Some Technical Suggestions For Institutions Targeted By Phishers

Valley Fraud Working Group
Emergency Training Center, 2nd & Chambers
Eugene, OR 10:30, January 25th, 2005

Joe St Sauver, Ph.D. (joe@uoregon.edu)
University of Oregon Computing Center

http://darkwing.uoregon.edu/~joe/antiphishing/

My Background; Sean’s Invitation

- I work for the UO Computing Center as Director, User Services and Network Applications; part of what I do there involves a variety of security-related projects both at the campus and national level. For example, I’m one of two senior technical advisors for MAAWG (the carrier Messaging Anti-Abuse Working Group), I’m an incoming co-chair for the Educause Security Effective Practices Group, I sit on the Internet2 Security at Line Speed (SALSA) working group and I’ll be teaching a course on computer and network security for the Applied Information Management program at UO in Portland later this term.
- I’m happy to say I’ve known Sean Hoar for some years, and when he heard some of my ideas about phishing, he was kind enough to get me added to today’s agenda.

Format/Goals/Audience for Today's Talk

- 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 goal today is just to offer some suggestions for your consideration. I know that many of you have probably been working on phishing-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 sound operational or financial reasons, or simply because you're busy putting out other more pressing fires first. My suggestions are just that, they're *not* meant as criticisms.
- I'm expecting that you, the audience, consist primarily of fraud investigators, financial institution folks, and law enforcement people (not computer/network geeks).

Let's Begin With Some Context: Phishing Has Become Ubiquitous

- "A recent study from TrustE and conducted by the Ponemon Institute found that 35 percent of survey respondents receive phishing e-mails once a week, while 70 percent have unintentionally visited a spoofed Web site—designed to get them to divulge personal information such as credit card numbers." "Security" (12/22/2004)
  http://www.pcmag.com/article2/0,1759,1744304,00.asp
- "US hit by 57 million phishing attacks in one year"
  http://news.zdnet.co.uk/0,39020330,39153695,00.htm
  May 5, 2004
  (for context, US population is ~295M, US Internet users are ~198M)
- "Survey: 2 Million Bank Accounts Robbed"
  http://www.msnbc.msn.com/id/5184077/
  June 14, 2004
  (for context, there were 215,470 armed robberies in 2002)
- "During the first two weeks in October, CipherTrust found that less than one percent of e-mail messages are phishing attacks."
  http://www.ciphertrust.com/resources/statistics/index.php
  (so what's going to happen when these guys get ramped up/serious?)

Some Highly Targeted Institutions Are Located Here in the Pacific Northwest

- For example, 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 connecting relay 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
```

The Phishvertised Message Has Become Very Professional

- For a long time, we were collectively lucky, and phishvertised messages were relatively crude and easy to spot, with poor production values, misspellings, odd grammatical usages, etc. No more! Contemporary phishing messages have become substantively indistinguishable from genuine institutional mail.
- Doubt that this is true? Try one of the Phishing Test pages such as The MailFrontier Phishing IQ Test (they now have both their original and a 2nd edition available from… http://survey.mailfrontier.com/survey/quiztest.cgi)
- Nice online archive of examples at: http://antiphishing.org/phishing_archive.html

Financial Loss Is a Real Risk, But the Bigger Risks Are Churn & Loss of Consumer Confidence in Online Operations

- Yes, the direct financial losses associated with phishing are bad, but…
- What if consumers lose trust in your institution, and leave for a more “security conscious” competitor? Customer churn can *kill* a financial institution.
- Or what if consumers become so afraid and confused about what is and isn’t “real” or “safe” online that they stop doing business online and revert to just bricks-and-mortar visits, physically depositing paychecks, avoiding ATMs, shunning online payment infrastructures, etc. Loss of consumer confidence can result in decreased use of automation/increased operational costs which may dwarf one time direct phishing-related losses.

So What Should You Do?

You REALLY Need to Publish SPF Records for Your Domains

- SPF records describe what network addresses should be originating email for a given domain. For example:

```
% 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“
% host -t txt smithbarney.com
smithbarney.com text "v=spf1 a:mail.citigroup.com ~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 ebay.com
ebay.com text "spf2.0/pra mx include:s._sid.ebay.com include:m._sid.ebay.com
include:p._sid.ebay.com include:c._sid.ebay.com ~all“
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“
% host -t txt americanexpress.com
americanexpress.com text "v=spf1 include:aexp.com ~all"
```

- For more information see “Sender Authentication: What to Do,” http://spf.pobox.com/whitepaper.pdf

You REALLY Need to Publish SPF Records for Your Domains (cont.)

- 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?

```
% host -t txt bankone.com
% host –t txt centennialbank.com
% host -t txt chase.com
% host -t txt firstunion.com
% host -t txt jpmorgan.com
% host –t txt key.com
% host –t txt mastercard.com
% host –t txt mbna.com
% host –t txt oregoncommunitycu.org
% host –t txt selco.org
% host –t txt suntrust.com
% host –t txt therightbank.com
% host –t txt usbank.com
% host –t txt visa.com
% host -t txt wamu.com
% host -t txt wellsfargo.com
```

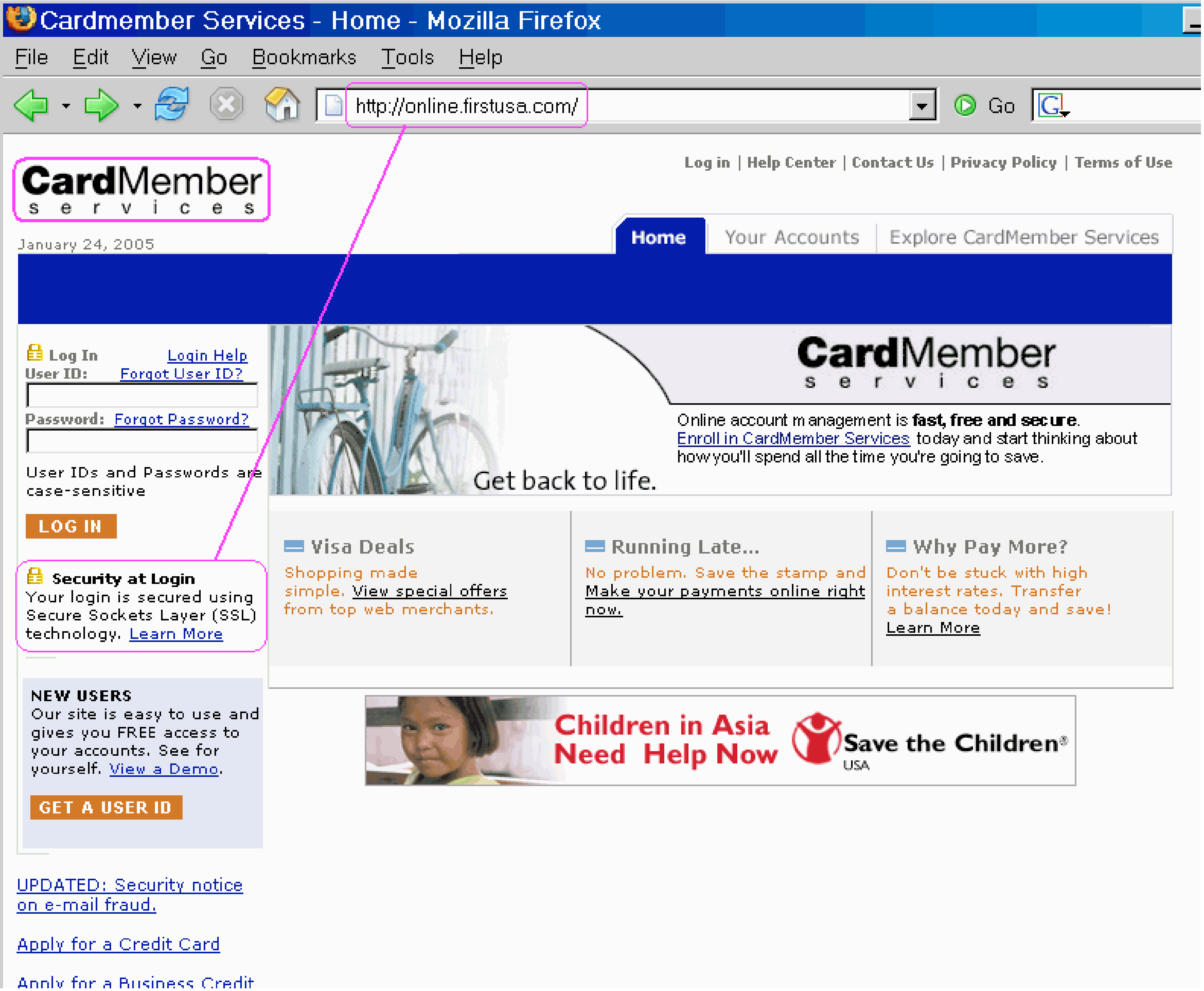
- Sorry if I missed checking your institution’s domain! :-)

Are You Digitally Signing The Email Your Institution Sends?

- We know that many of your customers wouldn’t know what an S/MIME-signed message or a PGP-signed message is (at least right now) but that’s not really sufficient justification for you not to begin exploring digitally signed email. Over time more users WILL begin to expect to see important messages digitally signed. You might as well learn how to do it now.
- Nice starting resource:
  “What Are S/MIME Digital Signatures?”
  http://www.antiphishing.org/smim-dig-sig.htm
- PGP takes a somewhat different approach; for a nice introduction to how PGP works, see:
  http://www.pgpi.org/doc/pgpintro/

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

- What happens if a user makes a trivial error, like misspelling/mistyping a domain name or accidentally omitting punctuation, such as a period?
- For example, BankOne uses http://online.firstusa.com/ for its online banking web site…
  online.firstusa.com ==> 159.53.216.62 ==> 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/

CardMember services

January 24, 2005

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

Home
Your Accounts
Explore CardMember Services

Log In Login Help

User ID: Forgot User ID?

Password: Forgot Password?

User IDs and Passwords are case-sensitive

LOG IN

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

NEW USERS
Our site is easy to use and gives you FREE access to your accounts. See for yourself. View a Demo.

GET A USER ID

UPDATED: Security notice on e-mail fraud.

Apply for a Credit Card

Apply for a Business Credit

Get back to life.

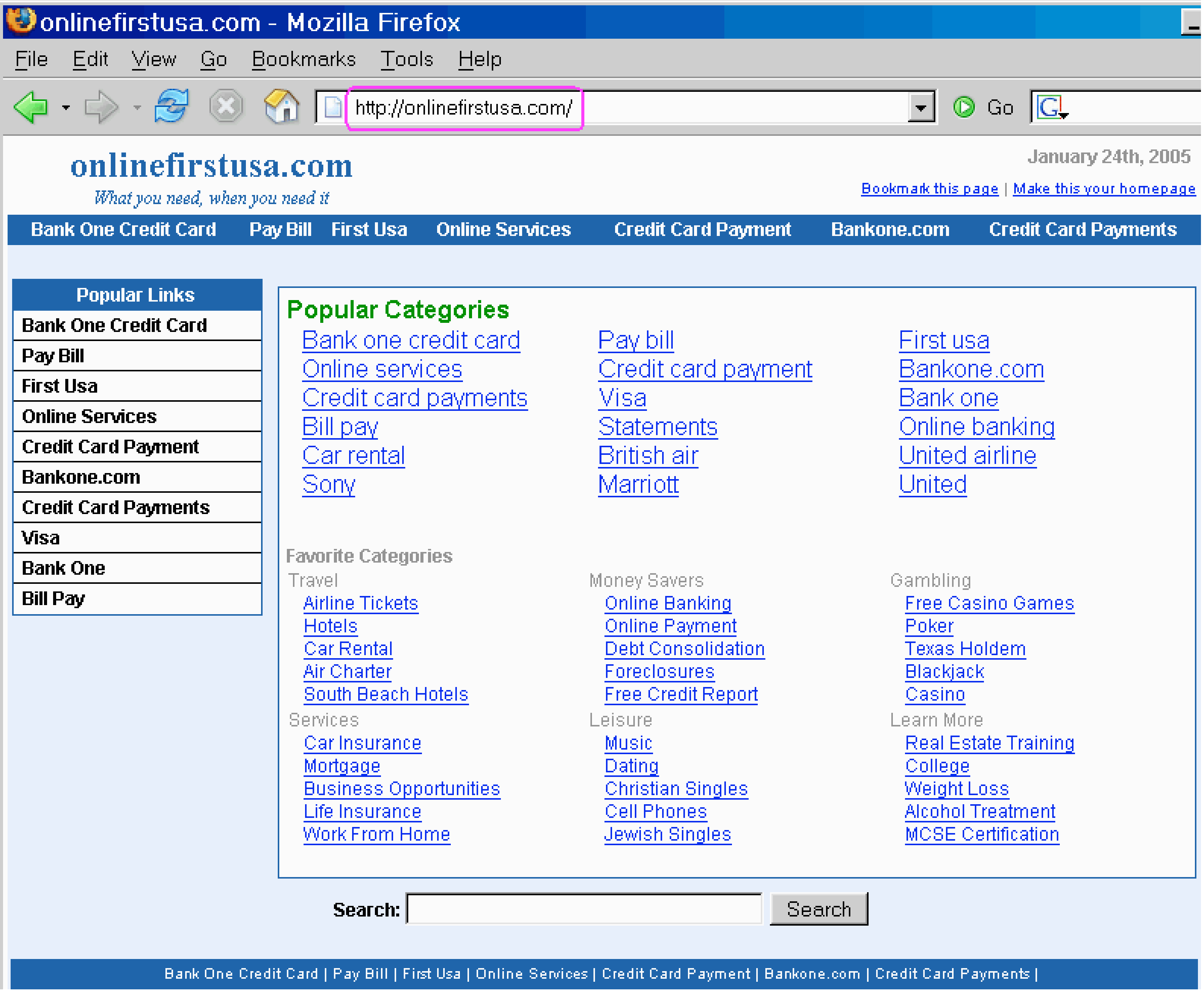
CardMember services

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

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


onlinefirstusa.com - Mozilla Firefox
File
Edit
View
Go
Bookmarks
Tools
Help
http://onlinefirstusa.com/
Go

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

Favorite Categories

Travel

- Airline Tickets
- Hotels
- Car Rental
- Air Charter
- South Beach Hotels

Services

- Car Insurance
- Mortgage
- Business Opportunities
- Life Insurance
- Work From Home

Money Savers

- Online Banking
- Online Payment
- Debt Consolidation
- Foreclosures
- Free Credit Report

Leisure

- Music
- Dating
- Christian Singles
- Cell Phones
- Jewish Singles

Gambling

- Free Casino Games
- Poker
- Texas Holdem
- Blackjack
- Casino

Learn More

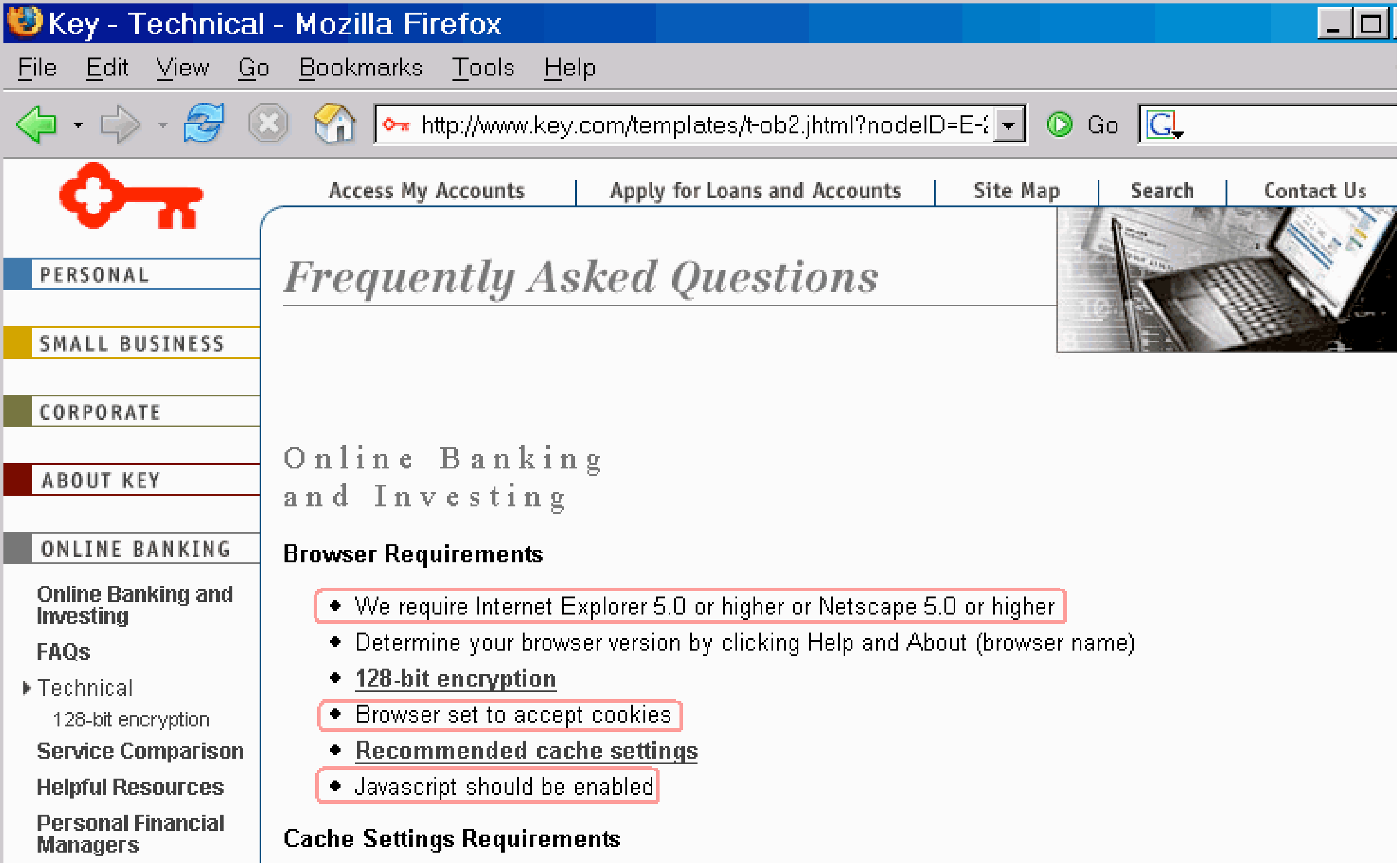
- Real Estate Training
- College
- Weight Loss
- Alcohol Treatment
- MCSE Certification

Search: Search

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

Make Sure Your Website Encourages/ Enables Good Security Practices

- Does your institutional web site require use of **Internet Explorer** for the web site to work properly? [Yes, we know that IE still has a 90% market share, but 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 or other alternatives work, too.
- Does your website require customers to use **Javascript** or other scripting technology? If so, please understand that doing so substantially increases your customers' exposure to a host of web-related vulnerabilities (see http://www.cert.org/tech_tips/malicious_code_FAQ.html)



Frequently Asked Questions

Online Banking and Investing

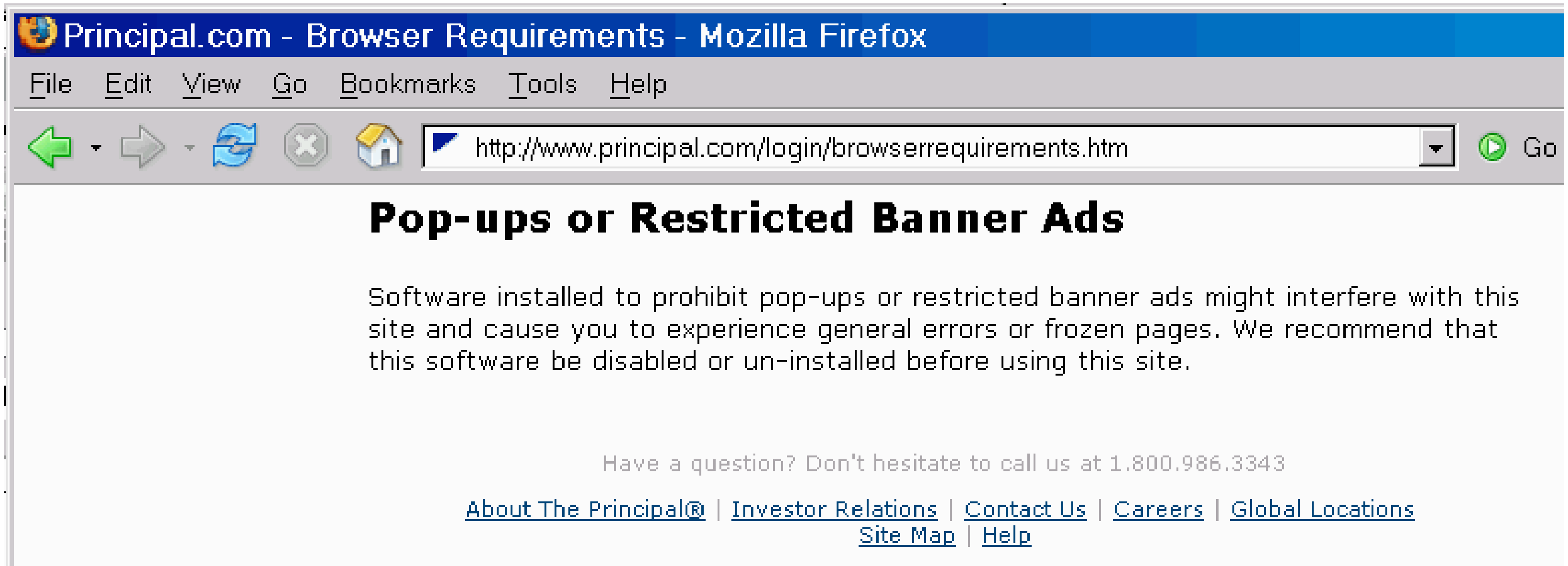
Browser Requirements

- 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

Make Sure Your Website Encourages/ Enables Good Security Practices (cont.)

- Does your site require use of 128 bit SSL encryption?
- Does your site require users to allow **popup windows**? (Remember that Windows XP SP2 now routinely blocks popup Windows. Should you be using that sort of feature on your 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
- Are your web pages **cacheable**? They 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?
- Do idle sessions time out?

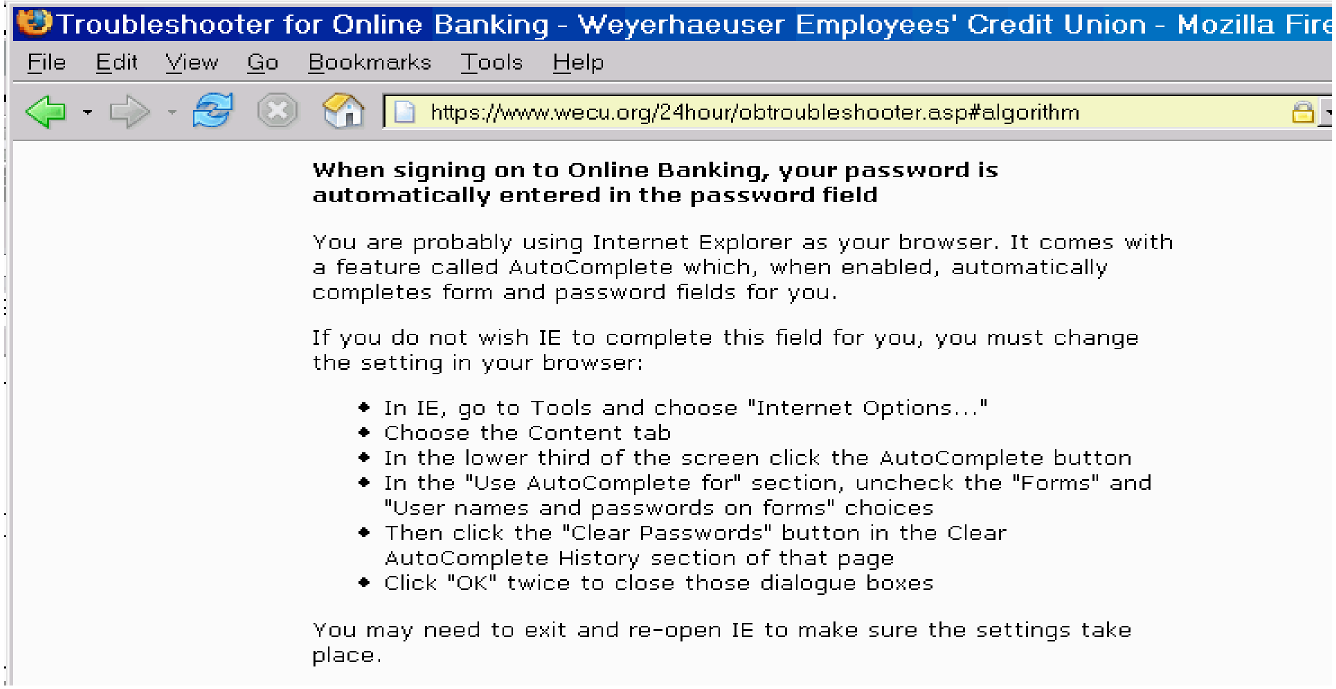

Principal.com - Browser Requirements - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.principal.com/login/browserrequirements.htm
Go

Pop-ups or Restricted Banner Ads

Software installed to prohibit pop-ups or restricted banner ads might interfere with this site and cause you to experience general errors or frozen pages. We recommend that this software be disabled or un-installed before using this site.

Have a question? Don't hesitate to call us at 1.800.986.3343

About The Principal® | Investor Relations | Contact Us | Careers | Global Locations
Site Map | Help


Troubleshooter for Online Banking - Weyerhaeuser Employees' Credit Union - Mozilla Fire
File Edit View Go Bookmarks Tools Help
https://www.wecu.org/24hour/obtroubleshooter.asp#algorithm

When signing on to Online Banking, your password is automatically entered in the password field

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.

If you do not wish IE to complete this field for you, you must change the setting in your browser:

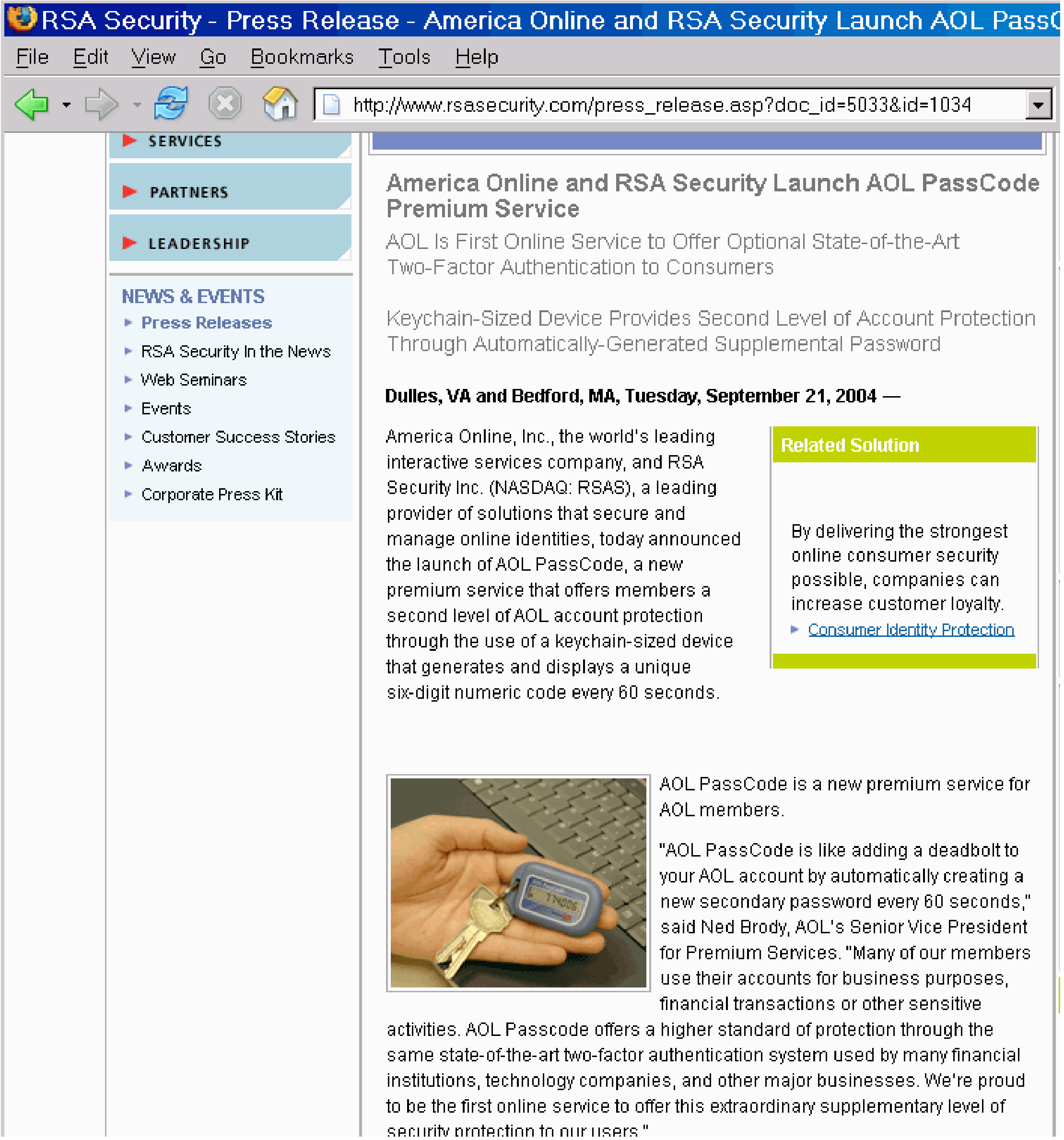
- In IE, go to Tools and choose "Internet Options..."
- Choose the Content tab
- In the lower third of the screen click the AutoComplete button
- In the "Use AutoComplete for" section, uncheck the "Forms" and "User names and passwords on forms" choices
- Then click the "Clear Passwords" button in the Clear AutoComplete History section of that page
- Click "OK" twice to close those dialogue boxes

You may need to exit and re-open IE to make sure the settings take place.

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.

Even AOL is Doing Two Factor These Days



http://www.rsasecurity.com/press_release.asp?doc_id=5033&id=1034

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.

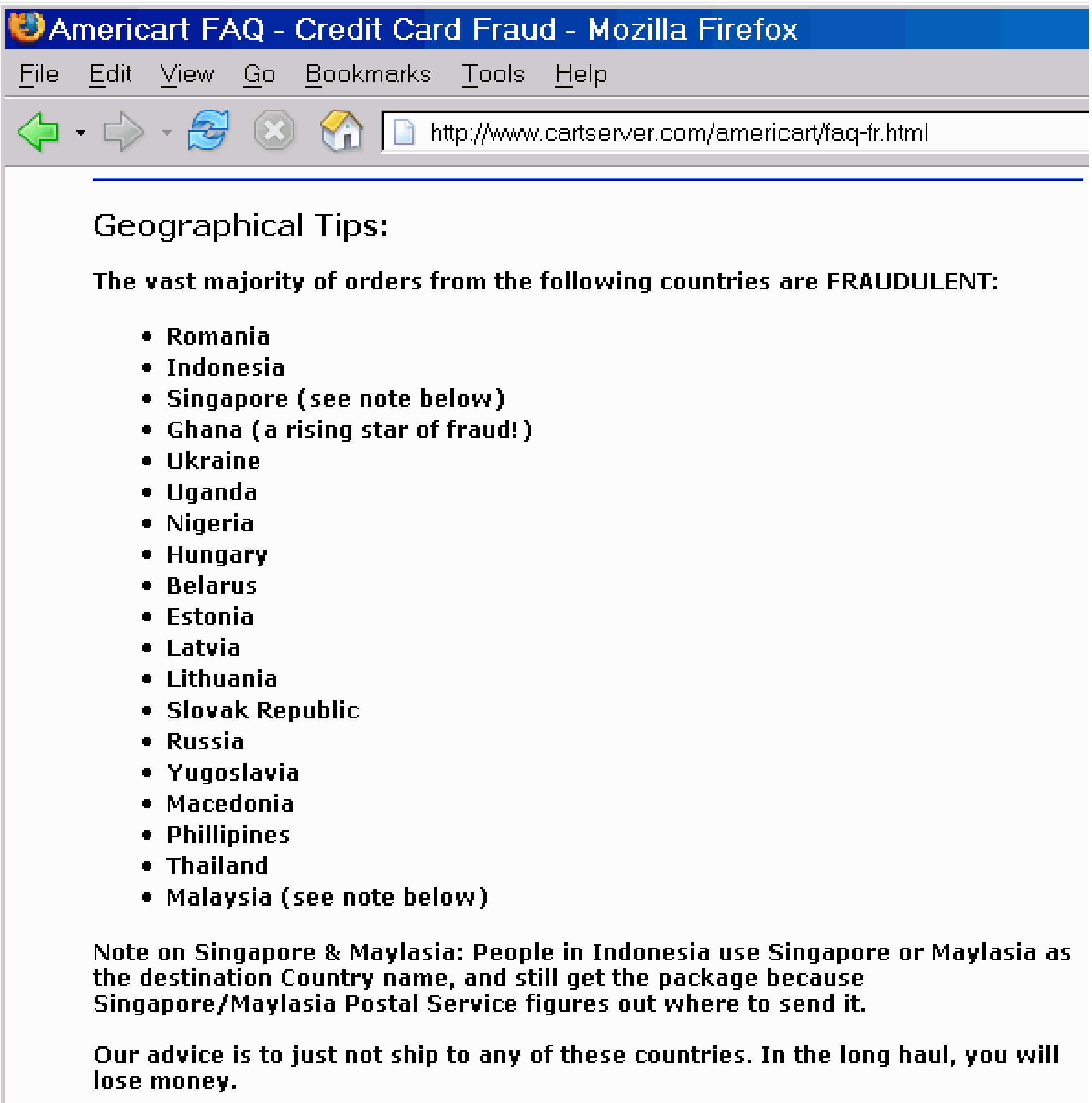
- Consumer Identity Protection

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 supplemental level of security protection to our users."

Are You Actively Monitoring Access to Online Banking Resources That Originate From “Unusual” Locations?

- 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.
- 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? [“What do you mean I last accessed my account from a cyber cafe somewhere in Budapest???”]
- Some countries may have particularly high levels of fraud-related activity. (Be aware that in some cases it may be hard to determine the true geolocation of a given Internet user due to abuse of open proxy servers)


Americart FAQ - Credit Card Fraud - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.cartserver.com/americart/faq-fr.html

Geographical Tips:

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

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

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

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

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

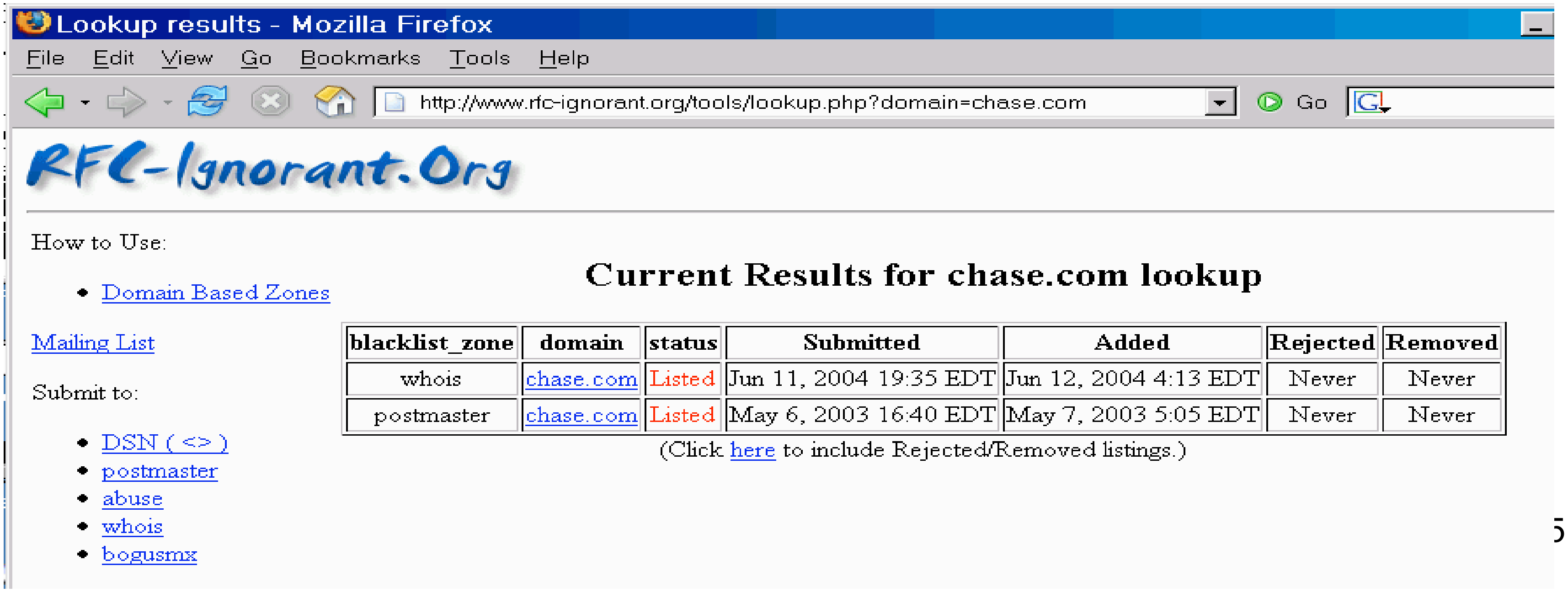
- Scam artists love to use graphics directly from your institutional web site; the URLs in their email help lull users into a false sense of security, and using hyperlinks instead of attached graphics helps reduce the size of each mail they send. You, obviously, want to prevent this.
- This problem is, in many ways, quite analogous to what “adult hosting” companies face when competitors try to include/reuse “graphical content” without permission.
- Solutions **have** been developed to eliminate or reduce this issue. Try googling for *anti-leach .htaccess* or see http://httpd.apache.org/docs/misc/rewriteguide.html under “Blocked Inline-Images”
- At a minimum, watch your server’s logs!

You 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 whois points of contact, etc. go through as RFC2142 (and common sense) say it should? Also be particularly careful that you're accepting spamcop.net reports; they're generally of remarkably high quality.


Lookup results - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.rfc-ignorant.org/tools/lookup.php?domain=chase.com
Go
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.)

What’s Next?

Beware of “New” DNS-Based Attacks

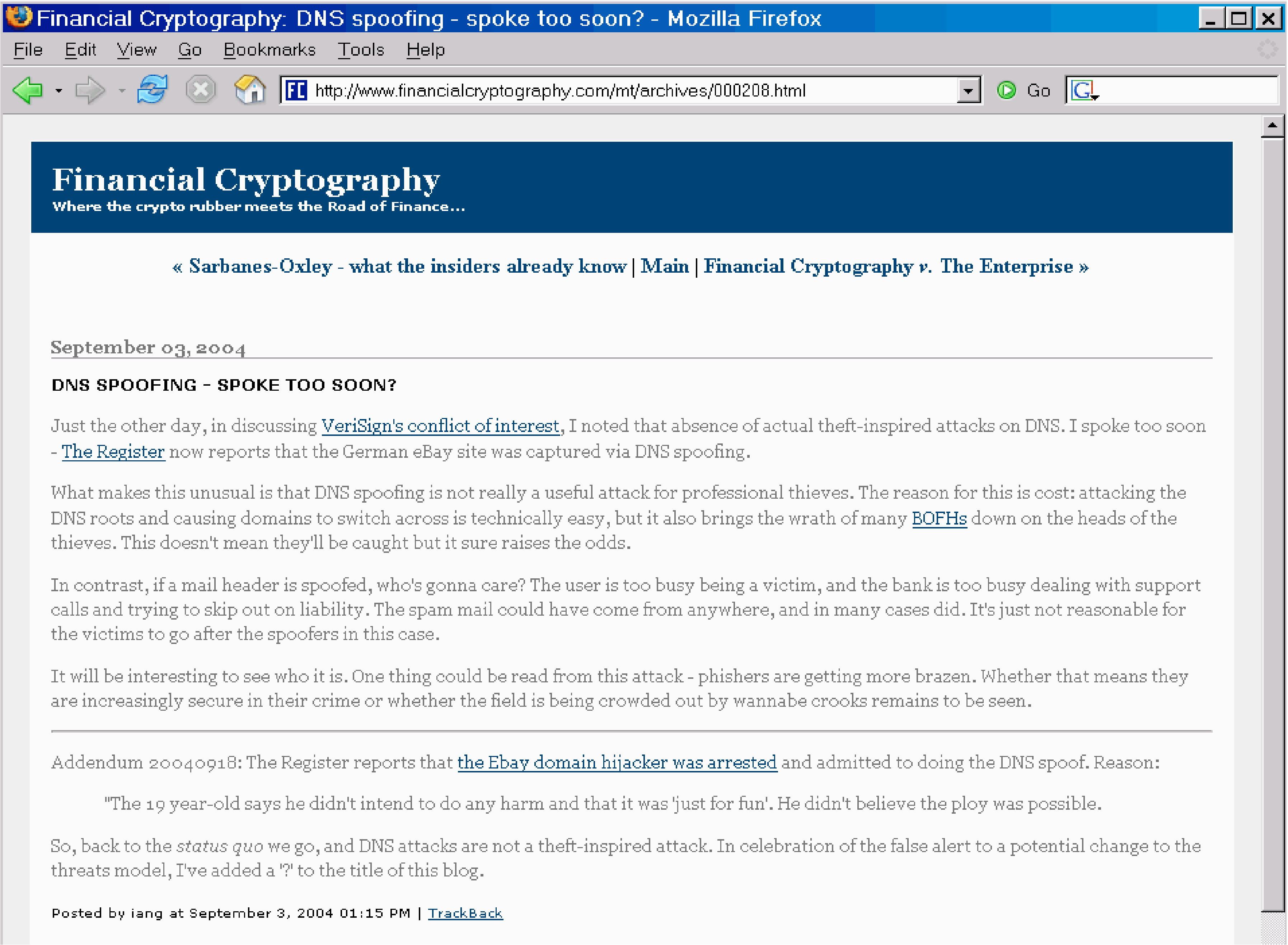
- While traditional phishing attacks have focused on luring users into clicking on links that appear to be legitimate (but which actually go to bogus sites), you should be aware that a new/emerging approach to doing phishing attacks has emerged which relies on changing the actual mapping of domain names to IP addresses.

> “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
Go

http://www.financialcryptography.com/mt/archives/000208.html

Financial Cryptography

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

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

September 03, 2004

DNS SPOOFING - SPOKE TOO SOON?

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

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

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

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

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

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

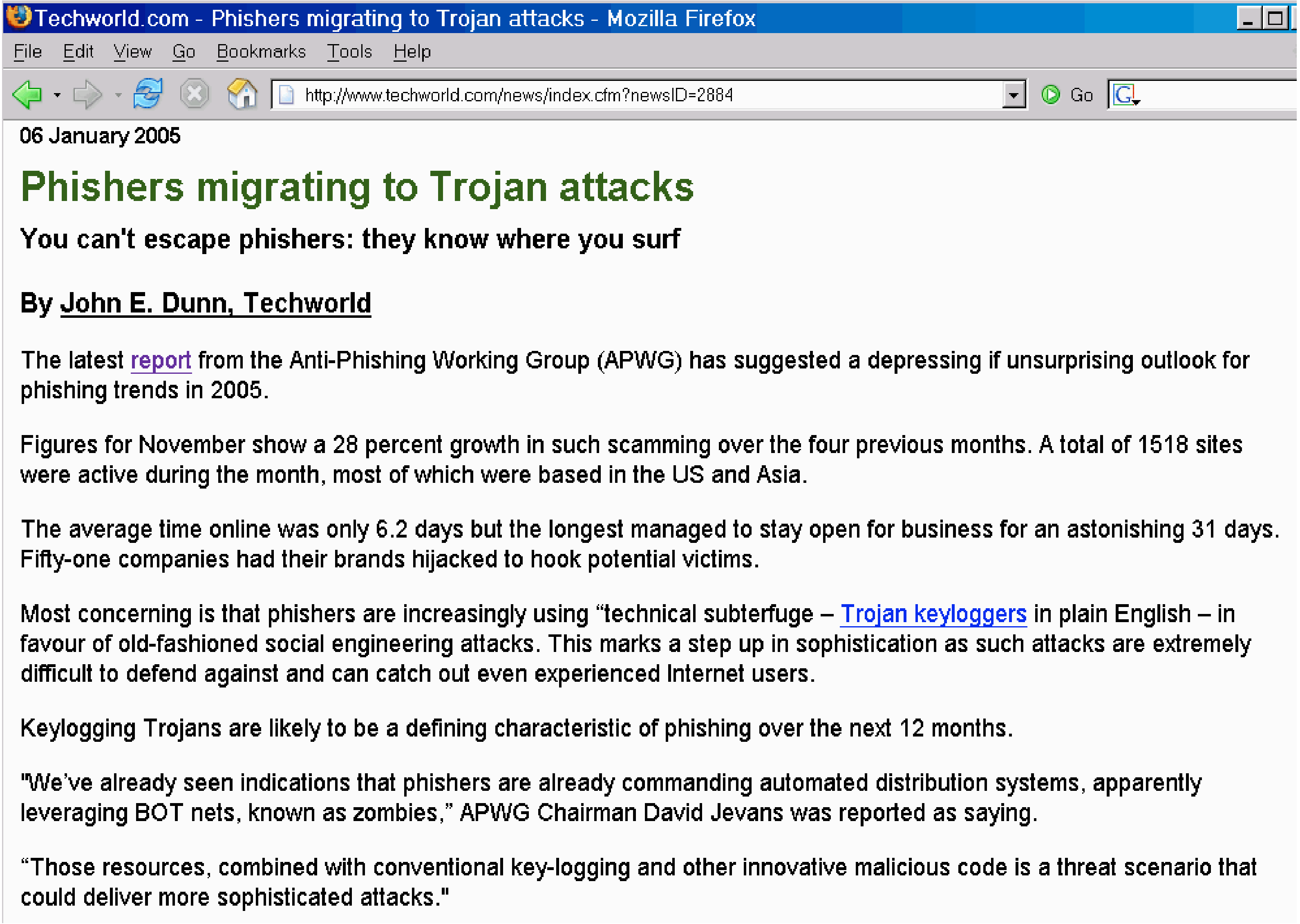
So, back to the *status quo* we go, and DNS attacks are not a theft-inspired attack. In celebration of the false alert to a potential change to the threats model, I've added a '?' to the title of this blog.

Posted by iang at September 3, 2004 01:15 PM | TrackBack

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
  -- 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
  -- 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).

Traditional Phishing Isn’t The Only Risk; Beware Keystroke Grabbing/Sniffing Spyware


Techworld.com - Phishers migrating to Trojan attacks - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.techworld.com/news/index.cfm?newsID=2884
Go

06 January 2005

Phishers migrating to Trojan attacks

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

By John E. Dunn, Techworld

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

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

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

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

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

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

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

Thanks For The Chance to Talk Today!

- Are there any questions?