about Dave Cullinane, SC's CSO of the Year, telling Illena Armstrong why infosec professionals need to be at the center of decision-making – and the best way to kill phishing sites. A photo of Dave Cullinane is shown to the right. A pink box highlights a quote from him: "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." Below this quote, another paragraph continues his statement about the pervasiveness of phishing attacks.

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

Technical Approaches to Dealing With Phishing Need to Come From YOU

- Your institution's senior management team cannot be expected to be conversant with highly technical emerging computing and networking security topics – they rely on you for that.
- Evaluating, and where appropriate, *advocating*, technical antiphishing measures (including possibly some discussed in this talk today) will depend in large measure on your interest and involvement.
- 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 your institution 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.
- “You” could have been sending email from anywhere. ¹⁵

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, domain owner publish 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 you 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!”¹⁶

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 you publish an SPF record, and IF the ISP that received “your” mail checks the SPF records you’ve published, spoofed mail that claims to be “from” your 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:sfmx02.bankofamerica.com
a:sfmx04.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

mbna.com

nationalcity.com

oregoncommunitycu.org

pncbank.com

regions.com

selco.org

suntrust.com

visa.com

wachovia.com

wamu.com

wellsfargo.com

worldsavings.com

etc., etc., etc.

- Sorry if I missed checking your institution's domain! :-) 21

When You Publish SPF Records, Make Sure You Publish for ALL Your 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...

- Review the SPF Whitepaper (really, *please*, RTFM :-))...
<http://spf.pobox.com/whitepaper.pdf>
- Get managerial/institutional “buy-in”
- Figure out where your mail will legitimately be coming from (including any authorized business partners)
- Decide what you ultimately want to have happen to mail that’s coming from a “wrong place” – hard fail? Soft fail? Just note/log its existence, starting gently at first?
- Then run the SPF Wizard to help you craft an initial SPF record: <http://spf.pobox.com/wizard.html>
- Check it using <http://freshmeat.net/projects/spfval/> or <http://www.vamsoft.com/orf/spfvalidator.asp>
- Have your DNS people publish your SPF records
- Refine your SPF records based on what you 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 your site can do one without having to do the other.
- **Also Note:** you 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 gives you 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.mspx>
- 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.²⁷

2. Digitally Sign the Messages You Do Send to Your Customers

Making Sure That The Email You Send Remains Credible

- While publishing SPF records will help to reduce the amount of spoofed phishing email many of your users might receive, what about the legitimate mail you'd like to send to your customers? Does the phishing problem mean that you need to abandon use of email as a communication channel?
- No... However, you SHOULD be moving toward digitally signing all bank email.
- Digital signatures allow your 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.

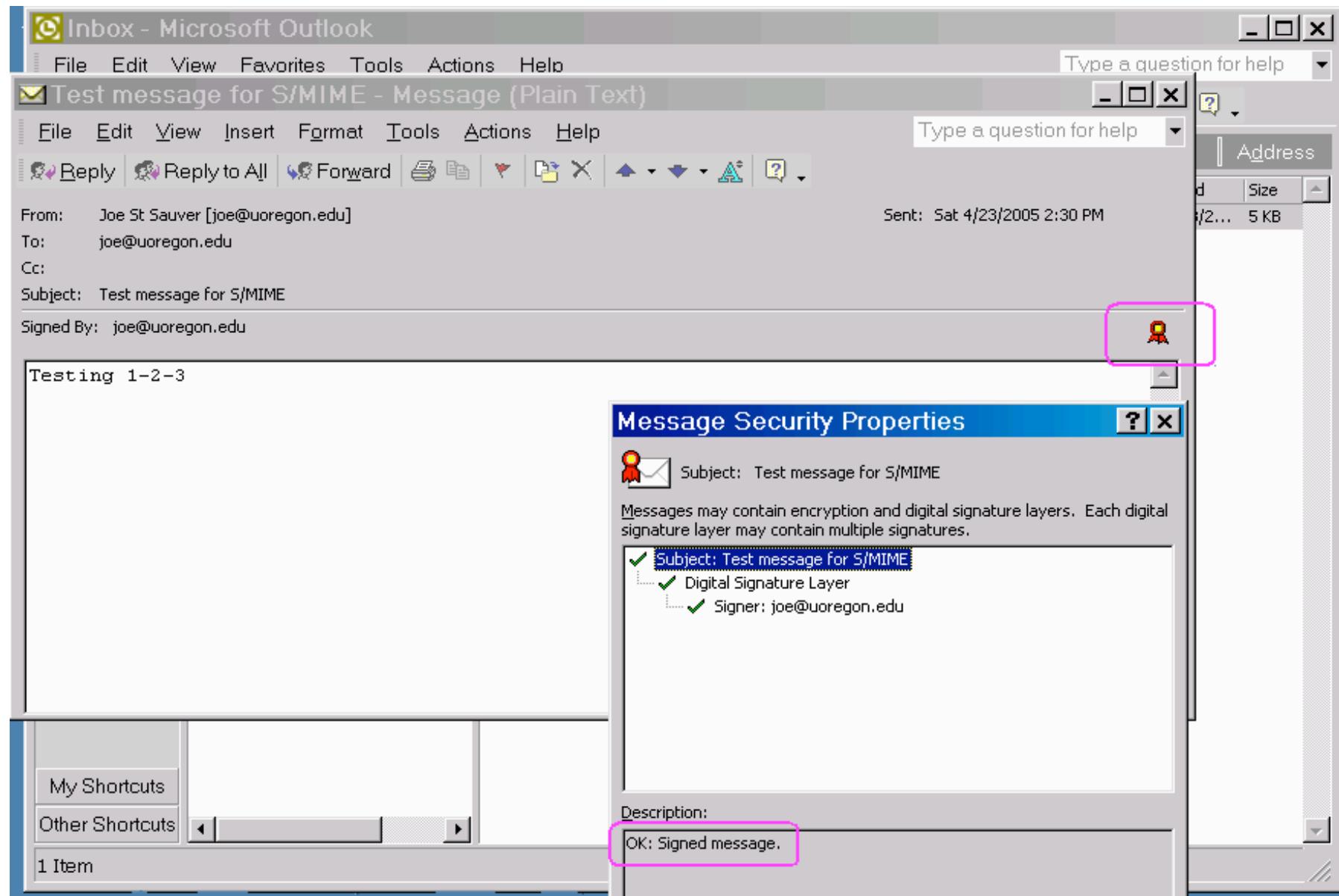
Digital Signing Is NOT Message Encryption

- 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 to be encrypted, but ALL of bank email should be digitally signed.

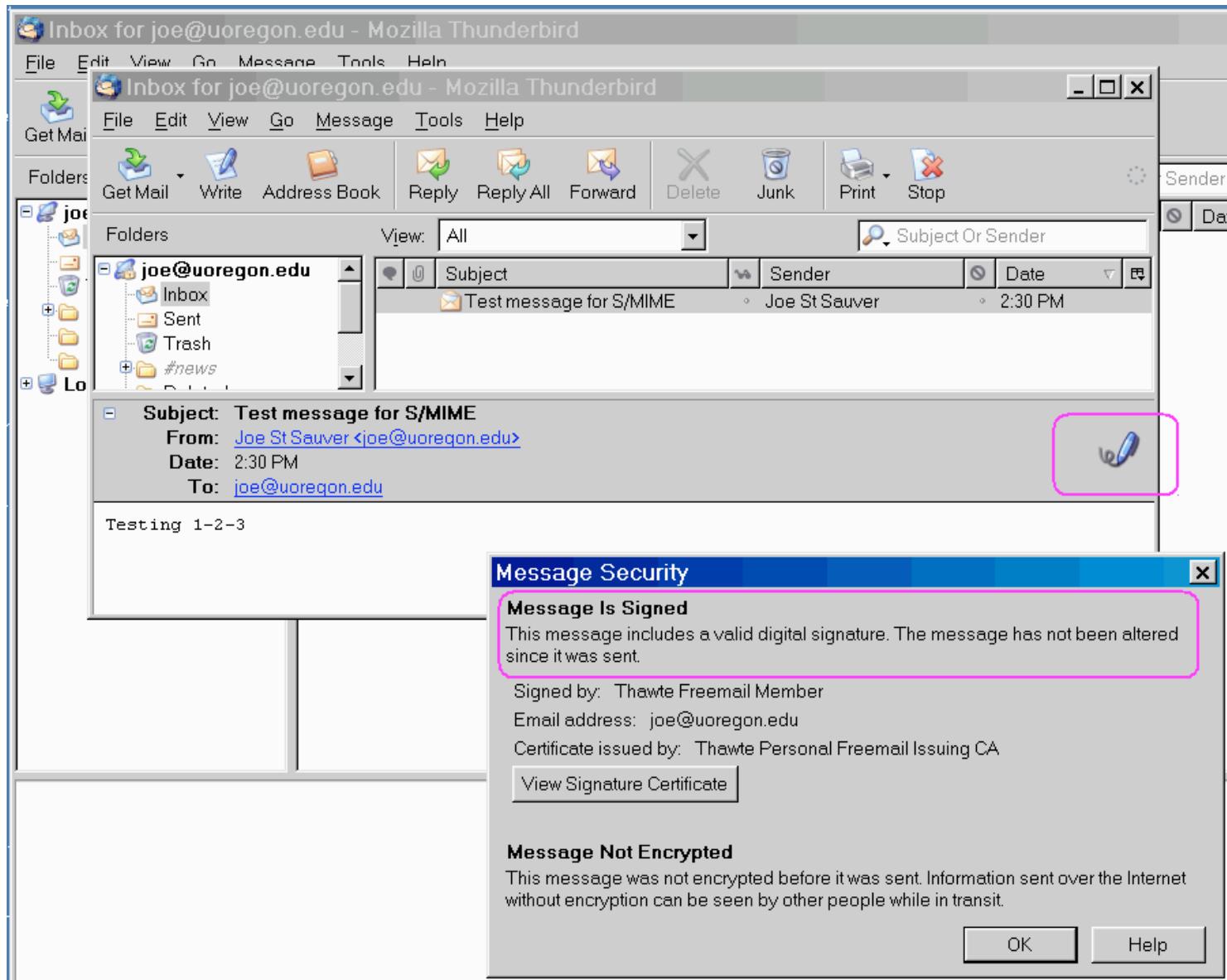
Will Customers Even *Know* or CARE What a Digital Signature Is?

- We know/agree that most of your 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...

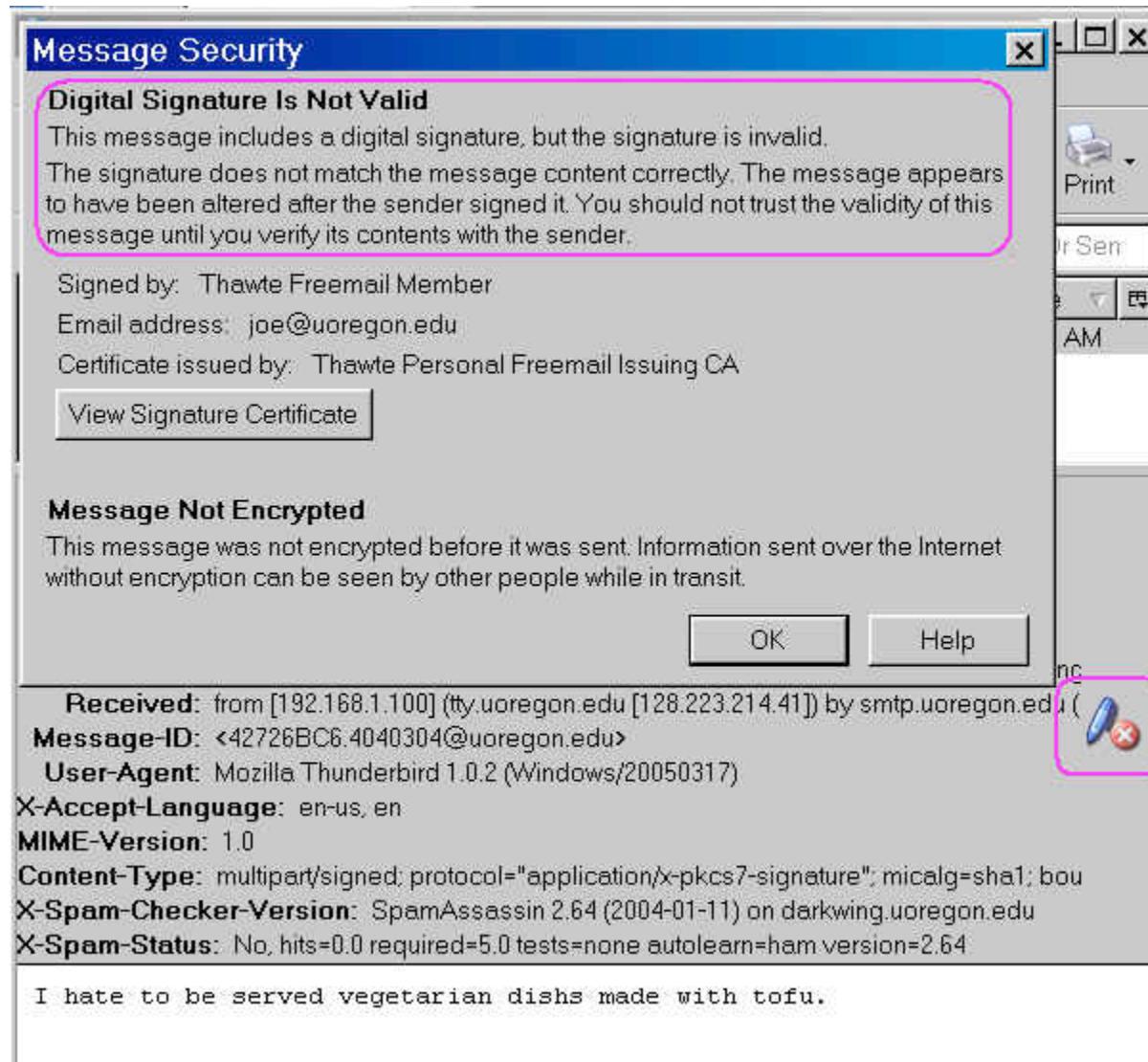
An S/MIME Signed Message in Microsoft Outlook



An S/MIME Digitally Signed Message In Thunderbird



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



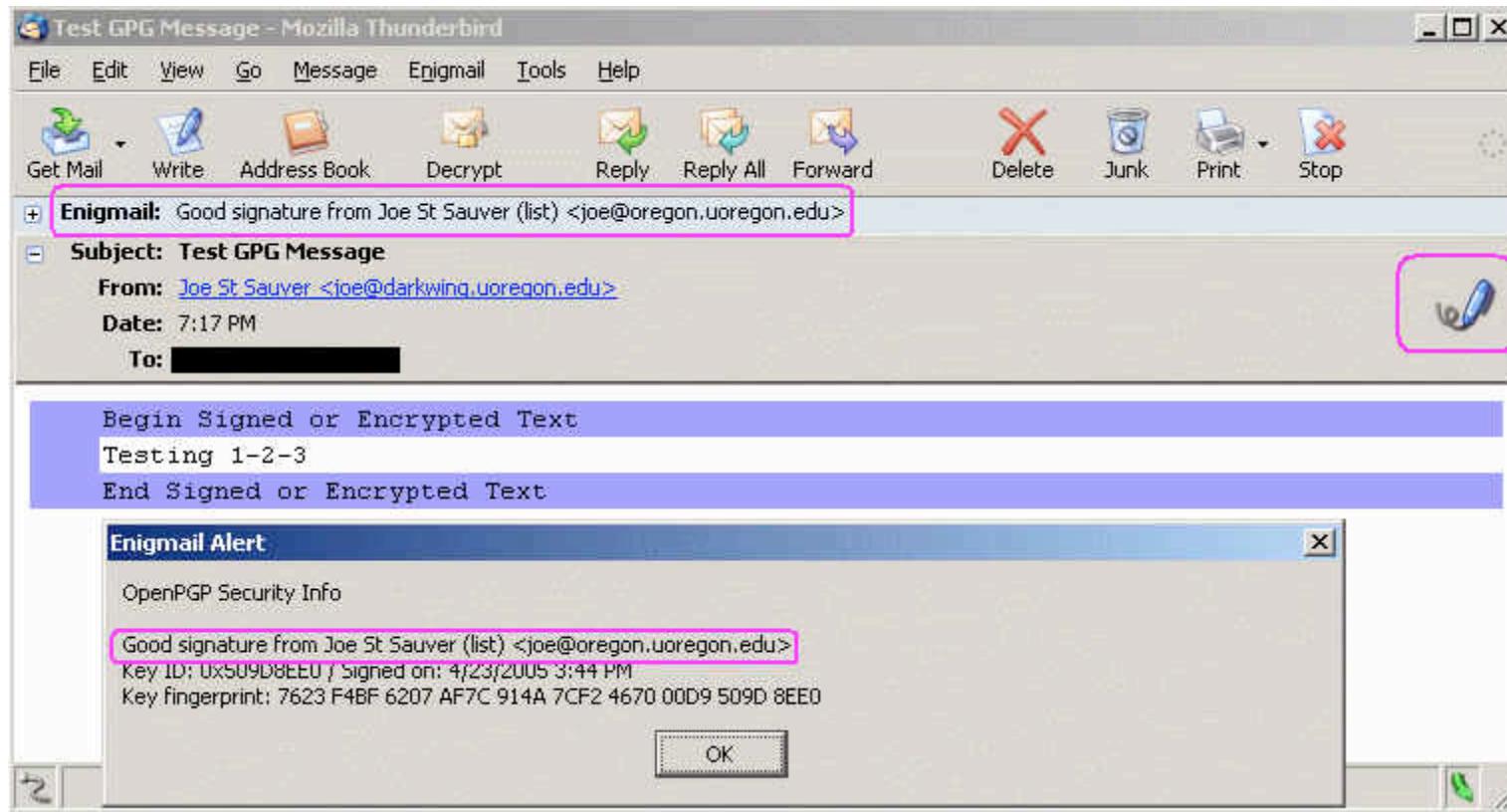
Trying S/MIME Yourself

- 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.ipasca.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
or see http://www.opengroup.org/smgi/cert/cert_prodst.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 identify 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?¹

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
- 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 you do develop problems with being blocked by some sites, one possible way of proving your 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 your web site 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.firststar.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)

wwwfirstar.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 your 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
s e r v i c e s

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

Get back to life.

CardMember
s e r v i c e s

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!

Visa Deals
Shopping made simple. [View special offers](#) from top web merchants.

Running Late...
No problem. Save the stamp and [Make your payments online right now](#).

Why Pay More?
Don't be stuck with high interest rates. Transfer a balance today and save! [Learn More](#)

 **Save the Children®**
USA

**Children in Asia
Need Help Now**

UPDATING: Security notice on e-mail fraud.

[Apply for a Credit Card](#)

[Announce for a Business Credit](#)

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 G

onlinefirstusa.com

What you need, when you need it

January 24th, 2005

[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

[Bank one credit card](#) [Pay bill](#) [First usa](#)
[Online services](#) [Credit card payment](#) [Bankone.com](#)
[Credit card payments](#) [Visa](#) [Bank one](#)
[Bill pay](#) [Statements](#) [Online banking](#)
[Car rental](#) [British air](#) [United airline](#)
[Sony](#) [Marriott](#) [United](#)

Favorite Categories

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

Search: Search

Bank One Credit Card | Pay Bill | First Usa | Online Services | Credit Card Payment | Bankone.com | Credit Card Payments | 57

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).
- Does YOUR site make it that easy for users to bookmark your real online banking site? What is your expectation for your users' home page? Do you have a home page that you recommend that they use, perhaps something like an "institutionally tweaked" version of a popular start page, prominently featuring a convenient link to your institution'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 does your bank's real web site also include non-institutional links?

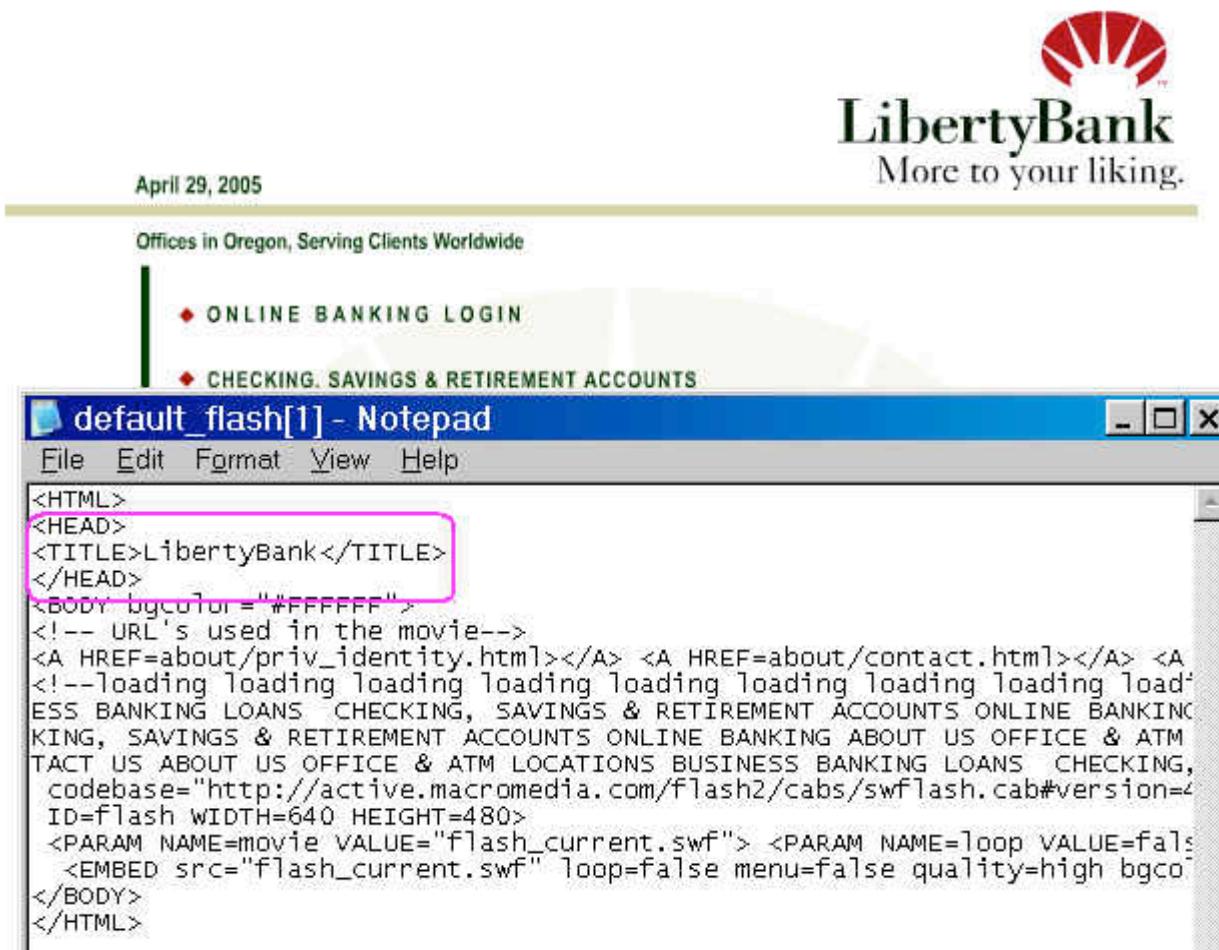
If you scroll back to the real bank page in this example, you'll see it links to "Save The Children" – unquestionably a worthy cause, but a dilution of the banks' web site's organic purpose and identity...

Be conservative and careful about anything that distracts from user assessment of your 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 – does your bank's real web site include keyword data "meta tags" in your web page's header aimed at helping Internet search engine users find your real web site?
- 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

The screenshot shows a Google search results page with the query "liberty bank". The results are categorized under "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/ - 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/ - 21k - [Cached](#) - [Similar pages](#)
- It's Your Bank ... Liberty Bank for Savings, Chicago, IL USA**
A locally owned, community oriented **bank**.
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/ - 9k - [Cached](#) - [Similar pages](#)
- Liberty Bank**
Liberty Bank has branches in Boulder Creek, Ben Lomond, and Felton.
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 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 Your Institutional Identity/Key Related Search Terms?

- Even if you do a great job of getting your 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 search for your bank's name, who (if anyone) shows up as a sponsored listing?
- While in most cases the folks who show up will simply be competing institutions, brokers, etc., what if a phisher did bid for your institutional identity, got good placement, and then attracted phishing victims that way?
- Are you even tracking what your 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 Results for "wells fargo" - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://search.yahoo.com/search?p=%22wells+fargo%22&prssweb=Search&

Yahoo! My Yahoo! Mail Welcome, Guest [Sign In] Search Home Help

Web Images Video Directory Local News Products

YAHOO! SEARCH ["wells fargo"] Search

My Web BETA

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
- [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

SPONSOR RESULTS

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

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

Shortcuts Advanced Search Preferences

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

[Wells Fargo Home Loans Online](#)
LendingLeaders.com will attempt to match you with a **Wells Fargo** broker. If not...
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

[Wells Fargo Mortgage - Free Quotes](#)
Get important **Wells Fargo** information. Includes a free service to compare mortgage....
www.4mortgagehelp.org

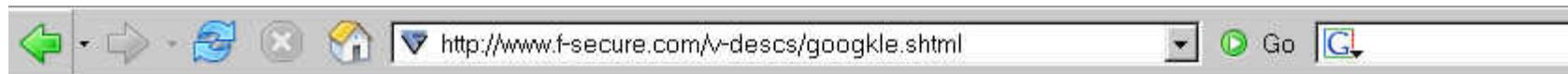
[Wells Fargo Mortgage Comparison](#)
Complete online comparison of national lenders, including **Wells Fargo**. Free online...
www.allpurposemortgage.com

[Wells Fargo Mortgages - Info and Quotes](#)
Find out more about **Wells Fargo** home loans and get up to four free

"Oopsie" Search Engines and Your Institution

- 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, eavesdropping 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 : Googkle

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

NAME: **Googkle**

ALIAS: Googkle.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]
[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>elp O>ptions P>rint G>o M>ain screen Q>uit /=search [d]elete=history list
```

Here's The Mainstream Version... The Cert For This Version Looks Fine...

The screenshot shows a web browser window with the following details:

- Address Bar:** https://www.elibertybankonline.com/engine/login/login.asp
- Toolbar:** Google, Search Web, PageRank, 4 blocked, AutoFill, Options
- Navigation:** Norton AntiVirus
- LibertyBank Logo:** More to your liking.
- Menu Bar:** HOME | ONLINE BANKING | CHECKING, SAVINGS & RETIREMENT | LOANS
BUSINESS BANKING | OFFICE & ATM LOCATIONS | ABOUT US | CONTACT US | PRIVACY
- Login Section:** Includes links for APPLY NOW, COMMERCIAL SIGN IN, LibertyBillPay FAQ, and a DEMO button.
- Billing Section:** You can now pay your bills online with LibertyBillPay.
- LibertyOnline Features:** Access accounts and transaction history online, transfer funds between accounts, customize account descriptions, place stop payments on checks.
- Certificate Dialog Box:** A modal window titled "Certificate" with tabs for General, Details, and Certification Path. It displays the following information:
 - Certificate Information:** This certificate is intended for the following purpose(s): Ensures the identity of a remote computer.
 - Issued to:** www.elibertybankonline.com
 - Issued by:** www.verisign.com/CPS Incorp. by Ref. LIABILITY LTD. (c)97 VeriSign
 - Valid from:** 1/17/2005 to 2/12/2006
- Buttons:** Install Certificate..., Issuer Statement, 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/cachepoisoning.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 your domain’s registration itself (ala panix.com’s 1/16/2005 incident,
http://news.com.com/2100-1025_3-5538227.html)

Financial Cryptography: DNS spoofing - spoke too soon? - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Back Forward Stop Home Address bar: http://www.financialcryptography.com/mt/archives/000208.html Go G

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. Your Web Site And User 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 you 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?
- You're not doing your customers any favors in the long run if you enable them to engage in risky behaviors – be a force for positive change by requiring them to use a current browser if they want to do online banking.

Design Your Website So That It 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 systems.
- Responsible web sites can use virtually any feature in a responsible way, and those features may improve your customers experience – on your web site.
- However, if you require customers to configure their browsers to permit risky actions, other malicious web sites may take advantage of those now-default risky configurations to harm your customer (users will NOT bother to change settings back and forth depending on whether they're using your web site or some other random/risky web site).

For Example: Scripting, and Cookies

- Does your website require customers to use Javascript or other scripting technology to use your site? If so, please understand that doing so substantially increases your customers' overall exposure to a host of web-related vulnerabilities (see 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's disabled.
- Cookies are used by some sites to track customers, often for advertising-related purposes. Does your site require customers to accept cookies? Why? Are they really needed if you have an SSL-secured connection established? If you do use cookies, do you clean them up at the end of the session? Again, help your users protect themselves by not mandating use of cookies.

Key - Technical - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

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

 PERSONAL
SMALL BUSINESS
CORPORATE
ABOUT KEY
ONLINE BANKING

Online Banking and Investing
FAQs
► Technical
 128-bit encryption
Service Comparison
Helpful Resources
Personal Financial Managers



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

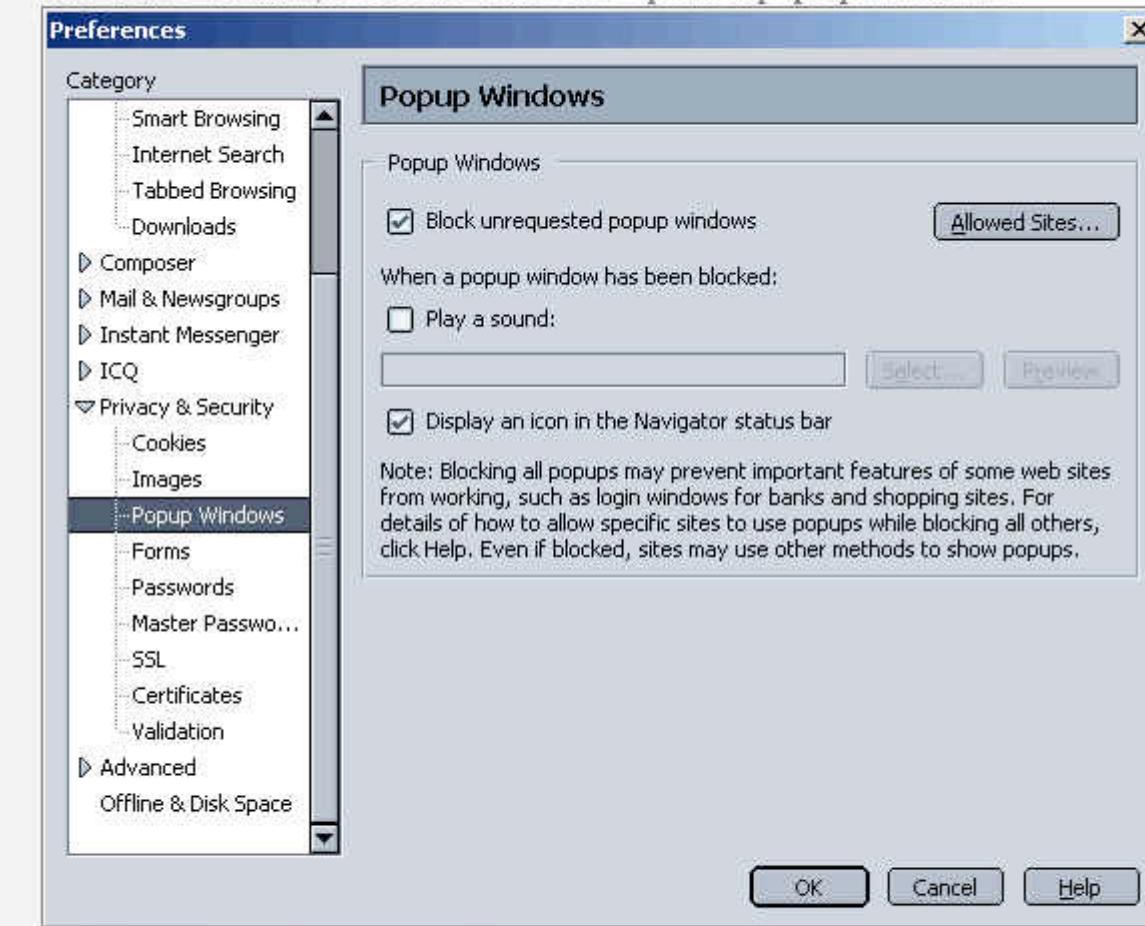
Cache Settings Requirements

Your Website And Popups...

- Does your site require users to permit popup windows?
- Remember that Windows XP SP2 now routinely blocks popup Windows. Should you be using that sort of feature on your bank's web site?
- 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 for your site as a persistent cookie on their system? Don't!
- Is browser form auto-completion *automatically* saving sensitive user account information and passwords?

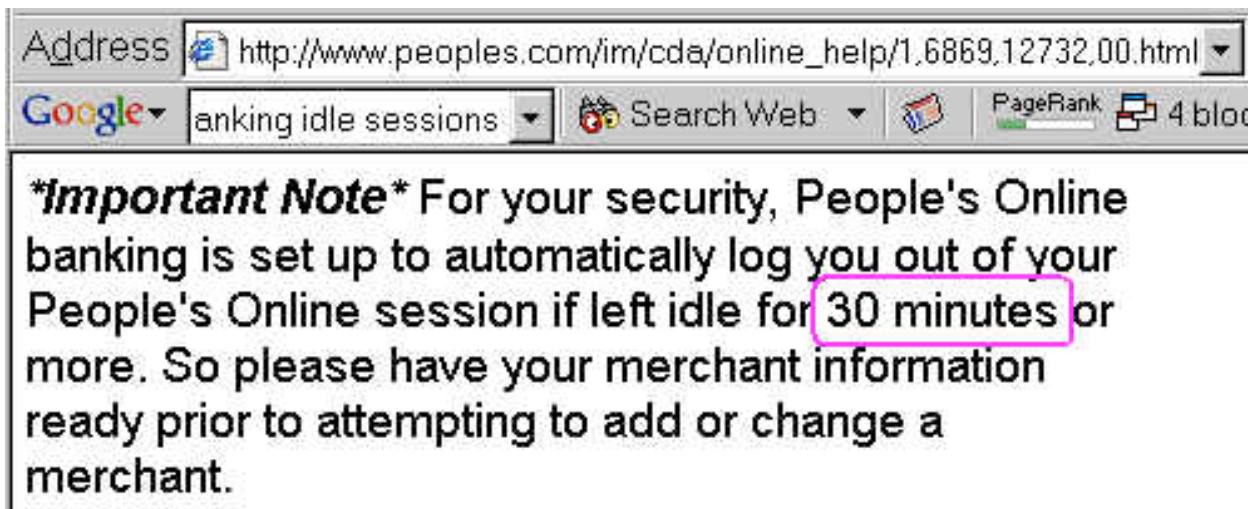
Autocompletion Symptomology

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** Troubleshooter for Online Banking - Weyerhaeuser Employees' Credit Union - Mozilla Fire
- Menu Bar:** File Edit View Go Bookmarks Tools Help
- Toolbar:** Back Forward Stop Home Address Bar (https://www.wecu.org/24hour/obtroubleshooter.asp#algorithm)
- Content Area:**
 - Section Header:** When signing on to Online Banking, your password is automatically entered in the password field
 - Text:** You are probably using Internet Explorer as your browser. It comes with a feature called AutoComplete which, when enabled, automatically completes form and password fields for you.
 - Text:** If you do not wish IE to complete this field for you, you must change the setting in your browser:
 - In IE, go to Tools and choose "Internet Options..."
 - Choose the Content tab
 - In the lower third of the screen click the AutoComplete button
 - In the "Use AutoComplete for" section, uncheck the "Forms" and "User names and passwords on forms" choices
 - Then click the "Clear Passwords" button in the Clear AutoComplete History section of that page
 - Click "OK" twice to close those dialogue boxes
 - Text:** You may need to exit and re-open IE to make sure the settings take place.

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 and the followup day's piece, "The Antiphishing Toolbars That Didn't,"
http://loosewire.typepad.com/blog/2005/04/the_antiphishin.html
- Most 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 you allow access to your customer online banking web site from anywhere in the world, you may want to reconsider that given the fact that the vast majority of your 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; you 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

Back Forward Stop Home http://www.cartserver.com/american/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.

You Need To Be Monitoring Your Web Server for Phishing That Use Your Own Web Site's Images, Logos, Etc.

- Scam artists love to use graphics directly from your 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.
- You, obviously, want 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 you're no longer using, consider "helping" them by making creative adjustments to those images being used without your permission.
- At a minimum, watch your server's logs!

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

- Are you letting your customers help you keep watch on their accounts? Do you routinely tell THEM the last place(s) where “they” accessed their online banking account? You 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 Your Users

Help Customers To Use The Financial Statements You Provide

- Many customers likely never look at the financial statements you 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: prioritize and highlight the important parts of what you tell your users. Odd transactions, relative to their norm? Highlight them so they stand out and can receive extra scrutiny by your customer.

You Really Need To Be Communicating With Your Customers; For Some Reason They May Not Trust Stuff Emailed to Them :-)

- Do your customers know what to do (and what NOT to do) if they receive phishing email? As a matter of due diligence/CYA, have you officially notified your customers about the phishing problem and what they should do if they receive phishing email?
- Does your web site 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.

Make Sure Your Users CAN Communicate With You!

- Users want to tell you about phishing that's going on -- be sure you're open to those reports!
- Does mail sent to:
 - abuse@<your domain>
 - postmaster@<your domain>
 - your domain whois points of contact
 - your network address range 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	chase.com	Listed	Jun 11, 2004 19:35 EDT	Jun 12, 2004 4:13 EDT	Never	Never
postmaster	chase.com	Listed	May 6, 2003 16:40 EDT	May 7, 2003 5:05 EDT	Never	Never

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

Make Sure Your Users Know How To Share Phishing Samples With Full Headers

- Potential scenario: 20,000 (or 200,000!) customers calling you to tell you that they've -- <gasp!> -- received a message that is claiming to be from your 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 you don't launch an immediate nuclear strike on the unidentifiably spamming phisher]
- 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. What's Next?

1. You 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

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

OPEN AN ACCOUNT

3.

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 seconds².
- SmartAlerts - configure to inform you of your account activity.
- Security specialists monitor your account for unusual activity.

Exclusive, Free,¹ Easy & Optional for E*TRADE Customers

Trading User ID: Password:

Investing Start In: User ID or Password?

Banking Get higher yields on CDs Markets Secured by RSA

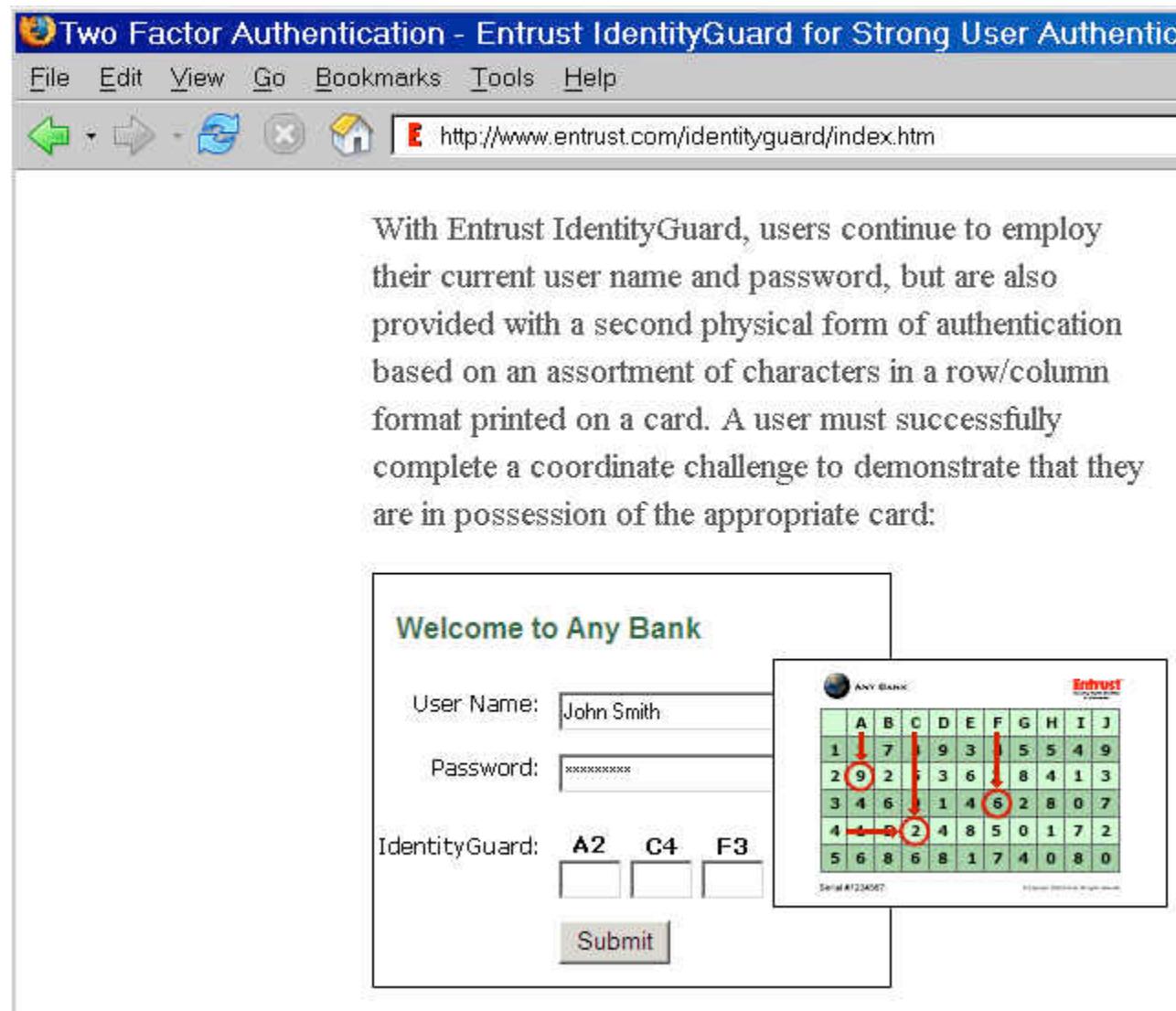
1 The Digital Security ID will be provided at no cost to Power E*TRADE and Priority E*TRADE customers. A \$25 charge may be imposed for each additional or replacement Digital Security ID. E*TRADE FINANCIAL at its sole discretion may impose a fee for this service in the future or may discontinue the service.

2 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

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

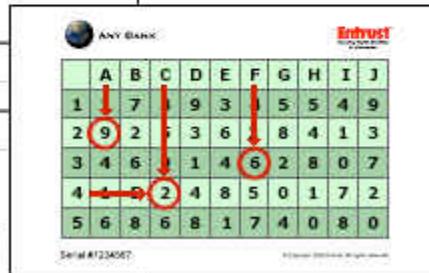
With Entrust IdentityGuard, users continue to employ their current user name and password, but are also provided with a second physical form of authentication based on an assortment of characters in a row/column format printed on a card. A user must successfully complete a coordinate challenge to demonstrate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

Welcome to Any Bank

User Name: John Smith

Password:

IdentityGuard: A2 C4 F3


ANY BANK
Entrust
Serial #1234567
© 2004 Entrust. All rights reserved.

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

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 window with the following details:

- Title Bar:** Techworld.com - Phishers migrating to Trojan attacks - Mozilla Firefox
- Menu Bar:** File Edit View Go Bookmarks Tools Help
- Toolbar:** Back Forward Stop Home Address Bar: http://www.techworld.com/news/index.cfm?newsID=2884
- Date:** 06 January 2005
- Section Headline:** Phishers migrating to Trojan attacks
- Sub-headline:** You can't escape phishers: they know where you surf
- Byline:** By John E. Dunn, Techworld
- Text:** The latest [report](#) from the Anti-Phishing Working Group (APWG) has suggested a depressing if unsurprising outlook for phishing trends in 2005.
- Text:** 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.
- Text:** 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.
- Text:** 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.
- Text:** Keylogging Trojans are likely to be a defining characteristic of phishing over the next 12 months.
- Text:** "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.
- Text:** "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

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?

**If We Have Time:
Looking At The Crumbs
Associated With A Sample eBay Phish**

Most of What We've Talked About Until Now Has Been "Defensive Ball"

- The first part of this talk was all about trying to defend against phishing.
- What if you wanted to actually see if you could go after a phisher, that is, what if you wanted to "go on the offense" for a change, looking purely at what's available from open sources?

Ripping Apart A Sample Phish

- This example is a real eBay phish, received on Saturday night, April 23rd, 2005, and forwarded to us by the recipient on Sunday morning. The reporting user, like most of our users, has been trained to supply spam samples complete with FULL HEADERS as described at <http://micro.uoregon.edu/fullheaders/>
- Unfortunately the vast majority of spam samples reported by casual email users, whether to ISPs or to government agencies, lack expanded headers (a fact which delights typical spammers, obviously).
- Make sure YOUR customers know how to enable full headers!

Headers From The Sample eBay Phish

```
>Return-Path: <wwwrun@golf.webmind.de>
>Received: from golf.webmind.de <[145.253.231.17]>
>          by darkwing.uoregon.edu <8.13.4/8.13.4> with ESMTP id j302SKxa011425
>          for <[redacted]@darkwing.uoregon.edu>; Sat, 23 Apr 2005 19:28:20 -0700 (PDT)
>Received: by golf.webmind.de (Postfix, from userid 30)
>          id 799FDE557C; Sun, 24 Apr 2005 04:29:17 +0200 (CEST)
>To: [redacted]@darkwing.uoregon.edu
>Subject: Your Account Will Be Suspended
>From: eBay Billing Department <Billing@eBay.com>
>Reply-To: update@eBay.com
>MIME-Version: 1.0
>Content-Type: text/html
>Content-Transfer-Encoding: 8bit
>Message-Id: <20050424022917.799FDE557C@golf.webmind.de>
>Date: Sun, 24 Apr 2005 04:29:17 +0200 (CEST)
>Status:
>
>Hello! <http://signin.ebay.com/ws2/eBayISAPI.dll?SignIn>Sign=20
>in/out<http://pages.ebay.com/ebay_IBM.html>.
>
>Dear eBay valued member,
```

Let's start with stuff from the full header, specifically the IP address that handed us the message. (After we get done poking at that, then we'll come back to the rather interesting Reply-To: address.) The whois command is the tool we'll use to see what's known about the IP.

Some Background on whois

- The whois command tells you "who is responsible" for a given network resource, such as a domain name, an IP address, an autonomous system number, etc.
- The easiest way to do whois queries is probably by using a command line whois client on a Unix host (now that Mac Mini's are available at under \$500, there's really no reason not to have a Unix box for use in hunting phishers!)
- Nonetheless, if you are forced to work in a web-only world, you can still do whois queries via services such as <http://www.completeswhois.com/>

The Phish Was Received From 145.253.231.17

```
% whois 145.253.231.17
[ querying whois.ripe.net for 145.253.231.17 ]
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

inetnum:      145.253.231.0 - 145.253.231.255
netname:      SIRCON-NET
descr:        Sirconic Group GmbH
descr:        Breslauer Str. 49
descr:        D-83395 Freilassing
descr:        Germany
country:      DE
admin-c:      SD2300-RIPE
tech-c:       ANOC1-RIPE
status:       ASSIGNED PA
mnt-by:       ARCOR-MNT
notify:       ip-registry@arcor.net
changed:      ip-registry@arcor.net 20040929
source:       RIPE

person:        Sezgin Demircan
address:      Breslauer Str. 49
address:      D-83395 Freilassing
address:      Germany
e-mail:        sd@sirconic-group.de
phone:        +49 8654 7788510
fax-no:        +49 8654 7788511
mnt-by:       ARCOR-MNT
notify:       ip-registry@arcor.net
nic-hdl:      SD2300-RIPE
changed:      ip-registry@arcor.net 20040929
source:       RIPE
```

What Does Whois say about sirconic-group.de?

```
* whois sirconic-group.de
[ querying whois.denic.de for sirconic-group.de ]
domain:      sirconic-group.de
status:      connect
```

- Dot de (German) domain registrations have taken privacy concerns to an absurd length, with the result that little if anything of use is shown for many .de domain names (unlike IP whois records, as shown on the preceding page).
- In this case, if we wanted to (e.g., to try to get this phishing site torn down), we could also look at the web site for the domain for contact information.
- We'll stay with the dotted quad (e.g., the IP address).

145.253.231.17 Isn't Blocklisted

The screenshot shows a Mozilla Firefox browser window with the title "Openrbl: Multi DNSBL Lookup 145.253.231.17 145.253.231.17 - Mozilla Firefox". The address bar displays the URL <http://www.openrbl.org/ip/145/253/231/17.htm>. The main content area is titled "Multi DNSBL Lookup" and contains the following information:

Lookup 145.253.231.17 (golf.webmind.de) in 20+8 Zones

AS: [145.253.0.0/16](#) AS3209 Arcor IP-Network UNKNOWN
Net [145.253-145.254](#) ARCOR-IP @adm.arcor.net

Results: Negative=28, Positive=0 (2005-04-24 16:00:27 UTC)

• Negative 28: @COUNTRY @DYNAMIC @ISP @SPAM AHBL AUDNSBL BOGONS BOPM CBL DRBL DSBL FIVETEN INTERSIL JIPPGMA LNSG NJABL NOMORE ORDB PSBL SBL SORBS SPAMBAG SPAMCOP SPAMRBL SPAMBSITE SPEWS UCEPROT WPBL

Hints for **145.253.231.17**: ([external](#) use BACK or ALT-LEFT when done)

- Track "golf.webmind.de" at [[Whois & Abuse](#)|[SpamCop*](#)]
- Search "145.253.231.17" at [[Google](#)][SpamCop*](#)[[SenderBase](#)] [[MAPS](#)][Schlund](#)
- **CHECK:** Nominate Relay-Test at: [[ORDB](#)] [[Add Comment](#)]

145.253.231.17 Has No Senderbase History

SenderBase - 145.253.231.17 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Home Domains IP's

http://www.senderbase.org/search?searchString=145.253.231.17

Report on IP address: **145.253.231.17**

Volume Statistics for this IP

	Magnitude	Vol Change vs. Average
Last day	0.0	-100%
Last 30 days	0.0	-100%
Average	0.0	

Third-party Certification

Bonded Sender?	Not Bonded
TRUSTe Privacy Seal?	Not Certified

Information from whois [Click to show details]

Network Owner:	RIPE Network Coordination Centre
Registered on:	1993-05-01
Updated on:	1993-05-01
Expires on:	unknown

Other information about this IP address

Sender Category	unknown
Network Owner	unknown
Domain	unknown
Date of first message seen from this address	
CIDR range	unknown
# of domains controlled by this network owner	0
Geography data	
Country	unknown
State	unknown
City	unknown
Postal code	unknown

Related links

Google groups	http://groups.google.com/groups?scoring=d&q=145.253.231.17+group:*abuse*
OpenRBL	http://openrbl.org/dnsbl?i=145.253.231.17
SpamCop	http://spamcop.net/w3m?action=checkblock&ip=145.253.231.17

Real-time blacklists [Click to view all]

not in any blacklists

No address list shown since no email was detected from 145.253.231.0/24.

Conclusion About This IP...

- 145.253.231.17 is likely a newly hijacked IP address at a compromised host, perhaps running a vulnerable web cgi-bin application of one sort or another (note the "wwrrun" Return-path in the phish, a username commonly associated with cgi-bin execution environments)

What About That Odd Reply-To Address?

[querying whois.wildwestdomains.com for eba-y.com]

Registrant:

Non
2341 21st. st. Apt. C.
San pablo, California 94806
United States

Registered through: GO PAPPY

Domain Name: EBA-Y.COM

Created on: 01-Apr-04
Expires on: 01-Apr-06
Last Updated on: 06-Apr-05

Administrative Contact:

Miranda, Carlos mugamil@webtv.net
Non
2341 21st. st. Apt. C.
San pablo, California 94806
United States
(888) 491-2133

Technical Contact:

Miranda, Carlos mugamil@webtv.net
Non
2341 21st. st. Apt. C.
San pablo, California 94806
United States
(888) 491-2133

Domain servers in listed order:

NS1.AFTERNIC.COM
NS2.AFTERNIC.COM

A Note On Email Addresses in Spam/Phishing Headers -- Real or Possibly Just "Joe Jobs"

- An email address seen in a mail message header may be one really controlled by the person sending the mail, or it may be a spoofed address (an address that has no connection to the spam/phishing message whatsoever).
- Why would a spammer potentially use a real address? A real address might be getting used to collect messages that bounce, or to handle communications with victims who try to reply to the phishing message (rather than visiting the phishvertised web form)
- A spoofed address might ALSO be used to misdirect the curious, or in an attempt to implicate a competitor or to punish an innocent party (such as an antispammer)
- Let's see if our conclusions are helped by "vetting" the whois data we just saw...

Is The Street Address Used for The Domain Whois Superficially Valid? Yes...

The screenshot shows a web browser window with the following details:

- Header:** UNITED STATES POSTAL SERVICE logo and the URL <http://www.usps.gov/zip4/>.
- Title:** ZIP Code Lookup
- Section:** ZIP + 4® Code Lookup Results
- Text:** Below is the correct ZIP + 4 Code from the address information that you provided.
- Address Input:** Address (Standard Format) [What is This?](#)
2341 21ST ST APT C
SAN PABLO CA 94806-3559
- Buttons:** [Mailing Industry Information](#) [What is This?](#) [Lookup another ZIP Code >](#)

Do We See the 1-888 Number Used In That Domain Registration Show Up Anywhere? Yes

The screenshot shows a Google search results page with the following details:

- Search Query:** 888-491-2133
- Results:** 1 - 10 of about 260 for 888-491-2133.
- Web Results:**
 - Nantucket Online.com - Classifieds**
... Madeleine Madelia • **888-491-2133** • Wilam, United States ... Van Morrison •
888-491-2133 • Wilam, NL, United States • spankaj82@yahoo.com ...
nantucketonline.com/classifieds/classifieds.php?classifieds_category_id=3 - 24k - [Cached](#) - [Similar pages](#)
 - WhoWon.com ... The Internet Source for Motorsports News and ...**
... Home Phone: **888-491-2133** Bus. Phone: **888-491-2133** Email:
paragchandrakanthmahajan@yahoo.com ... Home Phone: 1-**888-491-2133** Bus. Phone:
1-888-491-2133 ...
www.whowon.com/showclass50.asp?cat=15-50k - [Cached](#) - [Similar pages](#)
 - Sports collectible**
... 3.20.2005 Carlos Miranda (Alaska, Business) **888-491-2133** Visit website Send
... 4.5.2005 Van Morrison (Alabama, Business) **888-491-2133** Send e-mail E-mail ...
www.domesticsale.com/Classifieds/search/sports-collectible/ - 31k - [Cached](#) - [Similar pages](#)
 - Dialysis Employment**
... Phone: **888-491-2133**. Tuesday, April 12, 2005, Wilam, Act now have some fun
and make real money from now on. A life time opportunity to promote the dream ...
www.globaldialysis.com/Jobs.asp?t=9&Page=9 - 45k - [Cached](#) - [Similar pages](#)
 - Indonesia Interactive >> HOME**
... For more information you can call **888-491-2133**, or visit <http://sportsbookusa.us>.
Give a respond Modify Delete. posted by gautam at 4/13/05 2:40:38 PM ...
www.i2.co.id/mall/ad_list_new.asp?new=1 - 41k - [Cached](#) - [Similar pages](#)
 - kzn.co.za Classifieds: for sale, wanted, swap - General ...**
... Contact: Madeleine Madelia, Phone: **888-491-2133**, Price: \$18.5, Email:
krishnashankar77@yahoo.com. Town: Wilam, Province: Mpumalanga ...
www.kzn.co.za/business/classifieds.asp?page=5&classType=classifieds - 41k - [Cached](#) - [Similar pages](#)
- Toolbar:** Find, Find Next, Find Previous, Highlight, Match case
- Page Number:** 26

Can We Use Our Original Phone Number to Find Additional Ones? Yes

Nantucket Online.com - Classifieds - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Used farm tractors Wednesday April 20th 2005
06:18:33

Over 100 tractors in stock. Used and new tractors. A wide variety of quality and prices for all.

• Mahalia Mahari • 315-465-6492 • Loas, United States • paragchandra79@yahoo.com

The Instant Publisher Platinum CDROM Wednesday April 20th 2005
06:18:15

A fabulous collection of 750 Books, Reports & Manuals You Can Reprint & Sell and Make a Fortune! How to Write a Job Winning Resume, How to Sell Books ByMail, How to Write Profitable Classified Ads and many more!

• Mahari Mahari • 561-582-1874 • Hypoluxo, FL, United States • ganeshshivshan79@yahoo.com

Monday April 18th 2005 22:53:07

Increase your business productivity with our consulting services which includes Executive Coaching, Sales Training, and organizational analysis

• Maitland Maj • 317-290-6744 • Carmel, ID, United States • pankajosh79@yahoo.com

the free sports book Monday April 18th 2005 22:52:04

Act now have some fun and make real money from now on. An exciting product to make real money.

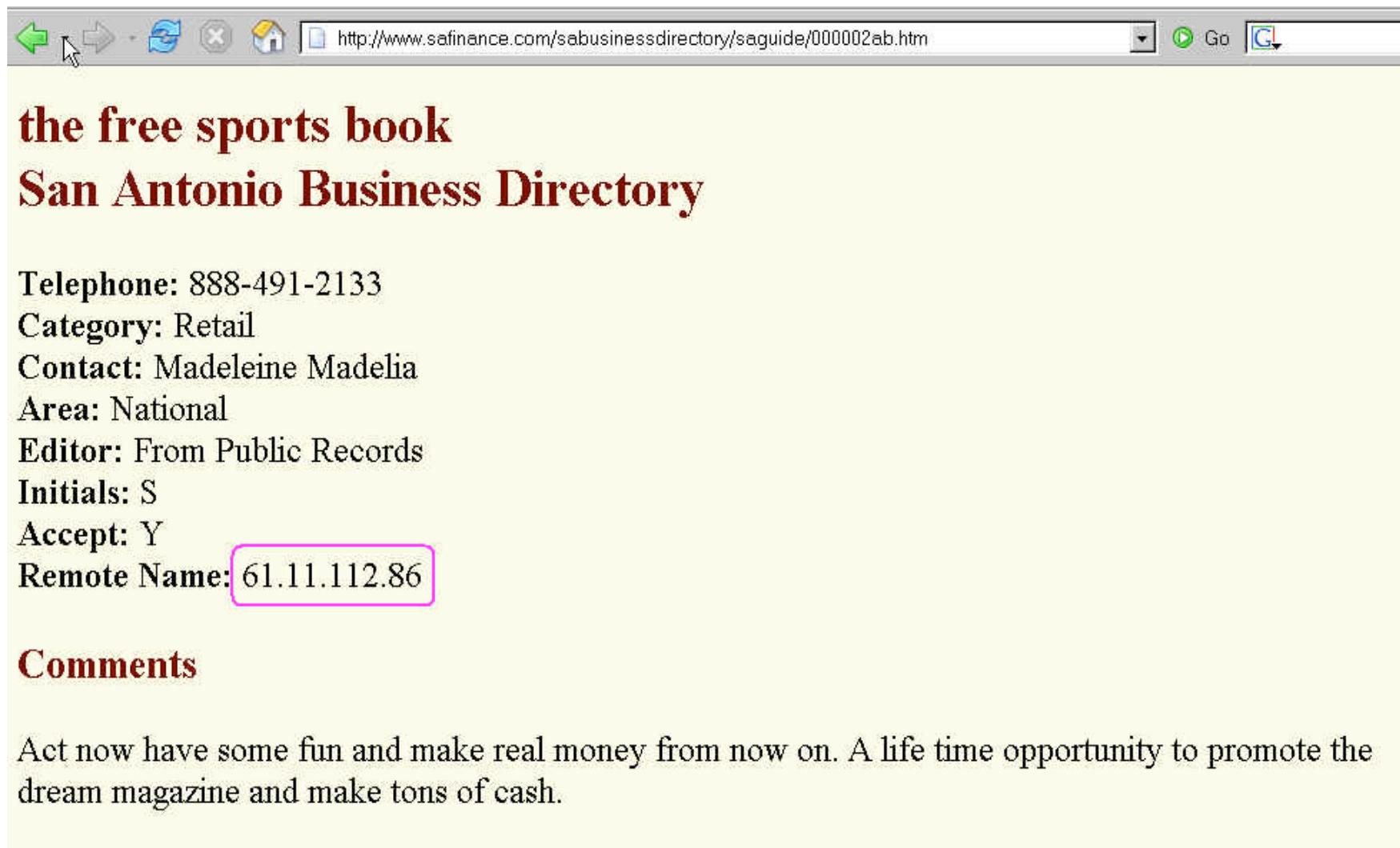
• Maitland Maj • 888-491-2133 • Wilam, United States • anilbalakar76@yahoo.com

the free sports book Monday April 18th 2005 06:43:34

Act now have some fun and make real money from now on. An exciting product to make real money.

• Maitland Maj • 888-491-2133 • Wilam, United States • anilbalakar76@yahoo.com

Some Free Classified Add Sites Record Where Postings Apparently Come From...



The screenshot shows a web browser window with the URL <http://www.safinance.com/sabusinessdirectory/saguide/000002ab.htm> in the address bar. The page content is as follows:

the free sports book
San Antonio Business Directory

Telephone: 888-491-2133
Category: Retail
Contact: Madeleine Madelia
Area: National
Editor: From Public Records
Initials: S
Accept: Y
Remote Name: 61.11.112.86

Comments

Act now have some fun and make real money from now on. A life time opportunity to promote the dream magazine and make tons of cash.

That's A Bombay, India Address

```
% whois 61.11.112.86
[ querying whois.apnic.net for 61.11.112.86 ]
% [whois.apnic.net node-1]
% Whois data copyright terms      http://www.apnic.net/db/dbcopyright.html

inetnum:      61.11.32.0 - 61.11.127.255
netname:      USNL-IN
descr:        Videsh Sanchar Nigam Ltd - India.
descr:        Videsh Sanchar Bhawan, M.G. Road
descr:        Fort, Bombay 400001
country:      IN
admin-c:      IA15-AP
tech-c:       VT43-AP
remarks:      -----
remarks:      This object can only be modified by APNIC hostmaster
remarks:      If you wish to modify this object details please
remarks:      send email to hostmaster@apnic.net with your organisation
remarks:      account name in the subject line.
remarks:      -----
mnt-by:       APNIC-HM
mnt-lower:    MAINT-USNL-AP
mnt-routes:   MAINT-USNL-AP
changed:      hostmaster@apnic.net 20010227
status:       ALLOCATED PORTABLE
changed:      hm-changed@apnic.net 20040930
source:       APNIC
```

Here's Another One from 61.11...

The screenshot shows a web browser window with the URL <http://www.safinance.com/sabusinessdirectory/saguide/000002af.htm>. The page content is as follows:

sports book for free
San Antonio Business Directory

Telephone: 888-491-2133
Category: Service
Contact: Maitland Maj
Area: I-35 Corridor
Editor: From Public Records
Initials: \$.18.5
Accept: Y
Remote Name: 61.11.23.240

Comments

Act now have some fun and make real money from now on. If you are a sports lover, make money by reaching out to other sport lovers.

But Those Posting May Not Have Really Originated From Someone In India: Proxies!

Openrbl: Multi DNSBL Lookup 61.11.23.240 61.11.23.240 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

open RBL http://www.openrbl.org/ip/61/11/23/240.htm

Openrbl DNSBL Whois Route Multi DNSBL Lookup

IP or Hostname: 61.11.23.240 Submit Singlepage

Lookup 61.11.23.240 (static23-240.dsl-pun.eth.net) in 20+8 Zones
AS: 61.11.16.0/21 AS10199 DishnetDSL Limited UNKNOWN
Net 61.11.0-31 DISHNET Pune, Maharashtra @eth.net
Results: Positive=5, Negative=23 (2005-04-24 19:05:24 UTC)

- [@DYNAMIC/dialup](#): 61.11.23/24: 553 ADSL/CABLE/DIALUP ADSL India DISHNET; SORBS DUL
- [AUDNSBL/dnsbl.net.au](#): 61.11.23/24: 553 AUDNSBL Multiple Spam Traps Block List [\[Remove\]](#)
- [CBL/abuseat.org](#): 553 CBL Proxy/Trojan [\[Remove\]](#)
- [SORBS/sorbs.net](#): 61.11.23/24: 553 SORBS DUL [\[Remove\]](#)
- [FIVETEN/61.11.8.157.misc.spam](#): miscellaneous address blocks that have sent spam here
- **Negative 23:** @COUNTRY @ISP @SPAM AHBL BOGONS BOPM DRBL DSBL INTERSIL JIPPGMA LNSG SPAMBAG SPAMCOP SPAMRBL SPAMSITE SPEWS UCEPROT WPBL

Hints for 61.11.23.240: ([external](#)) use BACK or ALT-LEFT when done)

- Track "static23-240.dsl-pun.eth.net" at [[Whois & Abuse|SpamCop*](#)]
- Search "61.11.23.240" at [[Google|SpamCop*](#)|[SenderBase](#)] [[MAPS|Schlund](#)]
- **CHECK:** Nominate Relay-Test at: [[ORDB](#)] [[Add Comment](#)]

An Aside: If You're Interested in Open Proxies or Spam Zombies, You May Want to See...

- "The Open Proxy Problem: Should I Worry About Half a Million Trivially Exploitable Hosts?"
[http://darkwing.uoregon.edu/~joe/jt-proxies/
open-proxy-joint-techs.ppt](http://darkwing.uoregon.edu/~joe/jt-proxies/open-proxy-joint-techs.ppt) (or .pdf)
- "Spam Zombies And Inbound Flows to Compromised Customer Systems,"
<http://darkwing.uoregon.edu/~joe/zombies.pdf>

Nutshell Summary for Accounts Associated with 888-491-2133

- That phone number is seen in conjunction with a wide variety of free/throw-away email accounts (often with stereotypical central asian-related names). At least some of the names used in conjunction with those accounts appear to be names of famous celebrities.

Maitland Maj anilbalakar76@yahoo.com

Margot Morrison pradeepbala74@yahoo.com

Madeleine Madelia krishnashankar77@yahoo.com

Van Morrison spankaj82@yahoo.com

Keanu Reeves paragchandrakanthmahajan@yahoo.com

David Bradshaw sowmyakrish82@yahoo.com

Maitland Maj chandrakantmahajan78@yahoo.co.in

Sam Dek paragsphade@yahoo.com

RekhaRekha rekhasanjaypatil74@rediffmail.com

Guyton Wanda DocNoah7@aol.com

raghu hms_raghavendra@yahoo.co.in

Rosalba Rosalia hms_1204ar8@yahoo.co.in

Aminah Amine iliashuss70@yahoo.com

Any Additional Data?

- 888-491-2133 was also seen in conjunction with sportsbookusa.us, a (domain registered to Carlos Miranda, 234 21st (apparently a typo) and/or 2341 21st. st. Apt. C., San Pablo, California, mugamil@yahoo.com (instead of mugamil@webtv.net) -- look familiar to what you saw for the eba-y.com whois? :-;
- Sportsbookusa.us and eba-y.com both live on 216.168.41.230 (that IP is part of a block allocated to digital.forest, Inc., 19515 North Creek Parkway, Suite 208, Bothell WA, 98011), and routed by AS11739 (digital.forest, Inc.).
- Someone interested in eba-y.com (like ebay.com, for example) would probably next go after the identity of the customer hosting those two domains at digital.forest using suitable legal paperwork.

Enough With The Headers, What Can We See In The Body of The Message?

- So far, remember that we've just been looking at the message headers.
- What can we see if we actually proceed down into the text of the body of the message? Quite a bit, actually, since our user submitted the actual raw text of the message the user received, rather than some HTML-rendered representation...

Raw Body of the Phishing Message...

#299 24-APR-2005 05:45:55.42 NEWMAIL
>Hello! <<http://signin.ebay.com/ws2/eBayISAPI.dll?SignIn>>Sign=20
>in/out<http://pages.ebay.com/ebay_IBM.html>.
>
>Dear eBay valued member,
>
>During our regularly scheduled account maintenance and verification=20
>procedures, we have detected an error in your billing information.
>
>This might be due to either of the following reasons:
>
>1. A recent change in your personal information (i.e. change of address).
>2. Submitting invalid information during the initial sign up process.
>3. An inability to accurately verify your selected option of payment due=20
>to an internal error within our processors.
>To avoid account suspension you must go to the link below and provide=20
>required informations:
><<http://ebaserv-cgi-update-account.com/>><http://cgi1.ebay.com/aw-cgi/eBayISAPI.php?MfcISAPICommand=3DSignInFPP=20>

Press RETURN for more...

- Obviously, <http://ebaserv-cgi-update-account.com/> is the phishvertised link that we'll want to pursue – it is a classic example of a underlying-link-not-agreeing-with-what-user-normally-sees-for-link-text vector.

Hmm... That Domain "Doesn't Exist..."

```
% date
Sun Apr 24 07:49:21 PDT 2005
% whois ebaserv-cgi-update-account.com
[ querying whois.internic.net for ebaserv-cgi-update-account.com ]

Whois Server Version 1.3

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

No match for "EBASERV-CGI-UPDATE-ACCOUNT.COM".

>>> Last update of whois database: Sat, 23 Apr 2005 19:11:12 EDT <<<
```

- One of the phishers favorite new phishing tricks is to register a new domain name and then IMMEDIATELY begin using it, "making hay while the sun shines" prior to the time the domain shows up in the whois database. (Once the domain shows up in whois, the likelihood that trademark infringing names will be noticed and potentially contested increases dramatically.)

But It Does Exist, and It Resolves Just Fine

```
% nslookup
> ebaseru-cgi-update-account.com
Server:      128.223.32.35
Address:     128.223.32.35#53

Non-authoritative answer:
Name:  ebaseru-cgi-update-account.com
Address: 65.54.132.254
> 65.54.132.254
Server:      128.223.32.35
Address:     128.223.32.35#53

Non-authoritative answer:
254.132.54.65.in-addr.arpa      name = yourpersonaladdress.net.

Authoritative answers can be found from:
54.65.in-addr.arpa      nameserver = NS1.MSFT.net.
54.65.in-addr.arpa      nameserver = NS2.MSFT.net.
54.65.in-addr.arpa      nameserver = NS3.MSFT.net.
54.65.in-addr.arpa      nameserver = NS4.MSFT.net.
54.65.in-addr.arpa      nameserver = NS5.MSFT.net.
NS1.MSFT.net      internet address = 207.46.245.230
NS2.MSFT.net      internet address = 64.4.25.30
NS3.MSFT.net      internet address = 213.199.144.151
```

We Can Also Use Curl To Visit That Site

```
% curl "http://ebaserv-cgi-update-account.com/" > temp.txt
% Total    % Received % Xferd  Average Speed   Time          Curr.
%          Dload  Upload Total   Current  Left   Speed
100  300     0  300     0      0  2941      0 --:--:-- 0:00:00 --:--:-- 82000
% more temp.txt
HTTP/1.1 302 Found
Connection: close
Date: Sun, 24 Apr 2005 15:06:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IUDo ONL OUR PHY SAMo TELo"
X-AspNet-Version: 1.1.4322
Location: http://www.bg124.de/php/%20%20/
Cache-Control: private
Expires: Sat, 01 Jan 2000 08:00:00 GMT
Content-Type: text/html

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href='http://www.bg124.de/php/%20%20/'>here</a>.</h2>
</body></html>
```

- Curl is a command line web page retrieval utility that's now a standard part of many Linux/Unix operating system builds. If you're using a system that doesn't have it, you can get a copy from <http://curl.haxx.se>
- You'll notice that curl lets you include http headers in the output (I have curl routinely aliased to curl -i)

Eventually, We Get To See The Domain Whois...

- The whois data for the phishvertised domain begins...

```
[ querying whois.enom.com for ebaseru-cgi-update-account.com ]  
  
Registration Service Provided By: Microsoft  
Contact: personal_address@css.one.microsoft.com  
Visit: http://support.msn.com/contactus.aspx?pk=PersonalAddress  
  
Domain name: ebaseru-cgi-update-account.com  
  
Registrant Contact:  
Barbara Reiter  
Barbara Reiter <tofey@ebaseru-cgi-update-account.com>  
+1.906283393452  
Fax: none  
P.O. Box 87  
Gulliver, MI 49840  
US  
  
Administrative Contact:  
Barbara Reiter  
Barbara Reiter <tofey@ebaseru-cgi-update-account.com>  
+1.906283393452  
Fax: none  
P.O. Box 87  
Gulliver, MI 49840  
US
```

- I would be exceedingly surprised if that information proves to be in any way shape or form "valid" and associated with the person truly controlling that domain. That page is just a redirector, anyhow...

Let's Look At The Real Site...

```
% curl "http://www.bg124.de/php/%20%20/" > temp2.txt
% Total    % Received % Xferd  Average Speed   Time          Curr.
%          Dload  Upload Total   Current  Left   Speed
100 11959  100 11959    0     0  16655      0  0:00:00  0:00:00  0:00:00 30055
% more temp2.txt
HTTP/1.1 200 OK
Date: Sun, 24 Apr 2005 15:11:57 GMT
Server: Apache/1.3.27 (Linux/SuSE) PHP/4.3.1 mod_ssl/2.8.12 OpenSSL/0.9.6i
Last-Modified: Sun, 24 Apr 2005 15:11:57 GMT
ETag: W/"5baab-2eb7-4da8a0f0"
Accept-Ranges: bytes
Content-Length: 11959
Content-Type: text/html

<html>
<head>
<!--eBay U3- msxml 4.0 XXXXXXXXXXXXXXXXXXXXXXXXX-->
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"><!--srcI
d: SignIn-->
<title>Sign In</title></head>
<body bgcolor="#ffffff">

<SCRIPT LANGUAGE="JavaScript">
  <!--
```



```
% whois www.bg124.de
[ querying whois.denic.de for www.bg124.de ]
domain:      www.bg124.de
status:      invalid
```

Rendered, The Phishvertised Page Looks Like:

Sign In - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.bqj24.de/php/%20%20/

eBay®

Sign In

New to eBay? or Already an eBay user?

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

Registration is fast and free.

Register >

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

eBay User ID

[Forgot your User ID?](#)

Password

[Forgot your password?](#)

Sign In Securely >

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

[Account protection tips](#)
Be sure the Web site address you see above starts with https://signin.ebay.com/

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

PASSPORT
Sign In .net

About eBay | Announcements | Security Center | Policies | Site Map | Help

Copyright © 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

[eBay official time](#)

reviewed by site privacy statement

Done Disabled

For Comparison, The Real eBay Sign In Page:

The screenshot shows a Mozilla Firefox browser window displaying the eBay sign-in page. The address bar at the top contains the URL <https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&ssPageName=h:h:sign:US>. The main content area is titled "Sign In" and features two sections: "New to eBay?" and "Already an eBay user?". The "Already an eBay user?" section includes fields for "eBay User ID" and "Password", both with "Forgot" links. It also features a "Sign In Securely >" button and a "Keep me signed in" checkbox. Below this is a note about account protection tips and a warning about the address bar. At the bottom, there are links for Microsoft Passport users, a footer with links like "About eBay", and a "TRUSTe site privacy statement" badge. The status bar at the bottom shows the URL "signin.ebay.com" and various browser status icons.

What Do We Know About www.bgl24.de ?

- www.bgl24.de (that's an ell, not a one, after the bg) turns out to resolve to 145.253.231.16.... Hmm, now doesn't THAT look familiar. Ah! That's because it is yet another host in the now-familiar 145.253.231.0/24 netblock.
- If you look at the URL to which you get redirected, it includes two hex-encoded spaces (%20's) as part of the path. That sort of trick is symptomatic of someone who's attempting to hide a directory from casual discovery rather than the sort of name that someone would normally use on a system they directly administered.
- The SIRCON-NET host not only sourced the phishing message, they're also hosting the phishvertised site. Dealing with that site now becomes more important... and in fact, after contacting German authorities, the site was torn down. Example endeth.

Miscellaneous Thoughts

1. Who Should I Contact About A Given Domain?



The screenshot shows a Mozilla Firefox browser window with the title bar "Look up an address in the abuse.net contact database - Mozilla Firefox". The menu bar includes File, Edit, View, Go, Bookmarks, Tools, and Help. The toolbar includes Back, Forward, Stop, Home, and Refresh buttons. The address bar shows the URL "http://www.abuse.net/lookup.phtml". Below the address bar is a toolbar with links to Firefox Help, Firefox Support, Plug-in FAQ, and RUS-CERT - Passive ...

NETWORK ABUSE CLEARINGHOUSE

Look up an address in the abuse.net contact database

Enter the name of the domain that you would like to check, such as `example.com`.

 [Look up another domain](#)
 [Return to the abuse.net home page.](#)

This page updated: 01/02/2004
© 1999-2001 I.E.C.C.

Are your domain's preferred reporting addresses on file?

2. I Know An IP, Are There Other Domains On That Same IP?

The screenshot shows a Mozilla Firefox browser window with the title bar "RUS-CERT - Passive DNS Replication - Mozilla Firefox". The address bar contains the URL "http://cert.uni-stuttgart.de/stats/dns-replication.php?query=145.253.231.16&submit=Query". The main content area displays the RUS-CERT logo and navigation menu. The left sidebar lists various services: Home, Aktuelle Meldungen, Betriebssysteme, Themen, Dienste (which is selected), Uni-Firewall, Verkehrsbeobachtung, Top 5, Mailinglisten, Passworttest, Angriff, Incident Response, Vulnerability Response, Projekte, Archive, and Jobs. The main content area includes a sub-navigation "Home > Dienste", the title "Passive DNS Replication", a descriptive text about the service, a note about bulk queries, a query input field containing "145.253.231.16", a "Query" button, and a table of results. The table lists domain names and their corresponding IP addresses.

Computer Emergency Response Team
DV-Sicherheit an der Universität Stuttgart

Kontakt Sitemap Impressum E-Mail-Abo Presse

Home > Dienste

Passive DNS Replication

RUS-CERT runs a DNS replication server as a service to the CERT community. By using this web page, you can query the replication database and obtain information that is not readily available through traditional DNS queries.

Do not run automatic queries against this database. If you want to submit bulk queries, please contact [the operators](#).

Query string:

The server returned the following data:

www.webmind.de	A 145.253.231.16
www.mappe.de	A 145.253.231.16
geigl.de	A 145.253.231.16
www.hotel-rosenbichi.de	A 145.253.231.16
prilhofer.de	A 145.253.231.16
www.lbt.de	A 145.253.231.16

The server status is **201 Okay**.

Passive DNS Replication Also Lets You See The Domains Using a Common Name Server (unrelated example)

The screenshot shows a Mozilla Firefox browser window with the title "RUS-CERT - Passive DNS Replication - Mozilla Firefox". The address bar displays the URL <http://cert.uni-stuttgart.de/stats/dns-replication.php?query=dog.ccpatoncejk.biz>. The left sidebar contains links for "Passworttest", "Angriff", "Incident Response", "Vulnerability Response", "Projekte", "Archive", and "Jobs", along with links for "Universität Stuttgart" and "Rechenzentrum der Universität Stuttgart". A search bar labeled "Suche in Meldungen" is present. The main content area has a "Query string: dog.ccpatoncejk.biz" input field with a "Query" button. Below it, a message says "The server returned the following data:" followed by a list of domain names and their NS records.

Domain	NS Record
burtonabdea.com	NS dog.ccpatoncejk.biz
anointefbha.com	NS dog.ccpatoncejk.biz
achotelcia.com	NS dog.ccpatoncejk.biz
disingledb.com	NS dog.ccpatoncejk.biz
guacofknhb.com	NS dog.ccpatoncejk.biz
gumiyndhib.com	NS dog.ccpatoncejk.biz
feputrefymb.com	NS dog.ccpatoncejk.biz
coder1bgfc.com	NS dog.ccpatoncejk.biz
stereeaafgc.com	NS dog.ccpatoncejk.biz
lygeumqjmic.com	NS dog.ccpatoncejk.biz
dutchibabd.com	NS dog.ccpatoncejk.biz
ambushlmdbd.com	NS dog.ccpatoncejk.biz
yunkghcd.com	NS dog.ccpatoncejk.biz
revertalimgd.com	NS dog.ccpatoncejk.biz
entitycdfjd.com	NS dog.ccpatoncejk.biz
ulemabid.com	NS dog.ccpatoncejk.biz
solveaiamd.com	NS dog.ccpatoncejk.biz
unbungkanbe.com	NS dog.ccpatoncejk.biz
editehkce.com	NS dog.ccpatoncejk.biz
visnengkge.com	NS dog.ccpatoncejk.biz
darjheef.com	NS dog.ccpatoncejk.biz
uigurimfif.com	NS dog.ccpatoncejk.biz
zinciccgag.com	NS dog.ccpatoncejk.biz
klfiduciaig.com	NS dog.ccpatoncejk.biz
lkchordabjg.com	NS dog.ccpatoncejk.biz

3. One More "Trick" To Think About

- As you collect information about phishing-related sites, you will often find yourself working with large lists of IP addresses. The IP addresses may not have working reverse DNS ("number-to-name"), and doing whois on lots of IP addresses quickly is impracticable (the whois servers may block you for doing too many queries).
- Consider using autonomous system numbers as a unit of aggregation, instead.
- Quick overview discussion of ASNs at
<http://darkwing.uoregon.edu/~joe/one-pager-asn.pdf>
- There are some nice tools for processing lists of IPs into a format suitable for sharing... for example...

Team Cymru Whois Server



Team Cymru is happy to announce the availability of a public whois server dedicated to mapping IP numbers to ASNs, located at **whois.cymru.com**. We have also extended the functionality of this daemon to support BULK IP submissions when combined with netcat, for those who wish to further optimize their queries. We recommend the use of the GNU version of netcat, not nc. GNU netcat can be downloaded from <http://netcat.sourceforge.net/download.php>.

The data provided by the whois server is based on 17 BGP peers, and is updated every 30 minutes.

Using the WHOIS Server

Following is a quick overview of how to use the Team Cymru whois server:

```
$ whois -h whois.cymru.com <IP>
```

Where <IP> is replaced by the IP you'd like to map, like so:

```
$ whois -h whois.cymru.com 68.22.187.8
ASN | IP | Name
23028 | 68.22.187.8 | SAUNET SAUNET
```

You can also include comments in your queries. These might be port information, timestamps or ...