How to Avoid Losing Your Money and Identity to Phishing

Tom Chen
tchen@engr.smu.edu

Outline

- What is Phishing?
- Examples
- Risks and threats
- Defenses

What is Phishing?

- A social engineering attack:
  - E-mail message (spam) appears from financial institution prompting user to a fake Website (eg, to verify your account)
  - Victim is tricked into submitting personal info. (account number, password) at fake Website
  - Fake Website steals confidential personal info. or downloads malicious code

Victims

- Consumers
- Financial organizations
  - Banks: Citibank, Wells Fargo, US Bank, NatWest, Barclays, Lloyds Bank,...
  - Credit card companies: VISA,...
  - Retailers: eBay, PayPal, Amazon,...
  - ISPs: AOL, MSN, Yahoo, Earthlink,...

Statistics

- $ 1.2 billion damages to US financial organizations so far
- In US, 57 million consumers have received phishing e-mail
  - 1.8 million consumers believe tricked (3% rate)
- Phishing sites are hosted mostly in US (32%), China (12%), Korea (11%), Japan (3%), others

December 2004 Statistics

- 1,707 active phishing Websites detected
- 24% monthly increase in phishing Websites
- Phishing Website is online for 5.9 days on average
- 55 brands hijacked

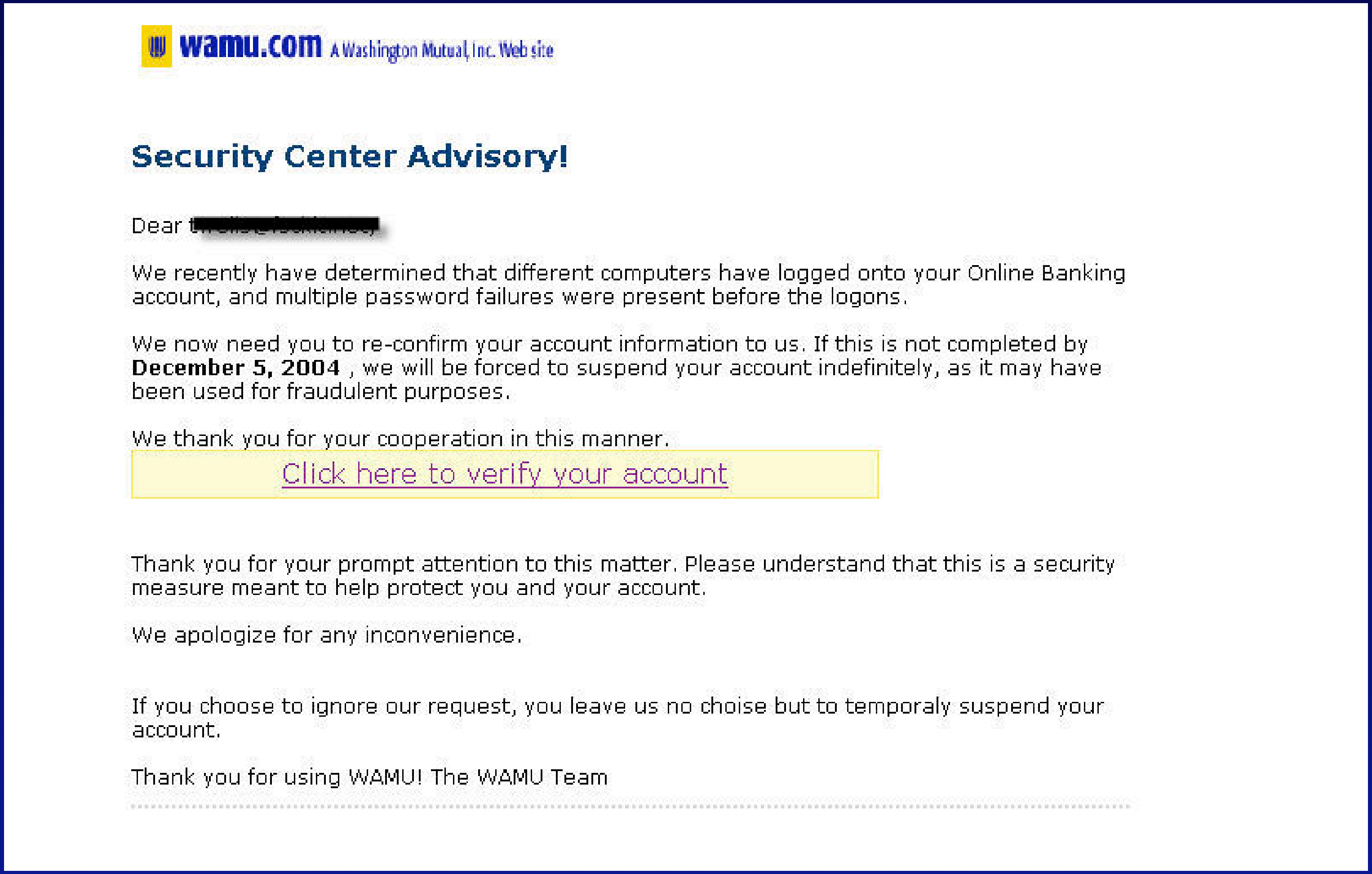
Nigeria 419 Scam

- Early example of spam used for online fraud
  - 419 is named after Nigerian criminal code
- Spam e-mail describes large funds or similar in Nigeria or other African nation (endless variations)
- User is asked for advance fee or similar to receive funds or goods

Nigeria 419 Scam

- Complications may require more advance fees until victim quits
  - Nothing is ever received
- Nigerian government is believed to running the scam, making $ billions from worldwide
  - A surprising number of people still fall victim to this scam monthly

Example 1: e-mail from Washington Mutual reports failed logins to online account and asks for confirmation of account info



wamu.com A Washington Mutual, Inc. Web site

Security Center Advisory!

Dear [redacted]

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us. If this is not completed by **December 5, 2004** , we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

We thank you for your cooperation in this manner.

Click here to verify your account

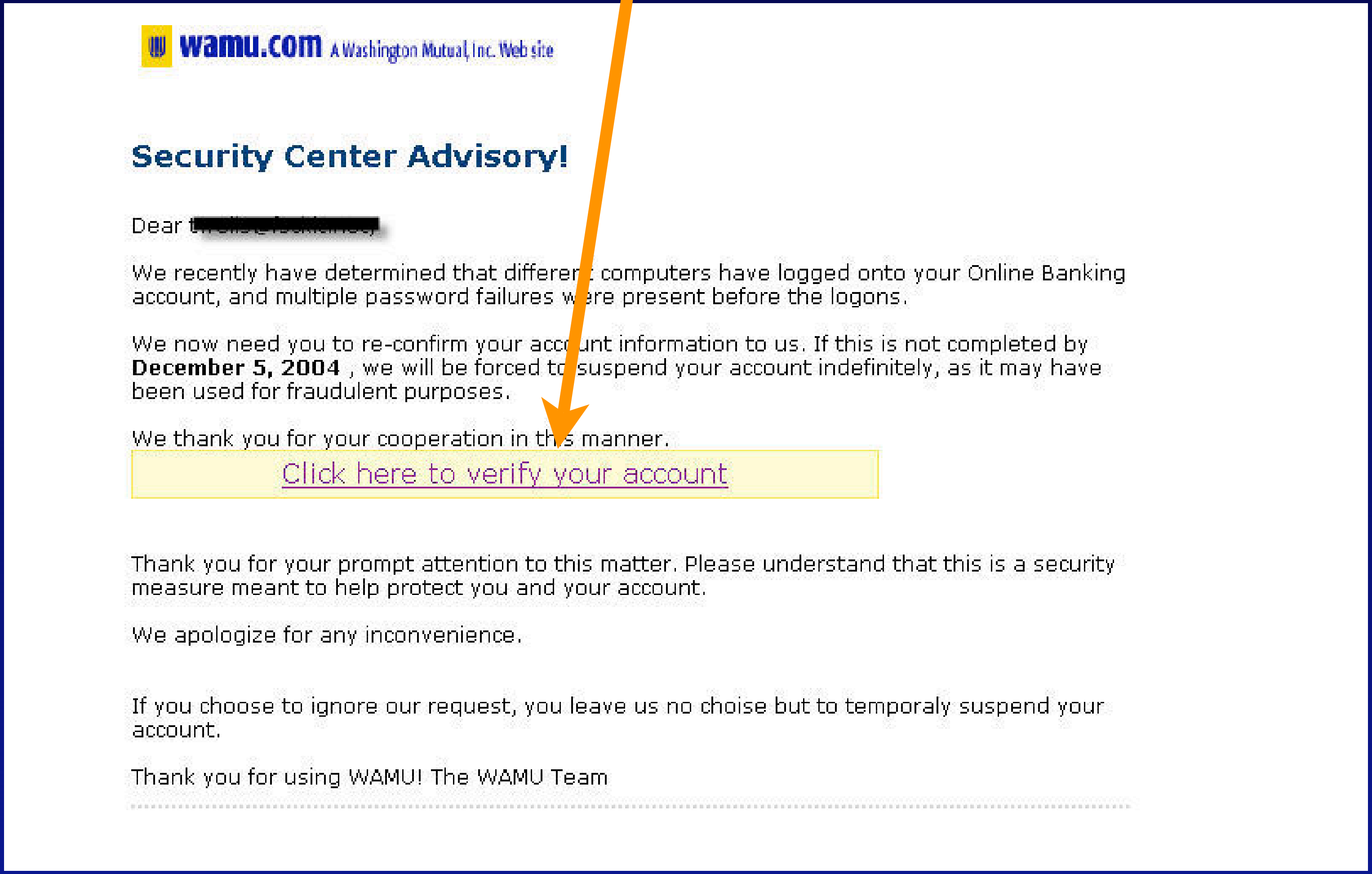
Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using WAMU! The WAMU Team

Link to IP address 218.68.80.234 (in China)



wamu.com A Washington Mutual, Inc. Web site

Security Center Advisory!

Dear [redacted]

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us. If this is not completed by **December 5, 2004** , we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

We thank you for your cooperation in this manner.

Click here to verify your account

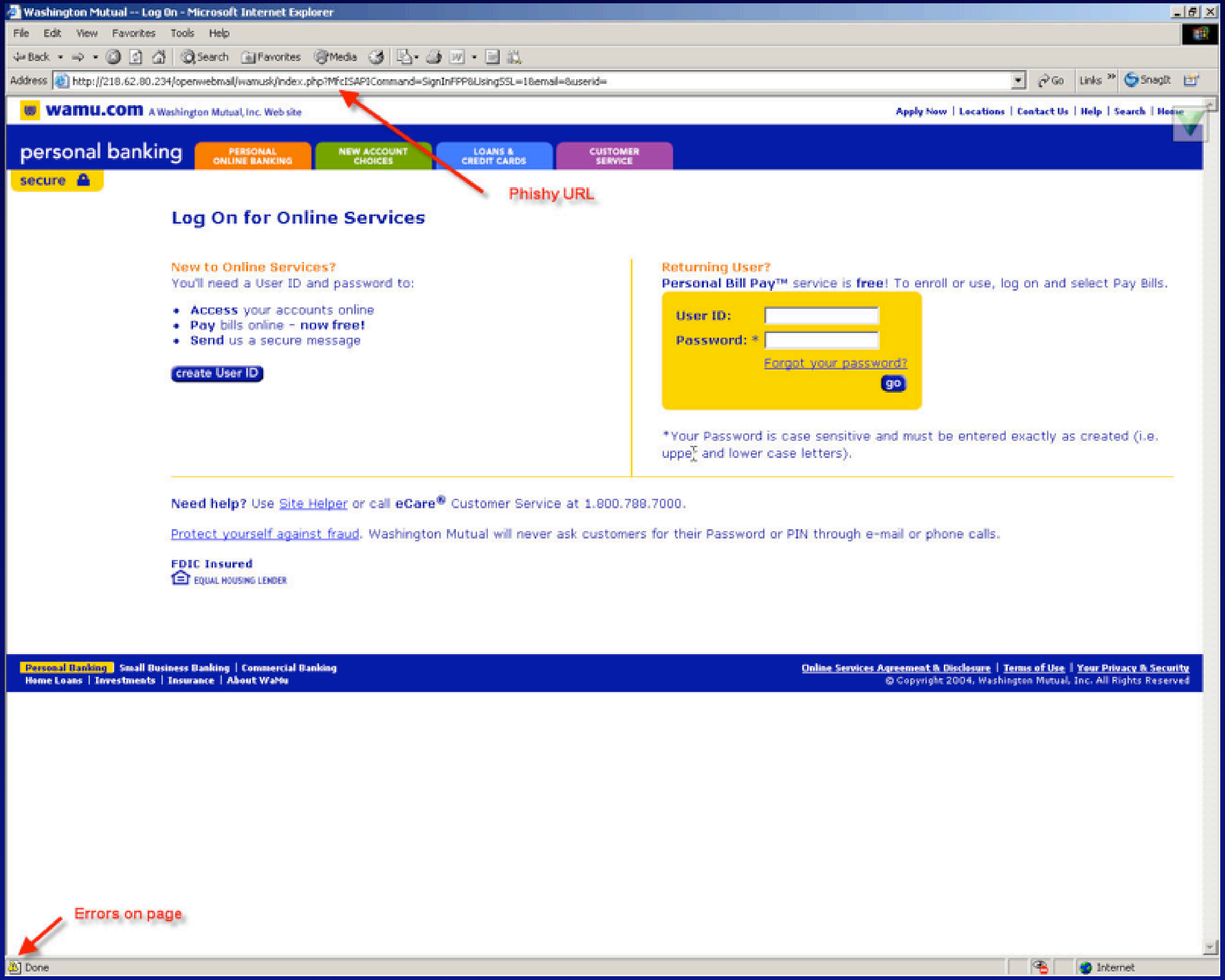
Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using WAMU! The WAMU Team

Clues on Website: long, strange URL “http://218.62.80.234/openwebmail/wamusk/....”


Washington Mutual -- Log On - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links SnagIt
Apply Now | Locations | Contact Us | Help | Search | Home
personal banking
PERSONAL ONLINE BANKING
NEW ACCOUNT CHOICES
LOANS & CREDIT CARDS
CUSTOMER SERVICE
secure
create User ID
go
Personal Banking | Small Business Banking | Commercial Banking
Home Loans | Investments | Insurance | About WaMu
Online Services Agreement & Disclosure | Terms of Use | Your Privacy & Security
Done
Internet

http://218.62.80.234/openwebmail/wamusk/index.php?MfcISAPICommand=SignInFPP&UsingSSL=1&email=&userid=

wamu.com A Washington Mutual, Inc. Web site

Log On for Online Services

New to Online Services?
You'll need a User ID and password to:

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

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

User ID:
Password: *
Forgot your password?

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

Need help? Use Site Helper or call eCare® Customer Service at 1.800.788.7000.

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

FDIC Insured
EQUAL HOUSING LENDER

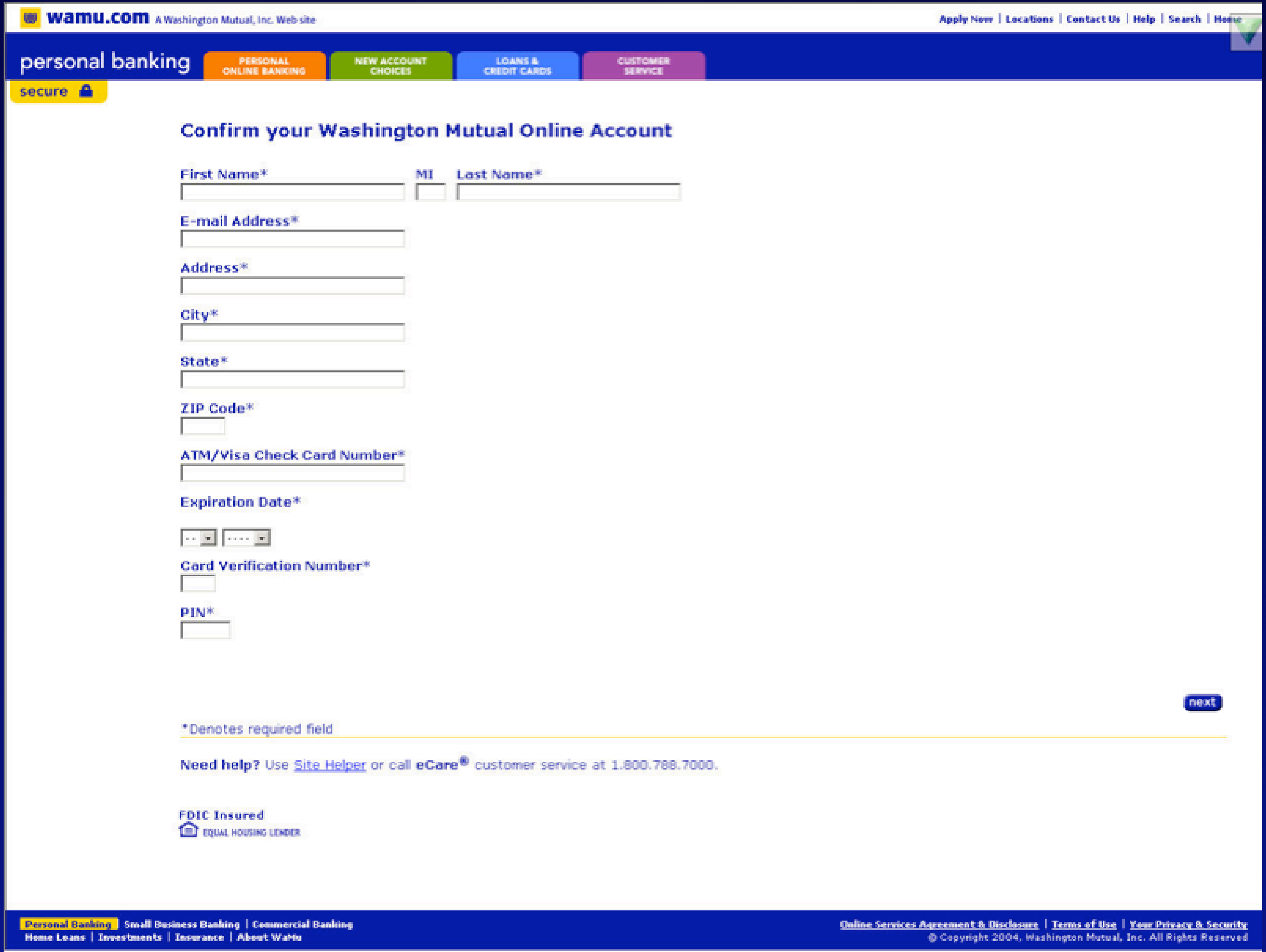
© Copyright 2004, Washington Mutual, Inc. All Rights Reserved

Phishy URL

Errors on page

IE shows rendering errors

After user logs in, Website asks for ATM/Visa check card info



wamu.com A Washington Mutual, Inc. Web site
Apply Now | Locations | Contact Us | Help | Search | Home
personal banking
PERSONAL ONLINE BANKING
NEW ACCOUNT CHOICES
LOANS & CREDIT CARDS
CUSTOMER SERVICE
secure

Confirm your Washington Mutual Online Account

First Name* MI Last Name*

E-mail Address*

Address*

City*

State*

ZIP Code*

ATM/Visa Check Card Number*

Expiration Date*

Card Verification Number*

PIN*

*Denotes required field

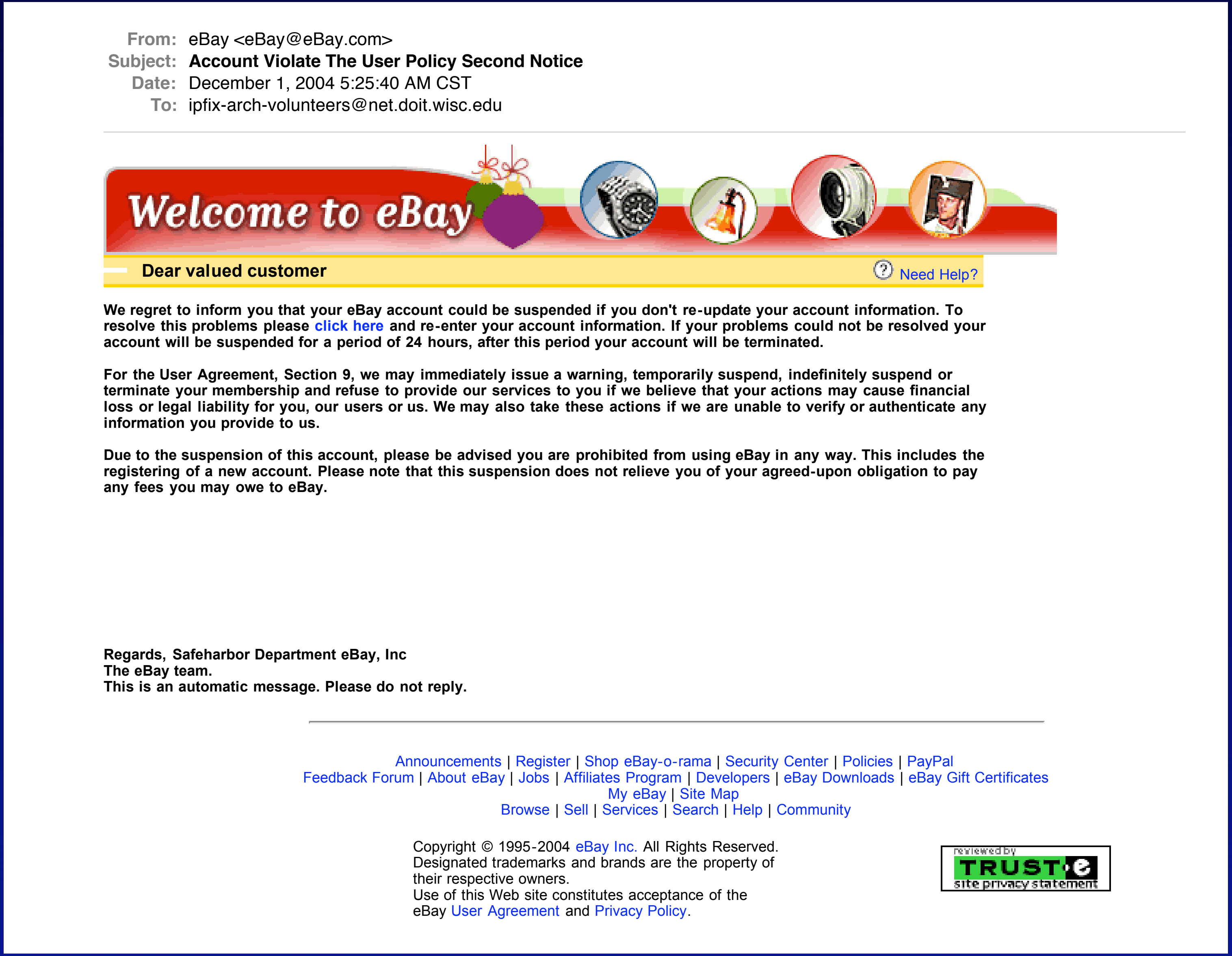
Need help? Use Site Helper or call eCare® customer service at 1.800.788.7000.

FDIC Insured
EQUAL HOUSING LENDER
Personal Banking | Small Business Banking | Commercial Banking
Home Loans | Investments | Insurance | About WaMu
Online Services Agreement & Disclosure | Terms of Use | Your Privacy & Security

© Copyright 2004, Washington Mutual, Inc. All Rights Reserved

Finally user is redirected to real "wamu.com" site

Example 2: e-mail asks for confirmation of eBay account or account will be suspended



From: eBay <eBay@eBay.com>
Subject: **Account Violate The User Policy Second Notice**
Date: December 1, 2004 5:25:40 AM CST
To: ipfix-arch-volunteers@net.doit.wisc.edu

Welcome to eBay

Dear valued customer Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

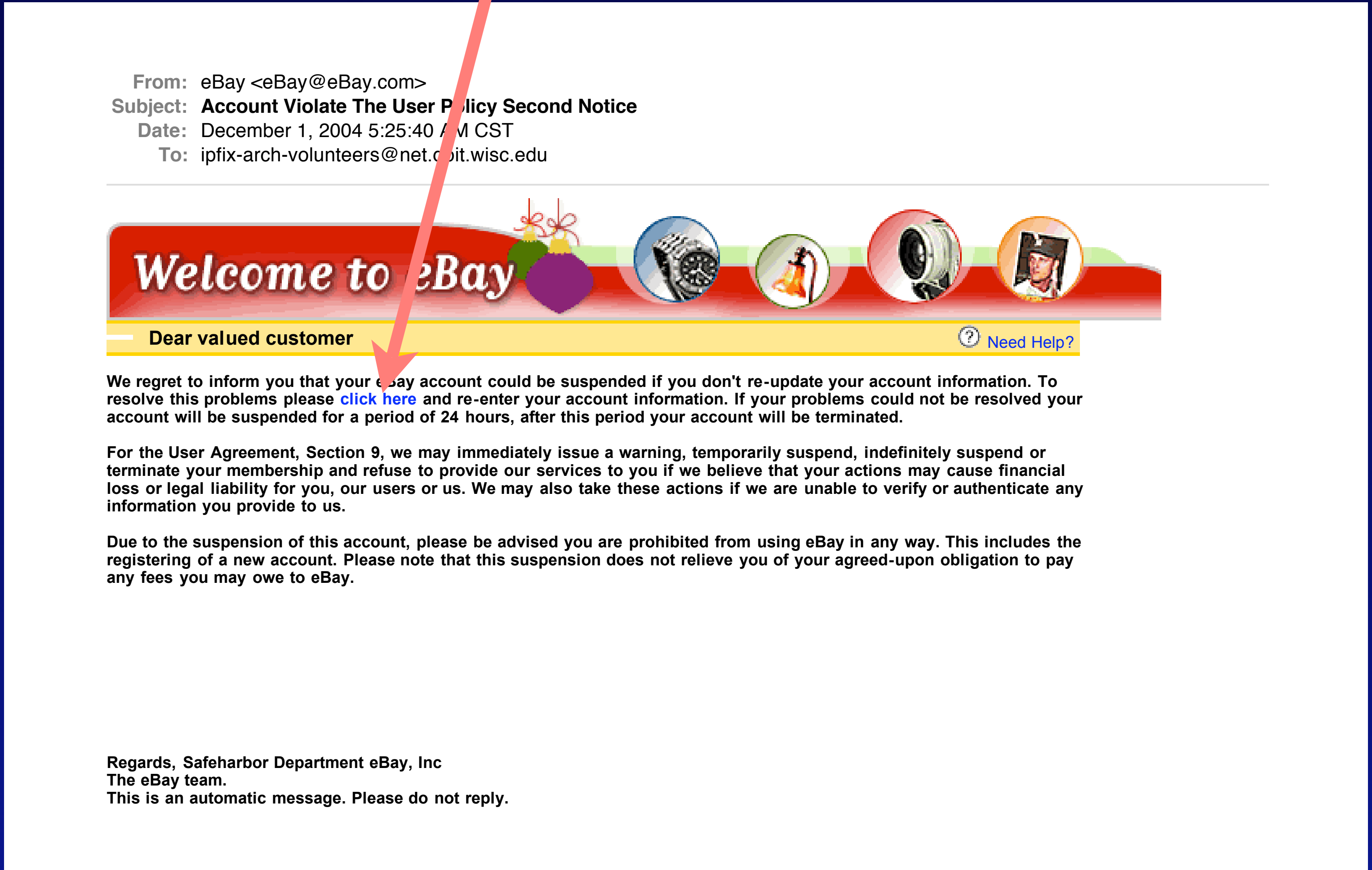
Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

Announcements | Register | Shop eBay-o-rama | Security Center | Policies | PayPal
Feedback Forum | About eBay | Jobs | Affiliates Program | Developers | eBay Downloads | eBay Gift Certificates
My eBay | Site Map
Browse | Sell | Services | Search | Help | Community

Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

reviewed by TRUSTe site privacy statement

Link calls "cgi3.ebay.com.wws2.us/update/aw-cgi/eBayISAPI.dll/index.html" intentionally similar to real eBay URL



From: eBay <eBay@eBay.com>
Subject: **Account Violate The User Policy Second Notice**
Date: December 1, 2004 5:25:40 AM CST
To: ipfix-arch-volunteers@net.doit.wisc.edu

Dear valued customer

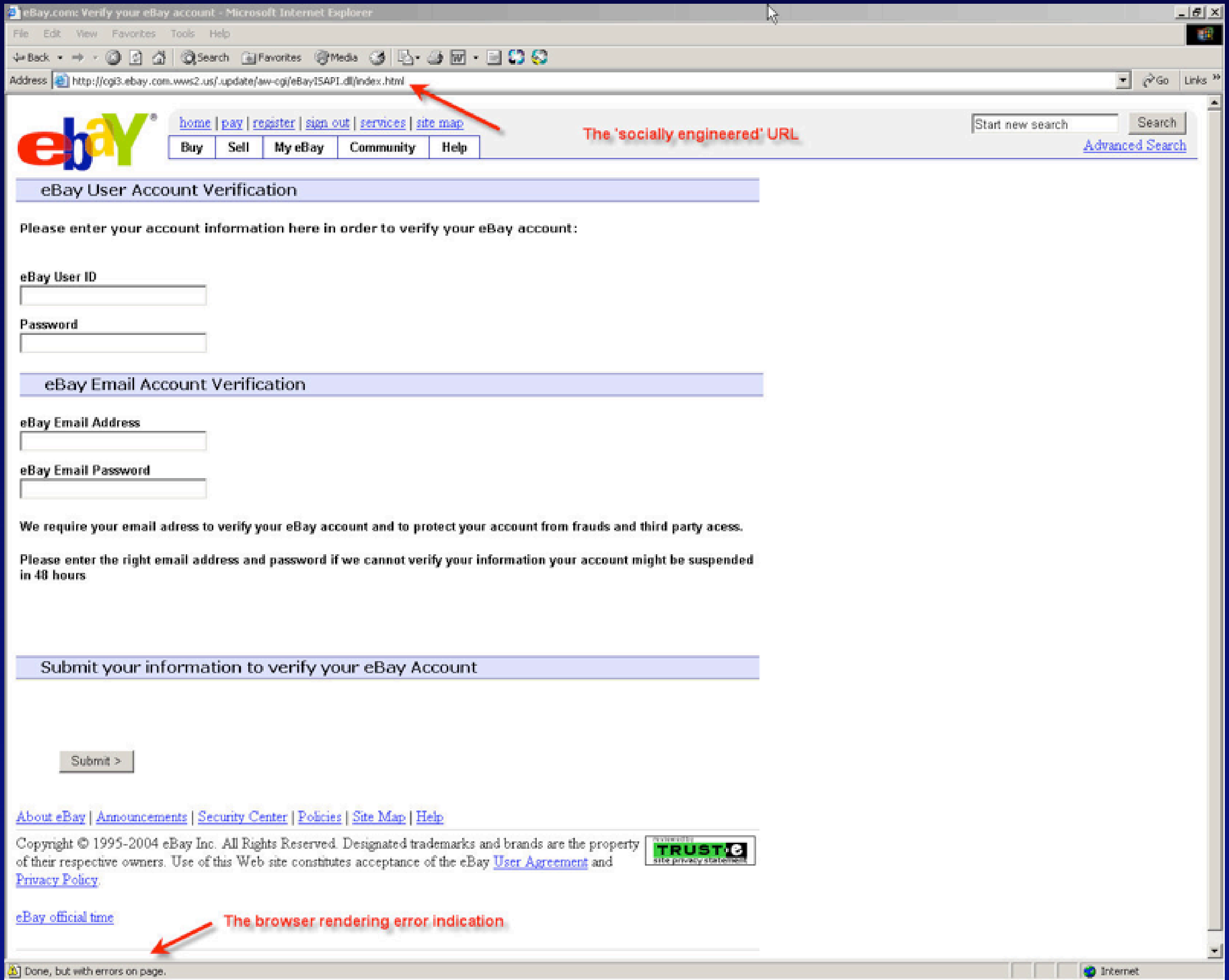
We regret to inform you that your ebay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

Clues: fake Website looks real except not exact URL


File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Go
Links
home | pay | register | sign out | services | site map
Buy
Sell
My eBay
Community
Help
Start new search
Search
Advanced Search
Submit >
About eBay | Announcements | Security Center | Policies | Site Map | Help
TRUSTe site privacy statement
Internet

eBay.com: Verify your eBay account - Microsoft Internet Explorer

Address http://cgi3.ebay.com.wws2.us/.update/aw-cgi/eBayISAPI.dll/index.html

The 'socially engineered' URL

eBay User Account Verification

Please enter your account information here in order to verify your eBay account:

eBay User ID

Password

eBay Email Account Verification

eBay Email Address

eBay Email Password

We require your email adress to verify your eBay account and to protect your account from frauds and third party acess.

Please enter the right email address and password if we cannot verify your information your account might be suspended in 48 hours

Submit your information to verify your eBay Account

Copyright © 1995-2004 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

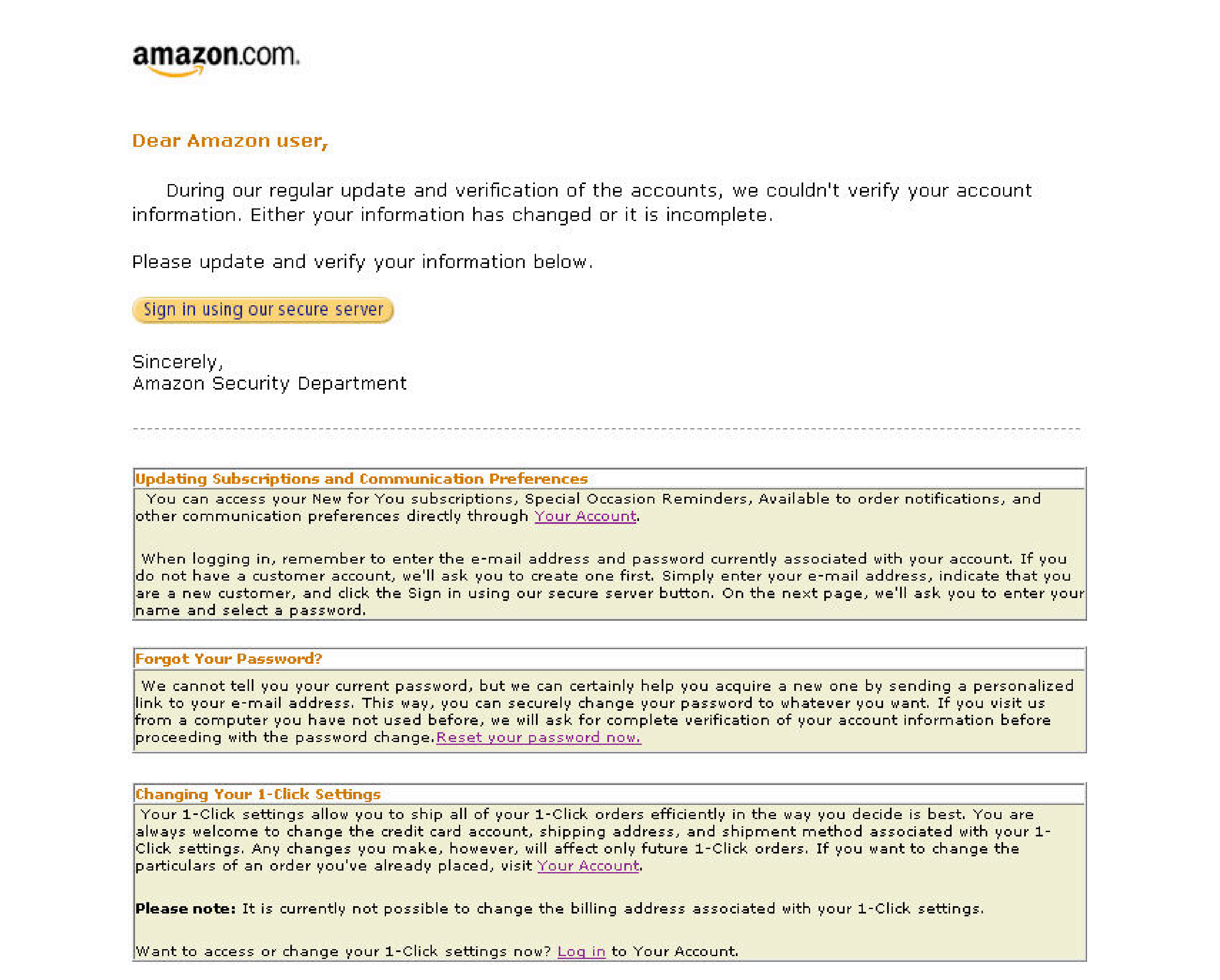
eBay official time

The browser rendering error indication

Done, but with errors on page.

IE shows rendering errors

Example 3: realistic e-mail from Amazon asking to verify account



amazon.com

Dear Amazon user,

During our regular update and verification of the accounts, we couldn't verify your account information. Either your information has changed or it is incomplete.

Please update and verify your information below.

Sign in using our secure server

Sincerely,
Amazon Security Department

Updating Subscriptions and Communication Preferences

You can access your New for You subscriptions, Special Occasion Reminders, Available to order notifications, and other communication preferences directly through Your Account.

When logging in, remember to enter the e-mail address and password currently associated with your account. If you do not have a customer account, we'll ask you to create one first. Simply enter your e-mail address, indicate that you are a new customer, and click the Sign in using our secure server button. On the next page, we'll ask you to enter your name and select a password.

Forgot Your Password?

We cannot tell you your current password, but we can certainly help you acquire a new one by sending a personalized link to your e-mail address. This way, you can securely change your password to whatever you want. If you visit us from a computer you have not used before, we will ask for complete verification of your account information before proceeding with the password change.Reset your password now.

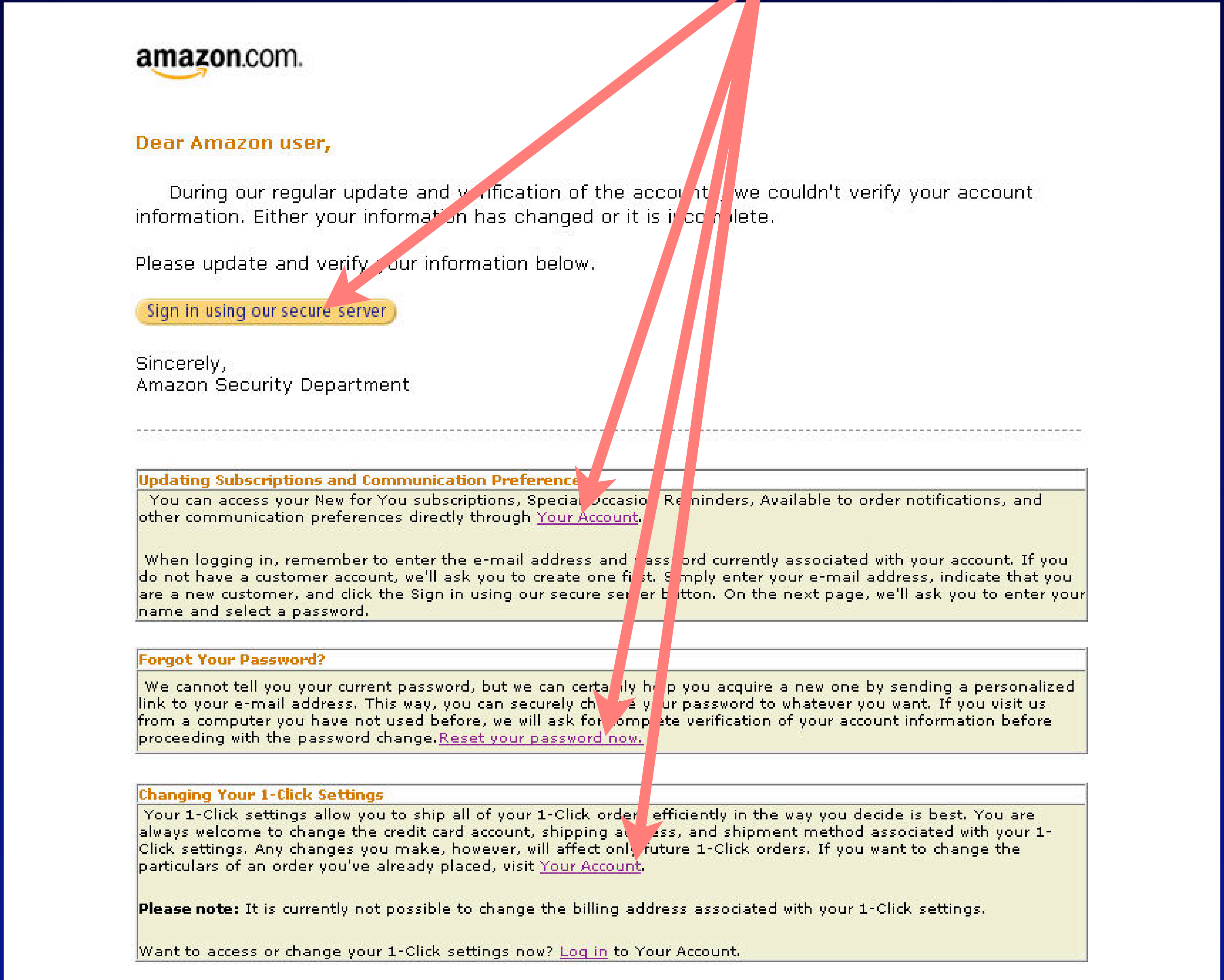
Changing Your 1-Click Settings

Your 1-Click settings allow you to ship all of your 1-Click orders efficiently in the way you decide is best. You are always welcome to change the credit card account, shipping address, and shipment method associated with your 1-Click settings. Any changes you make, however, will affect only future 1-Click orders. If you want to change the particulars of an order you've already placed, visit Your Account.

Please note: It is currently not possible to change the billing address associated with your 1-Click settings.

Want to access or change your 1-Click settings now? Log in to Your Account.

All links go to “http://www.amazon-department.com/exec/...” (IP 68.142.234.35)



amazon.com

Dear Amazon user,

During our regular update and verification of the accounts, we couldn't verify your account information. Either your information has changed or it is incomplete.

Please update and verify your information below.

Sign in using our secure server

Sincerely,
Amazon Security Department

Updating Subscriptions and Communication Preferences

You can access your New for You subscriptions, Special Occasion Reminders, Available to order notifications, and other communication preferences directly through Your Account.

When logging in, remember to enter the e-mail address and password currently associated with your account. If you do not have a customer account, we'll ask you to create one first. Simply enter your e-mail address, indicate that you are a new customer, and click the Sign in using our secure server button. On the next page, we'll ask you to enter your name and select a password.

Forgot Your Password?

We cannot tell you your current password, but we can certainly help you acquire a new one by sending a personalized link to your e-mail address. This way, you can securely change your password to whatever you want. If you visit us from a computer you have not used before, we will ask for complete verification of your account information before proceeding with the password change. Reset your password now.

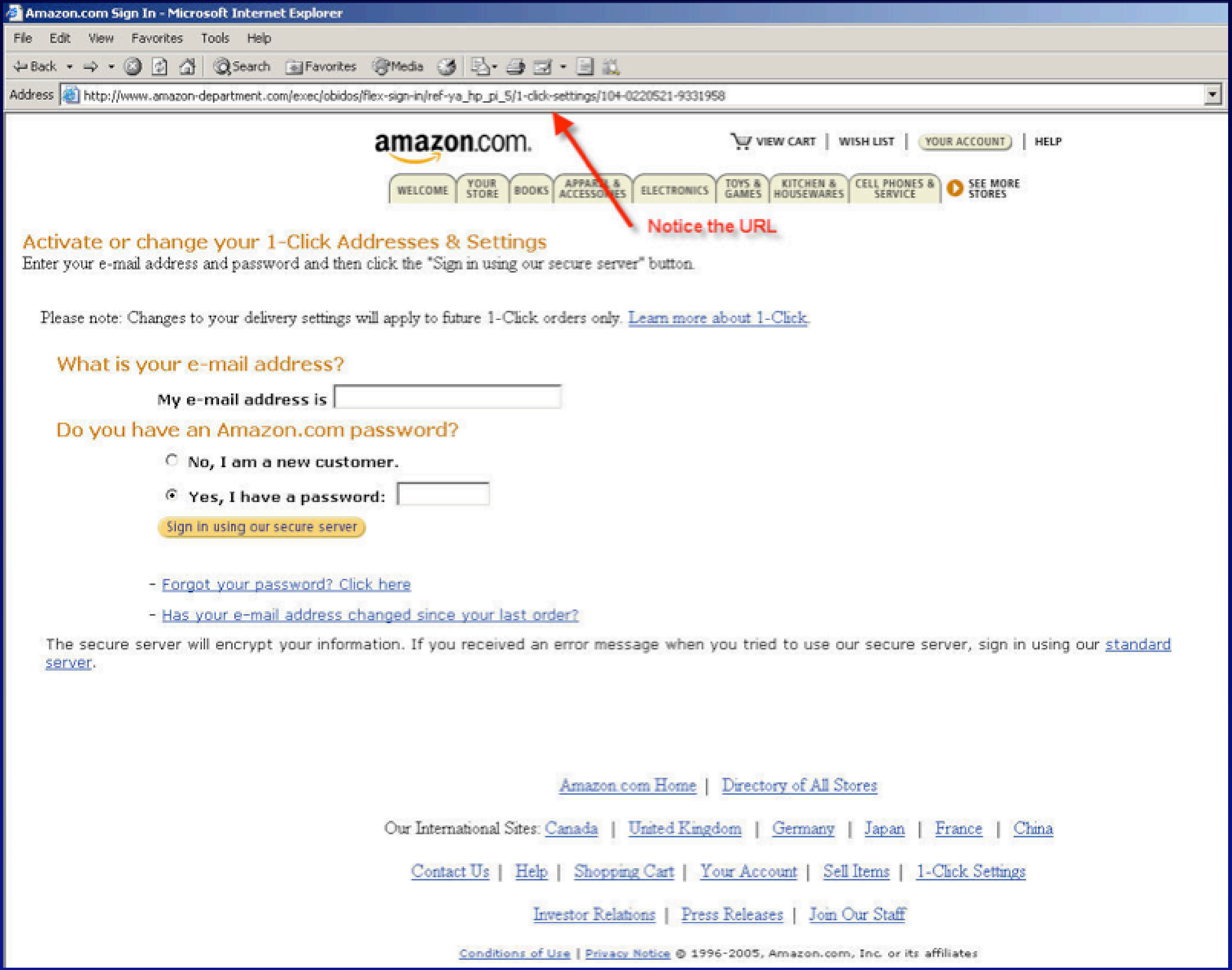
Changing Your 1-Click Settings

Your 1-Click settings allow you to ship all of your 1-Click orders efficiently in the way you decide is best. You are always welcome to change the credit card account, shipping address, and shipment method associated with your 1-Click settings. Any changes you make, however, will affect only future 1-Click orders. If you want to change the particulars of an order you've already placed, visit Your Account.

Please note: It is currently not possible to change the billing address associated with your 1-Click settings.

Want to access or change your 1-Click settings now? Log in to Your Account.

Looks realistic but “http”, not “https”


Amazon.com Sign In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
amazon.com.
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
WELCOME
YOUR STORE
BOOKS
APPAREL & ACCESSORIES
ELECTRONICS
TOYS & GAMES
KITCHEN & HOUSEWARES
CELL PHONES & SERVICE
SEE MORE STORES
Sign in using our secure server

http://www.amazon-department.com/exec/obidos/flex-sign-in/ref-ya_hp_pi_5/1-click-settings/104-0220521-9331958

Notice the URL

Activate or change your 1-Click Addresses & Settings

Enter your e-mail address and password and then click the "Sign in using our secure server" button.

Please note: Changes to your delivery settings will apply to future 1-Click orders only. Learn more about 1-Click.

What is your e-mail address?

My e-mail address is

Do you have an Amazon.com password?

○ No, I am a new customer.

● Yes, I have a password:

- Forgot your password? Click here
- Has your e-mail address changed since your last order?

The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.

Amazon.com Home | Directory of All Stores

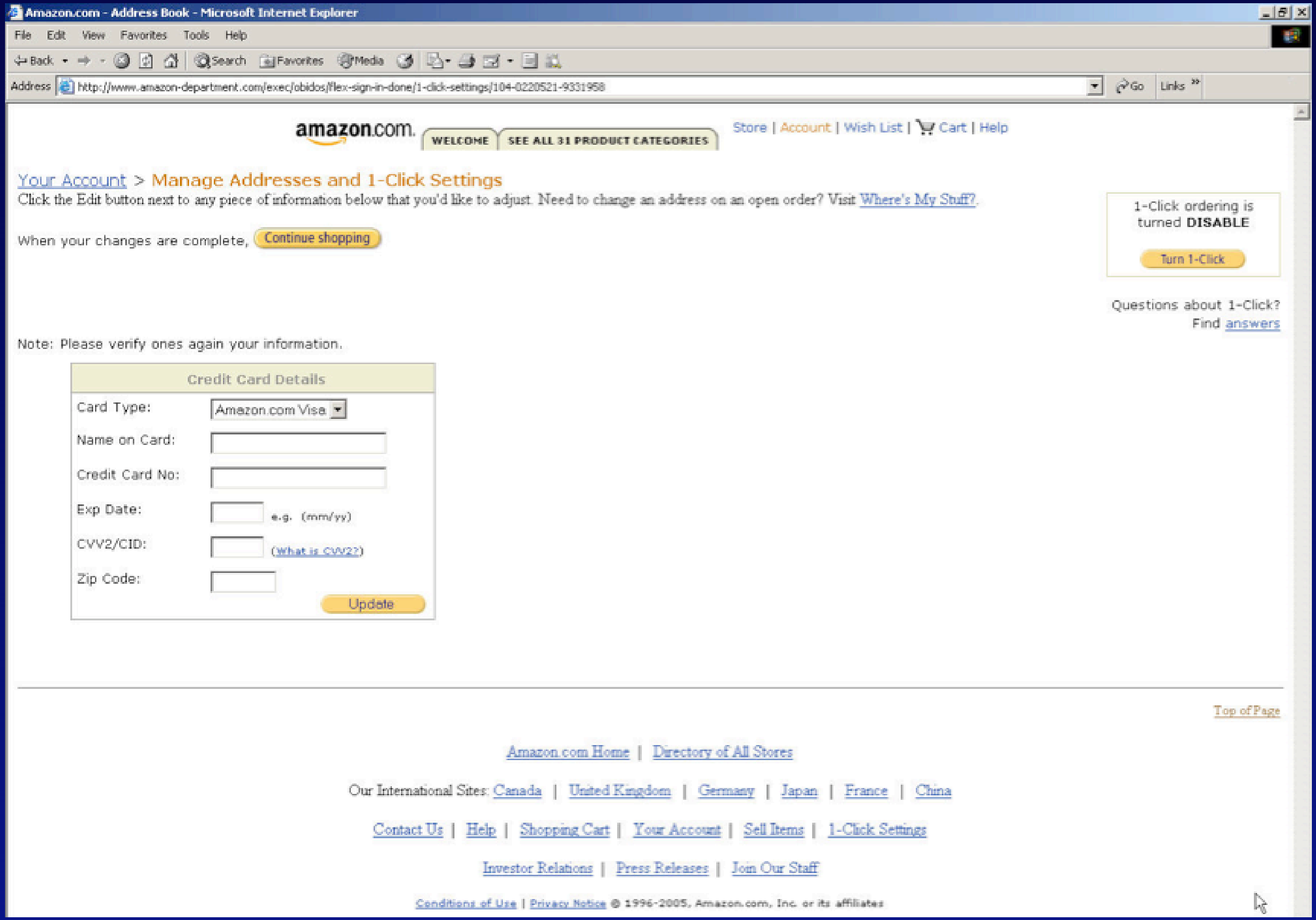
Our International Sites: Canada | United Kingdom | Germany | Japan | France | China

Contact Us | Help | Shopping Cart | Your Account | Sell Items | 1-Click Settings

Investor Relations | Press Releases | Join Our Staff

Conditions of Use | Privacy Notice © 1996-2005, Amazon.com, Inc. or its affiliates

Next page looks real too, asking for credit card info



Amazon.com - Address Book - Microsoft Internet Explorer

Address http://www.amazon-department.com/exec/obidos/flex-sign-in-done/1-click-settings/104-0220521-9331958

Your Account > Manage Addresses and 1-Click Settings

Click the Edit button next to any piece of information below that you'd like to adjust. Need to change an address on an open order? Visit Where's My Stuff?.

When your changes are complete,

1-Click ordering is turned **DISABLE**

Questions about 1-Click? Find answers

Note: Please verify ones again your information.

Credit Card Details

Card Type:	Amazon.com Visa
Name on Card:	
Credit Card No:	
Exp Date:	e.g. (mm/yy)
CVV2/CID:	(What is CVV2?)
Zip Code:	

Amazon.com Home | Directory of All Stores

Our International Sites: Canada | United Kingdom | Germany | Japan | France | China

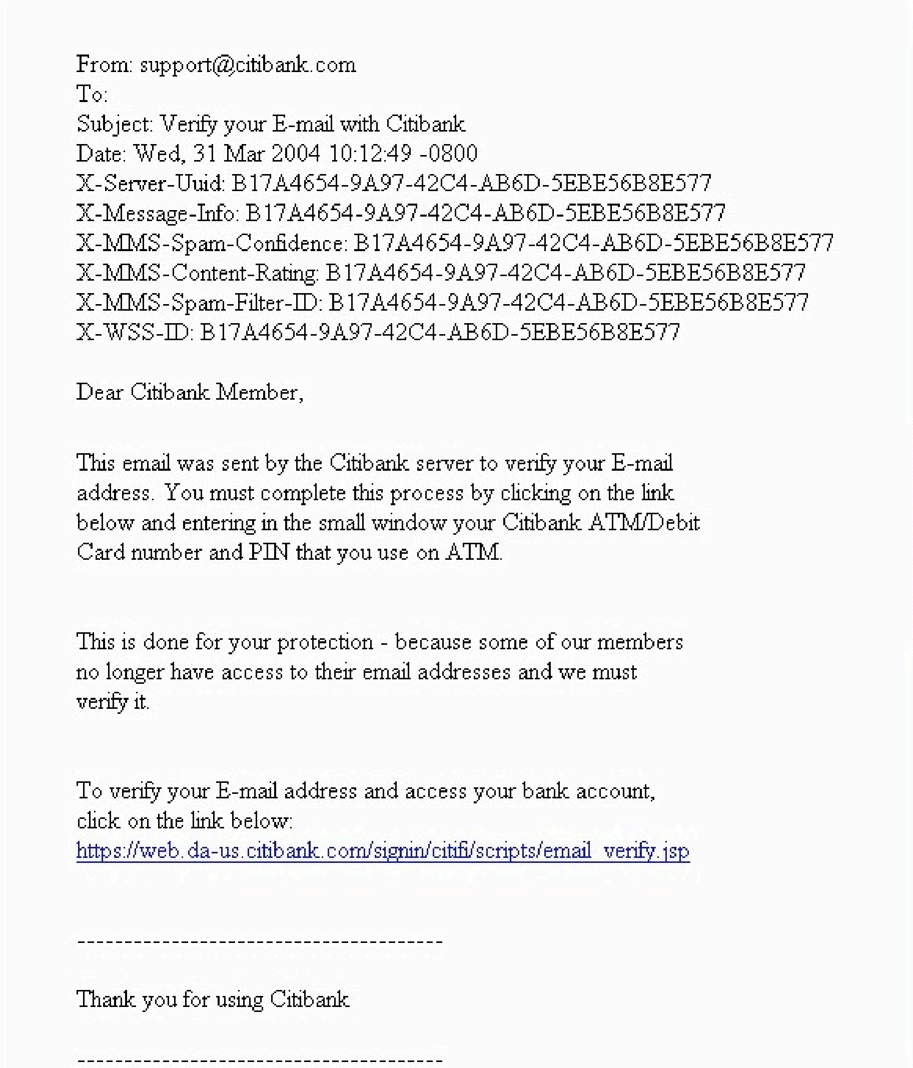
Contact Us | Help | Shopping Cart | Your Account | Sell Items | 1-Click Settings

Investor Relations | Press Releases | Join Our Staff

Conditions of Use | Privacy Notice © 1996-2005, Amazon.com, Inc. or its affiliates

Finally user is redirected to real Amazon site

Example 4: generic, plain email asks to verify Citibank account info.



From: support@citibank.com
To:
Subject: Verify your E-mail with Citibank
Date: Wed, 31 Mar 2004 10:12:49 -0800
X-Server-Uuid: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-Message-Info: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Confidence: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Content-Rating: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Filter-ID: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-WSS-ID: B17A4654-9A97-42C4-AB6D-5EBE56B8E577

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

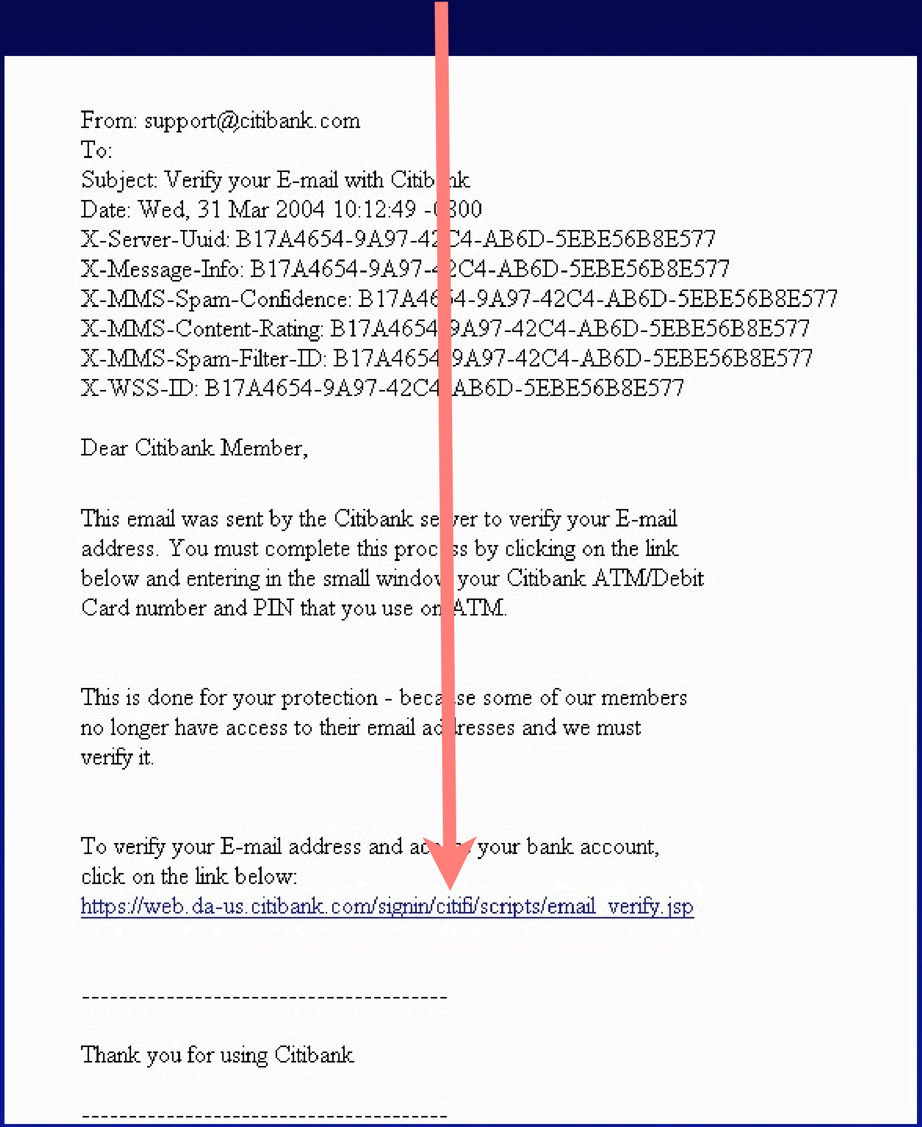
This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

----

Thank you for using Citibank

Link to “https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp” actually goes to IP address 69.65.202.82 (registered to ThePlanet Internet Services)



From: support@citibank.com
To:
Subject: Verify your E-mail with Citibank
Date: Wed, 31 Mar 2004 10:12:49 -0800
X-Server-Uuid: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-Message-Info: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Confidence: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Content-Rating: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Filter-ID: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-WSS-ID: B17A4654-9A97-42C4-AB6D-5EBE56B8E577

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

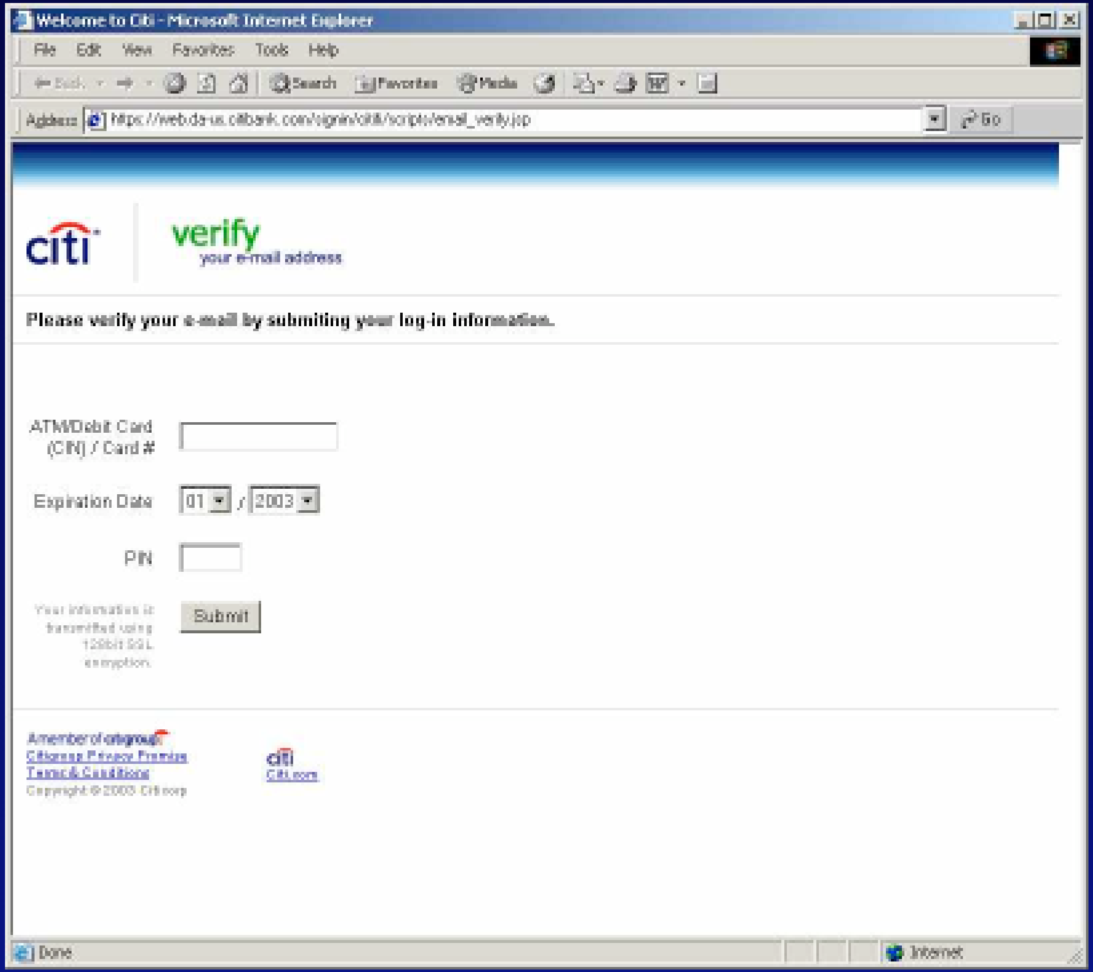
This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

----

Thank you for using Citibank

Convincing address bar shows "https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp"


Welcome to Citi - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp
Go
citi
Done
Internet

verify
your e-mail address

Please verify your e-mail by submiting your log-in information.

ATM/Debit Card (CIN) / Card #

Expiration Date 01 / 2003

PIN

Your information is transmitted using 128bit SSL encryption.

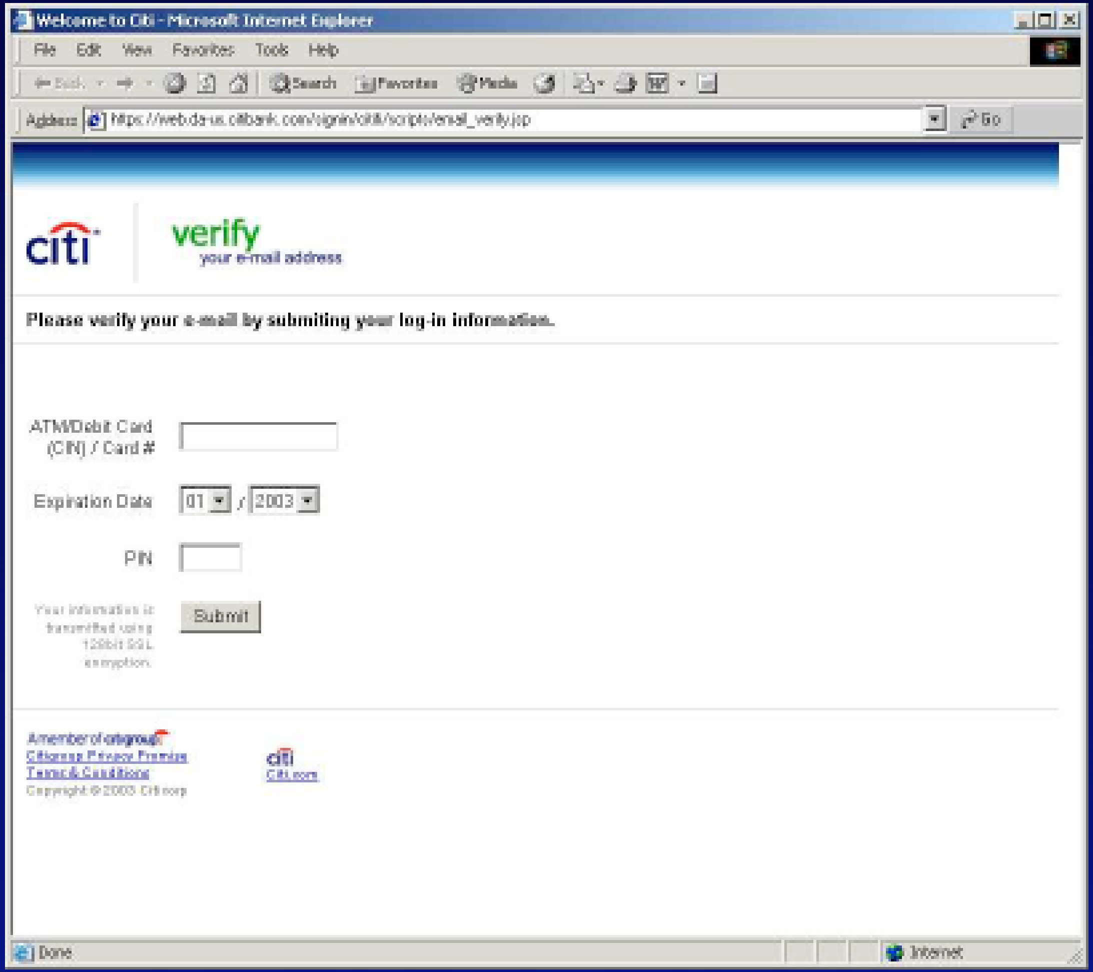
Submit

A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

citi
Citi.com

But real address bar is actually covered by a fake address bar graphic using Javascript and frames

Clue: "https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp" should be secure HTTP


Welcome to Citi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
citi
Submit
Done
Internet

https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

verify
your e-mail address

Please verify your e-mail by submiting your log-in information.

ATM/Debit Card (CIN) / Card #

Expiration Date 01 / 2003

PIN

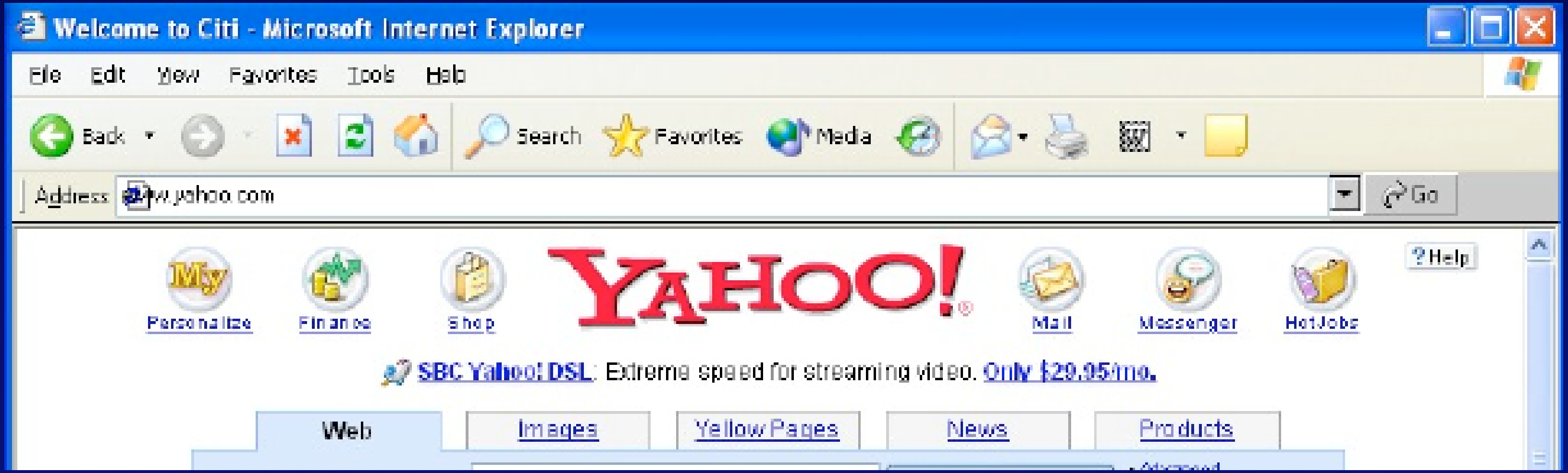
Your information is transmitted using 128bit SSL encryption.

A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

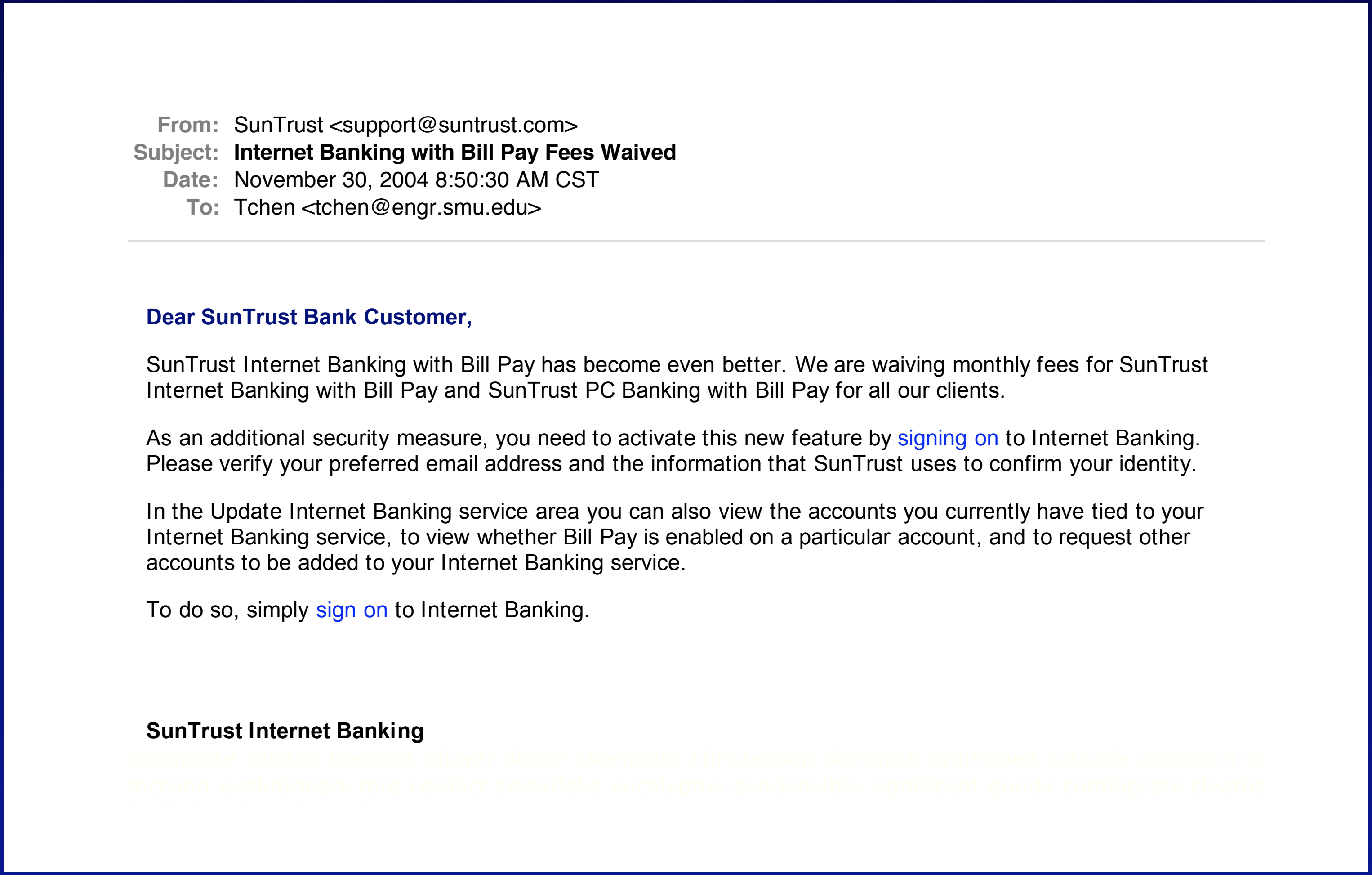
Citi.com

But browser does not show padlock icon at bottom

Another clue: going to another URL (Yahoo) still shows top frame that says "Welcome to Citi"


Welcome to Citi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
w.yahoo.com
Go
Personalize
Finance
Shop
YAHOO!
Mail
Messenger
HotJobs
? Help
SBC Yahoo! DSL: Extreme speed for streaming video. Only $29.95/mo.
Web
Images
Yellow Pages
News
Products

Example 5: email from SunTrust Bank promotes fee waiver but feature must be activated at Website



From: SunTrust <support@suntrust.com>
Subject: **Internet Banking with Bill Pay Fees Waived**
Date: November 30, 2004 8:50:30 AM CST
To: Tchen <tchen@engr.smu.edu>

Dear SunTrust Bank Customer,

SunTrust Internet Banking with Bill Pay has become even better. We are waiving monthly fees for SunTrust Internet Banking with Bill Pay and SunTrust PC Banking with Bill Pay for all our clients.

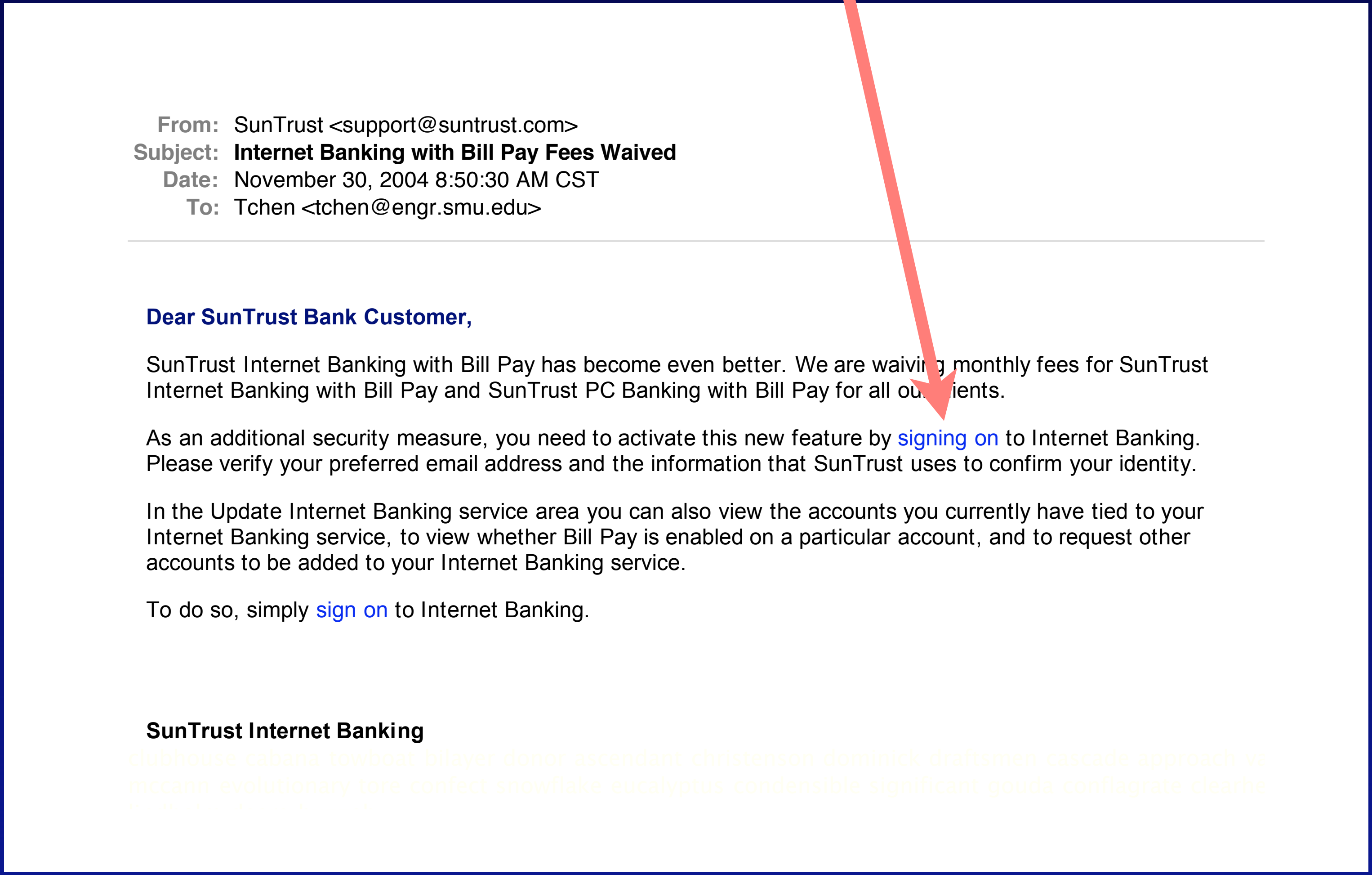
As an additional security measure, you need to activate this new feature by signing on to Internet Banking. Please verify your preferred email address and the information that SunTrust uses to confirm your identity.

In the Update Internet Banking service area you can also view the accounts you currently have tied to your Internet Banking service, to view whether Bill Pay is enabled on a particular account, and to request other accounts to be added to your Internet Banking service.

To do so, simply sign on to Internet Banking.

SunTrust Internet Banking

Link calls "www.people-online.net" at IP address 196.40.75.39 (in Costa Rica)



From: SunTrust <support@suntrust.com>
Subject: **Internet Banking with Bill Pay Fees Waived**
Date: November 30, 2004 8:50:30 AM CST
To: Tchen <tchen@engr.smu.edu>

Dear SunTrust Bank Customer,

SunTrust Internet Banking with Bill Pay has become even better. We are waiving monthly fees for SunTrust Internet Banking with Bill Pay and SunTrust PC Banking with Bill Pay for all our clients.

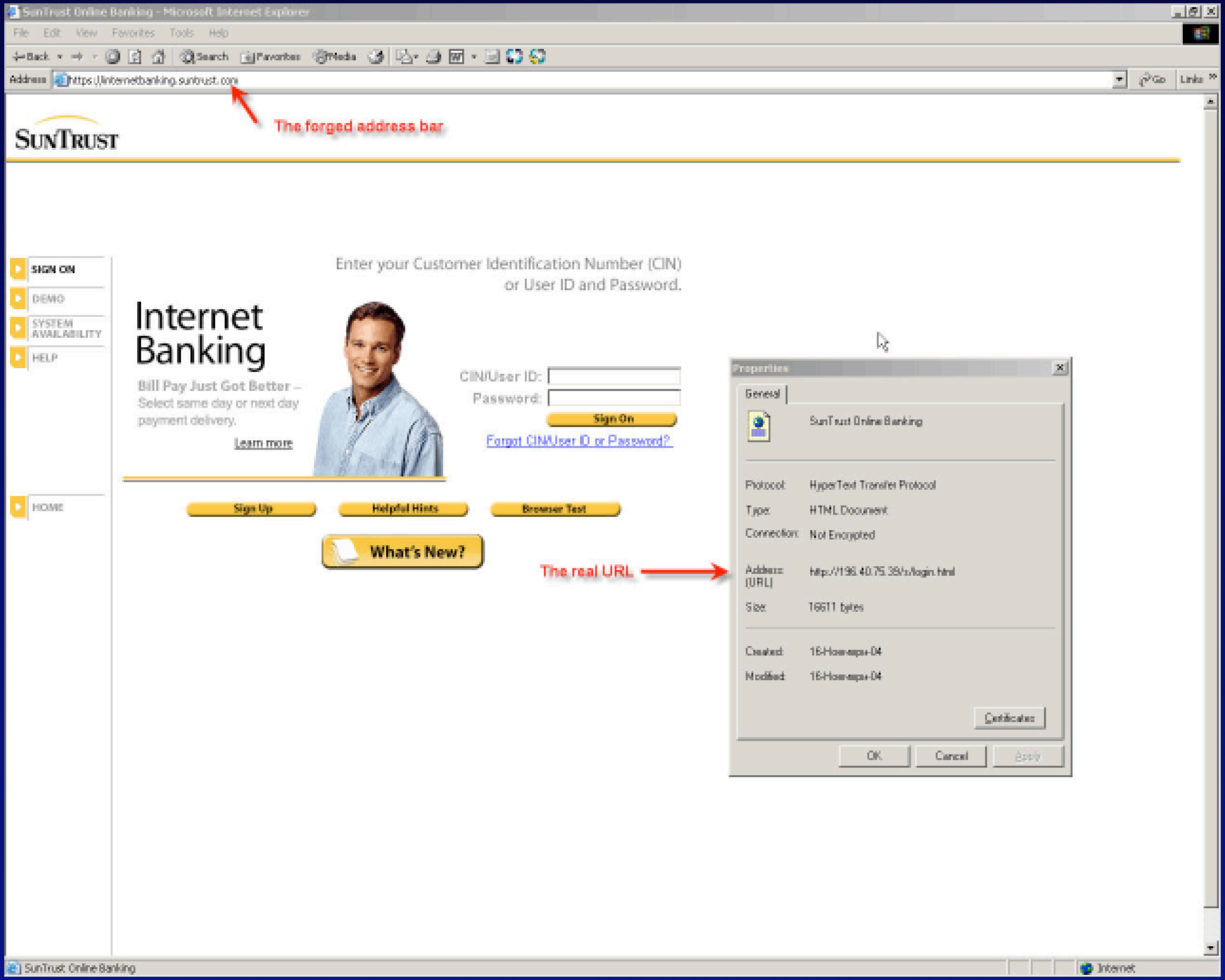
As an additional security measure, you need to activate this new feature by signing on to Internet Banking. Please verify your preferred email address and the information that SunTrust uses to confirm your identity.

In the Update Internet Banking service area you can also view the accounts you currently have tied to your Internet Banking service, to view whether Bill Pay is enabled on a particular account, and to request other accounts to be added to your Internet Banking service.

To do so, simply sign on to Internet Banking.

SunTrust Internet Banking

Convincingly forged IE address bar shows “https://internetbanking.suntrust.com”



Address https://internetbanking.suntrust.com

The forged address bar

Enter your Customer Identification Number (CIN) or User ID and Password.

Internet Banking

Bill Pay Just Got Better – Select same day or next day payment delivery.

Learn more

CIN/User ID:

Password:

Sign On

Forgot CIN/User ID or Password?

The real URL

Properties

General

SunTrust Online Banking

Protocol: HyperText Transfer Protocol

Type: HTML Document

Connection: Not Encrypted

Address (URL): http://196.40.75.39/s/login.html

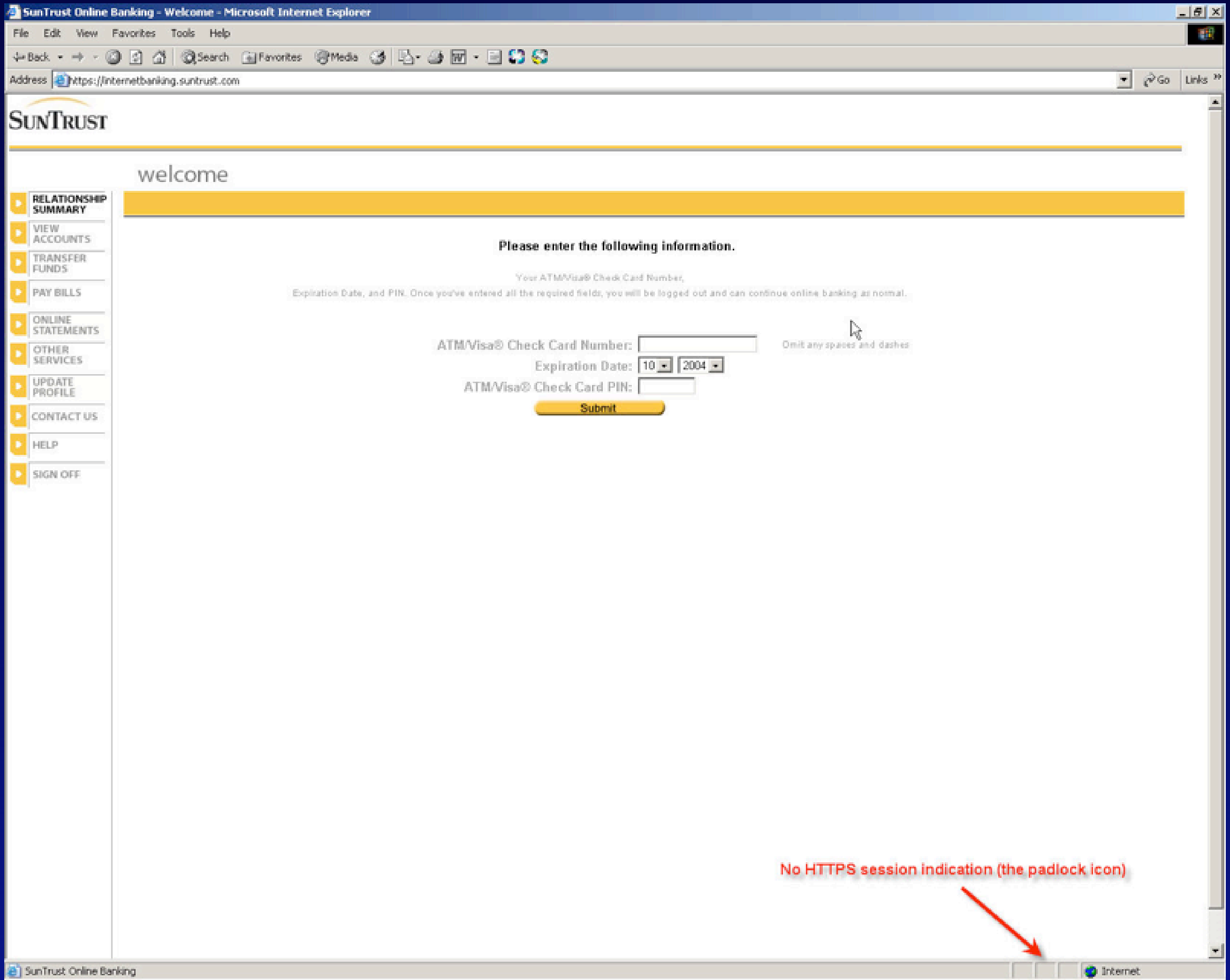
Size: 16611 bytes

Created: 16-[illegible]-04

Modified: 16-[illegible]-04

Properties page show real URL is “http://196.40.75.39/s/login.html”

After user logs in, Website asks for ATM/Visa check card info



Please enter the following information.

Your ATM/Visa® Check Card Number,
Expiration Date, and PIN. Once you've entered all the required fields, you will be logged out and can continue online banking as normal.

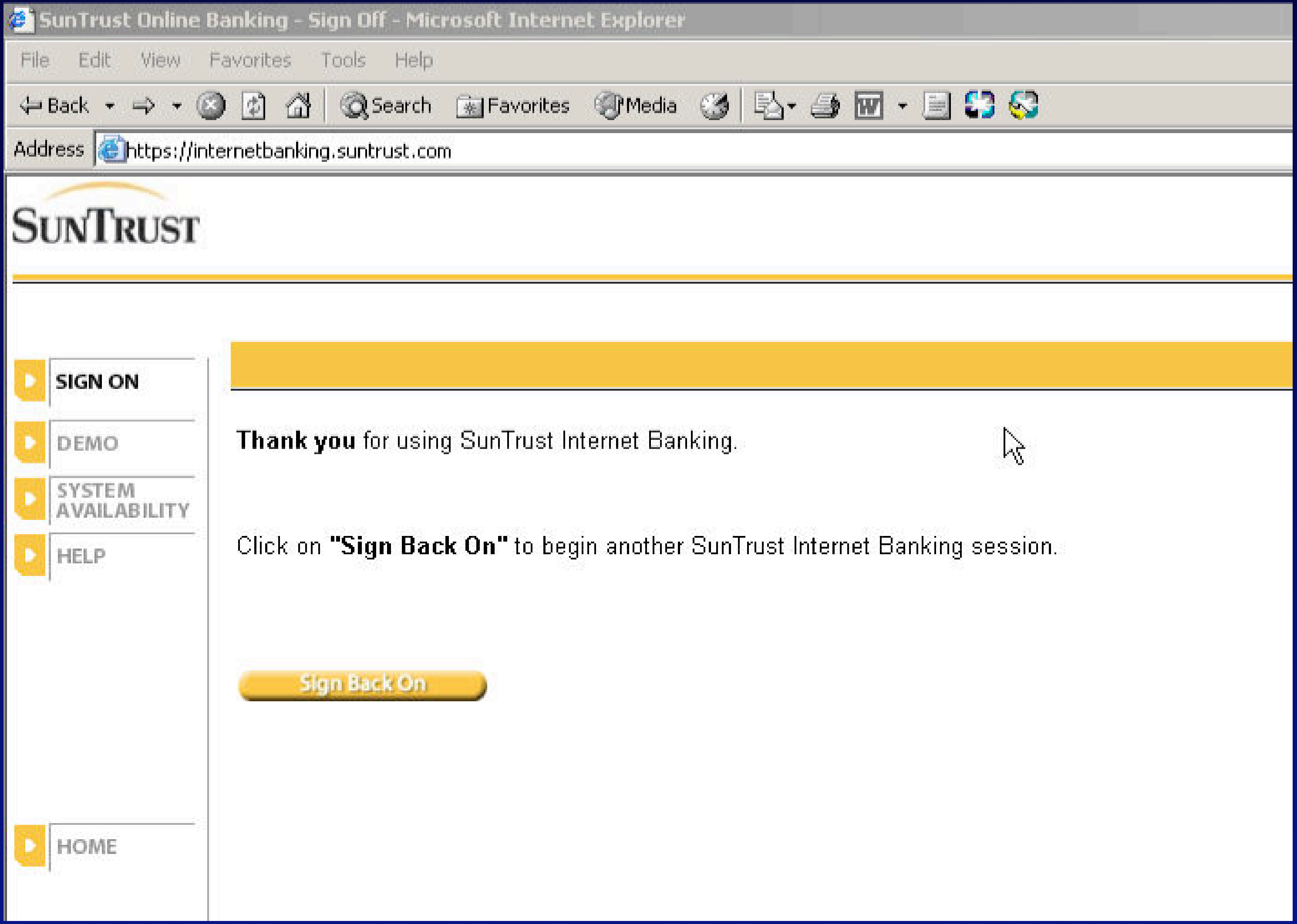
ATM/Visa® Check Card Number:		Omit any spaces and dashes
Expiration Date:	10 2004	
ATM/Visa® Check Card PIN:		

Submit

No HTTPS session indication (the padlock icon)

IE status bar does not show secure HTTP session

Final "log-out" page...



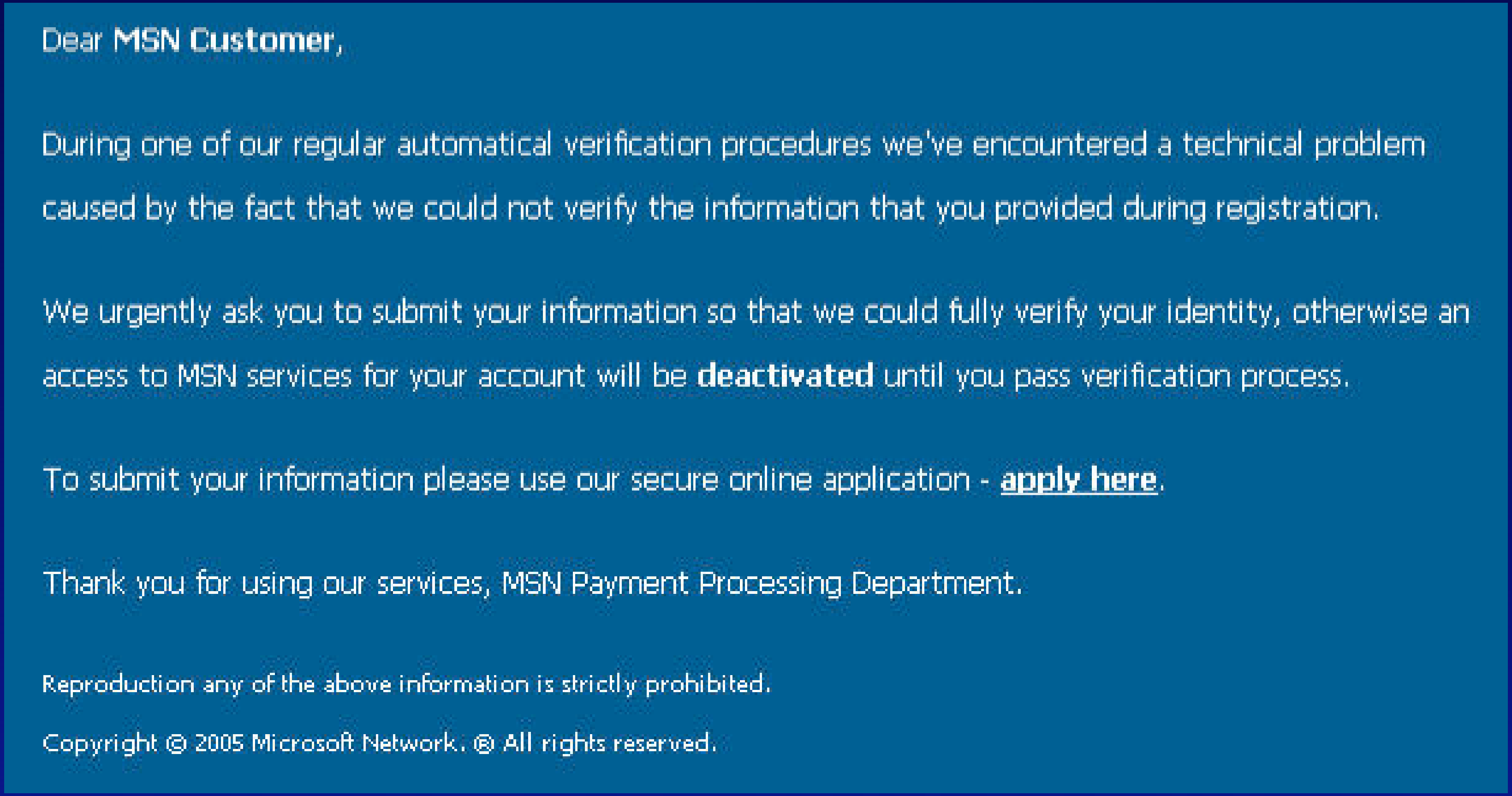
SunTrust Online Banking - Sign Off - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://internetbanking.suntrust.com
SUNTRUST
SIGN ON
DEMO
SYSTEM AVAILABILITY
HELP
HOME
Sign Back On

Thank you for using SunTrust Internet Banking.

Click on **"Sign Back On"** to begin another SunTrust Internet Banking session.

Finally user is redirected to real "suntrust.com" site

Example 6: e-mail from MSN looks normal asking for verification of account...



Dear **MSN Customer**,

During one of our regular automatical verification procedures we've encountered a technical problem caused by the fact that we could not verify the information that you provided during registration.

We urgently ask you to submit your information so that we could fully verify your identity, otherwise an access to MSN services for your account will be **deactivated** until you pass verification process.

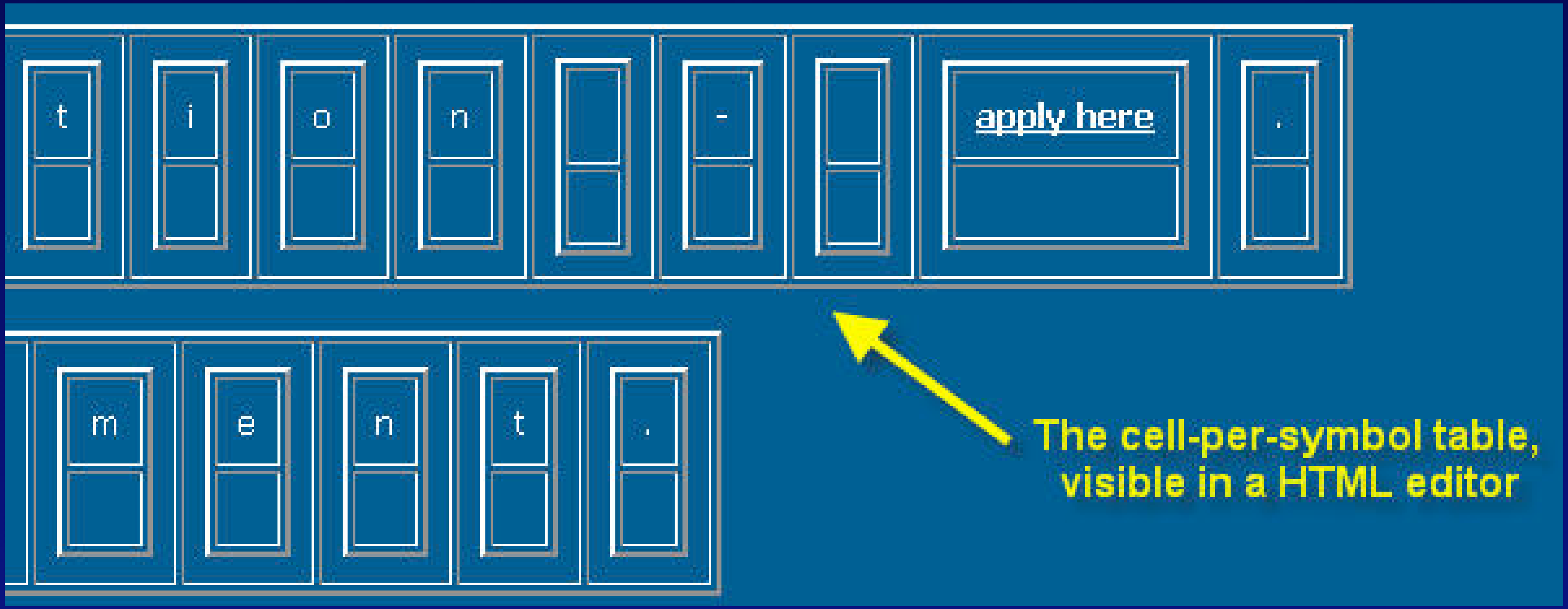
To submit your information please use our secure online application - **apply here**.

Thank you for using our services, MSN Payment Processing Department.

Reproduction any of the above information is strictly prohibited.

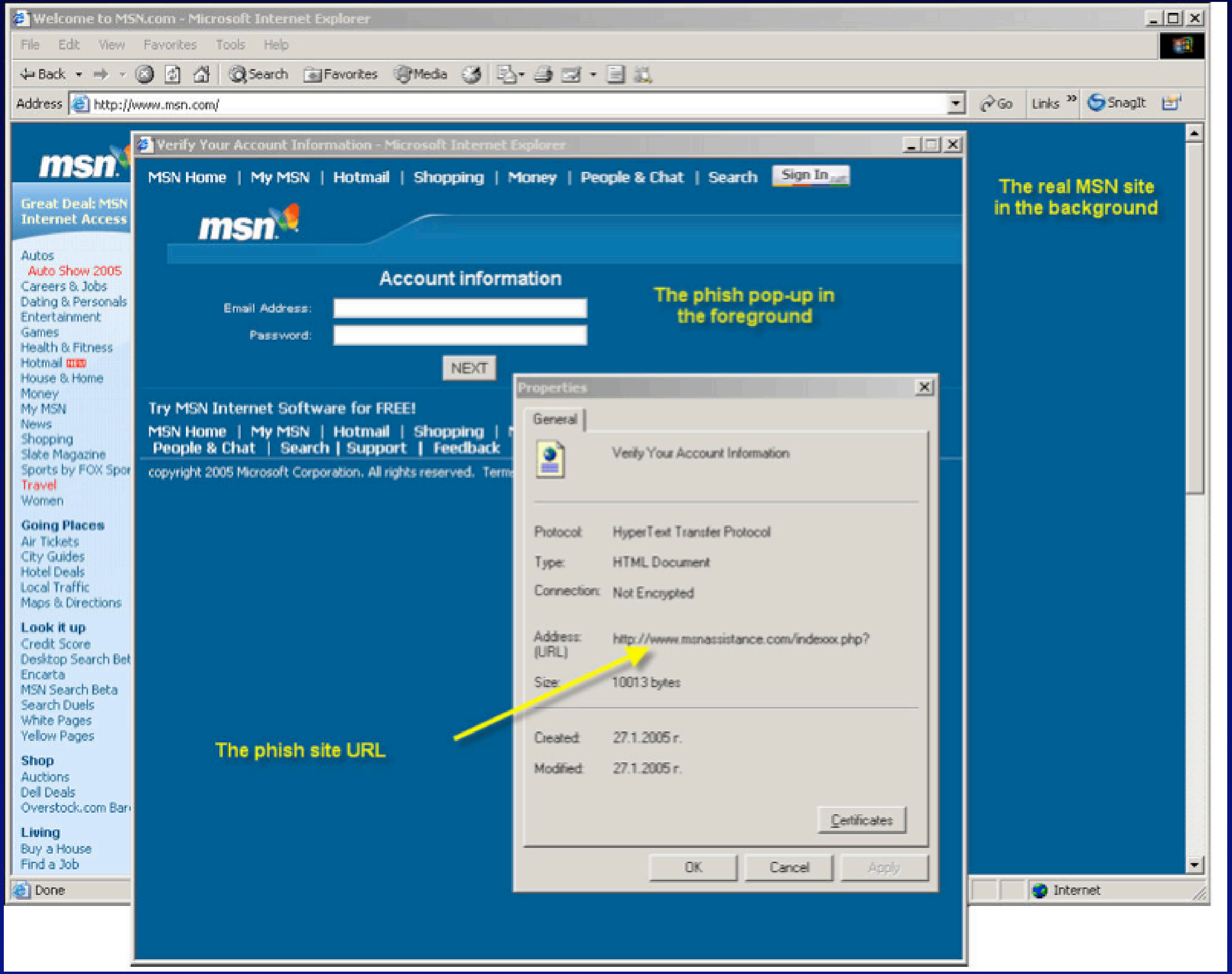
Copyright © 2005 Microsoft Network. ® All rights reserved.

In HTML editor, text is actually an HTML table with letters in separate cells - to avoid spam filters



The cell-per-symbol table, visible in a HTML editor

Phish page opens in front of real MSN page, looking very similar



Welcome to MSN.com - Microsoft Internet Explorer

Address http://www.msn.com/

Verify Your Account Information - Microsoft Internet Explorer

Account information

Email Address:

Password:

Try MSN Internet Software for FREE!

copyright 2005 Microsoft Corporation. All rights reserved.

Properties

Verify Your Account Information

Protocol: HyperText Transfer Protocol

Type: HTML Document

Connection: Not Encrypted

Address: (URL) http://www.msnassistance.com/indexxx.php?

Size: 10013 bytes

Created: 27.1.2005 г.

Modified: 27.1.2005 г.

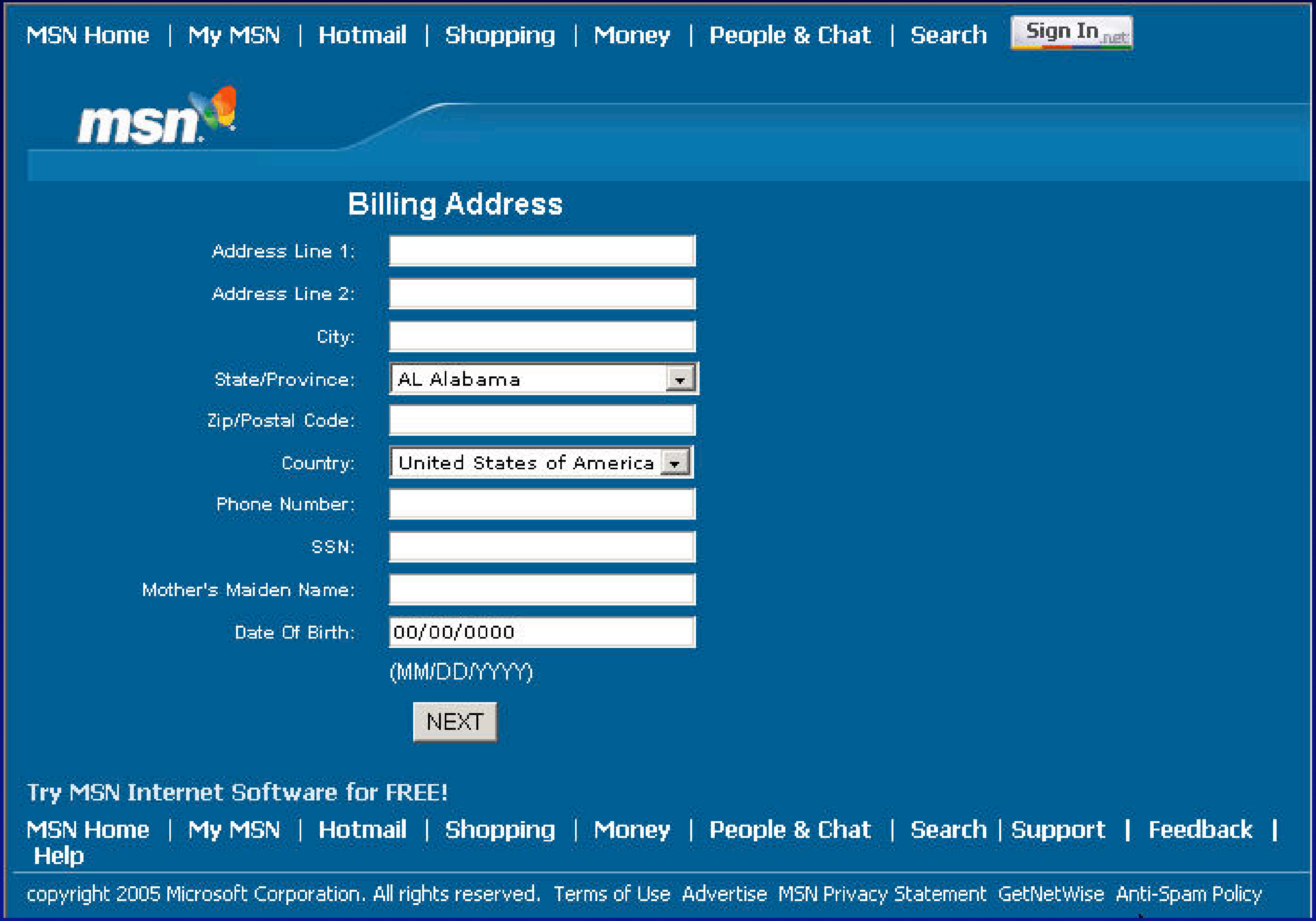
The real MSN site in the background

The phish pop-up in the foreground

The phish site URL

Phish page has no address bar to reveal actual URL, which is "www.msnassistance.com"

Next page asks for personal info...


MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search
Sign In .net
msn

Billing Address

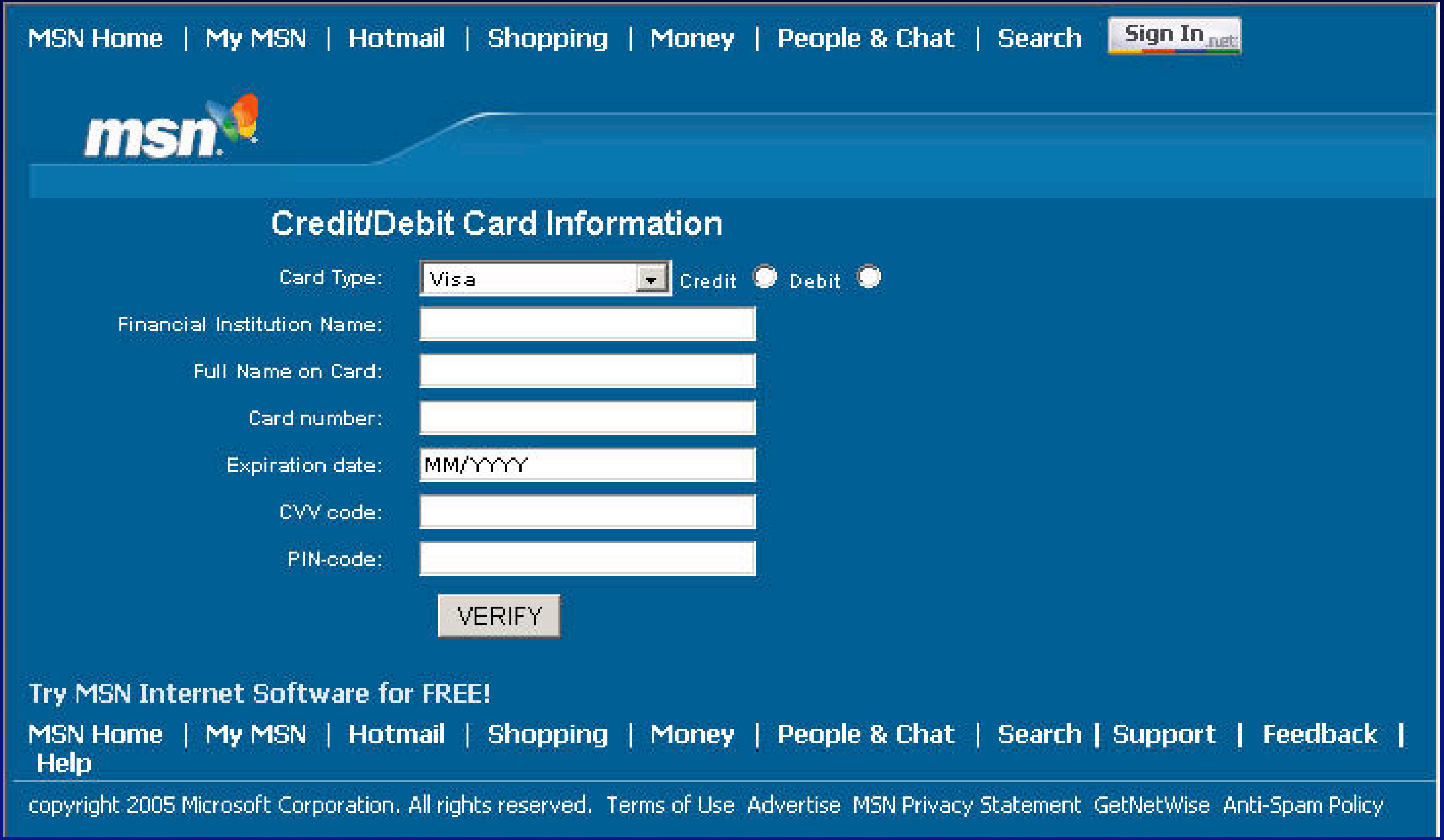
Address Line 1:	
Address Line 2:	
City:	
State/Province:	AL Alabama
Zip/Postal Code:	
Country:	United States of America
Phone Number:	
SSN:	
Mother's Maiden Name:	
Date Of Birth:	00/00/0000
	(MM/DD/YYYY)

Try MSN Internet Software for FREE!

MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search | Support | Feedback | Help

copyright 2005 Microsoft Corporation. All rights reserved. Terms of Use Advertise MSN Privacy Statement GetNetWise Anti-Spam Policy

Next page asks for credit card info...



MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search | Sign In .net

msn

Credit/Debit Card Information

Card Type:	Visa ▾ Credit ○ Debit ○
Financial Institution Name:	
Full Name on Card:	
Card number:	
Expiration date:	MM/YYYY
CVV code:	
PIN-code:	

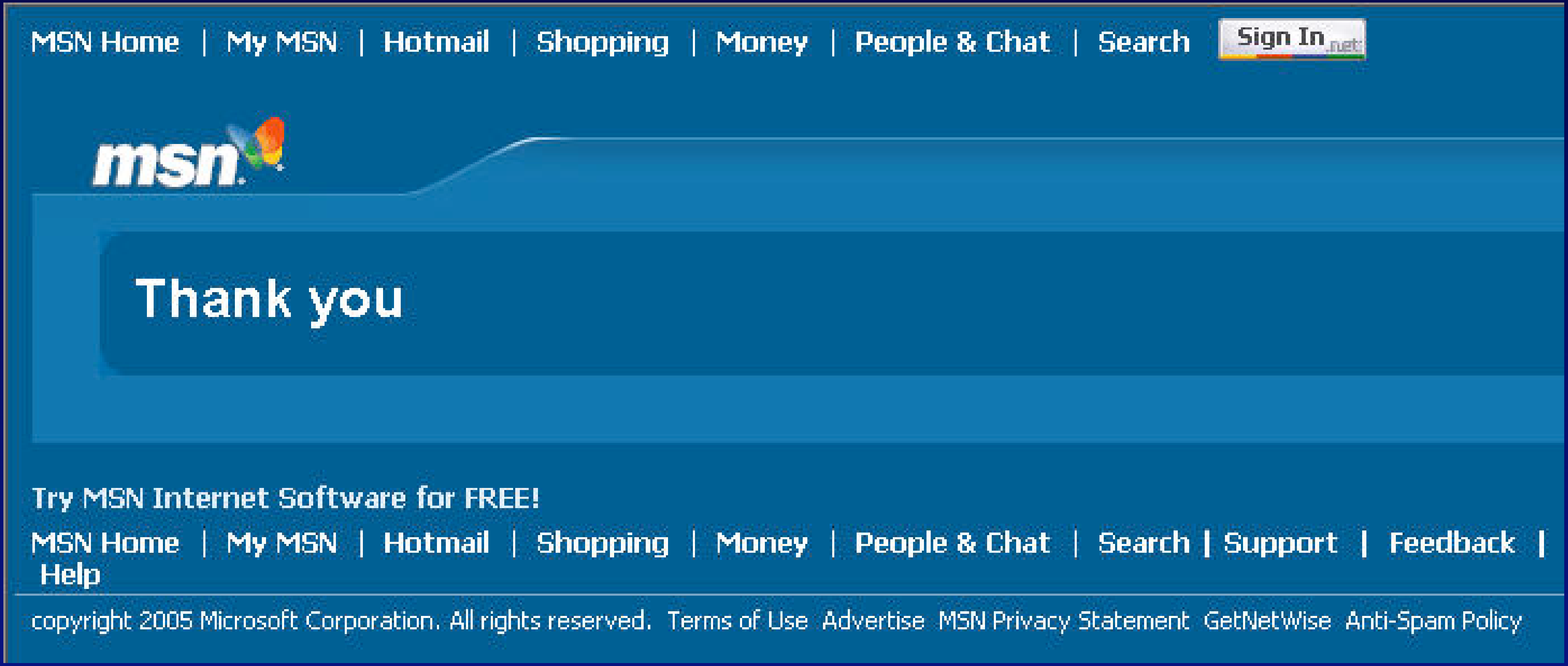
VERIFY

Try MSN Internet Software for FREE!

MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search | Support | Feedback | Help

copyright 2005 Microsoft Corporation. All rights reserved. Terms of Use Advertise MSN Privacy Statement GetNetWise Anti-Spam Policy

Final log-out page...



MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search
Sign In .net
msn

Thank you

Try MSN Internet Software for FREE!

MSN Home | My MSN | Hotmail | Shopping | Money | People & Chat | Search | Support | Feedback | Help

copyright 2005 Microsoft Corporation. All rights reserved. Terms of Use Advertise MSN Privacy Statement GetNetWise Anti-Spam Policy

Motivations

- Easy profits:
  - Phishing e-mails (like spam) are low cost to hit millions of people
  - Social engineering attack is low tech and easy to craft
  - Easy to register and set up phishing Websites (and move later)
  - Even low success rate (3% or perhaps higher) can be very profitable

Motivations (cont)

- Low risk
  - Phishing e-mail often sent through compromised “zombies” or open mail relays are hard to trace
  - Phishing Websites are registered with phony info and moved around frequently to different IP addresses

Risks and Threats

- Identity theft
  - Stolen bank accounts, passwords/PINs, social security numbers, addresses, credit card numbers
- Websites can exploit browser vulnerabilities to download malicious code (viruses, Trojan horses, spyware) to victim PCs

Defenses

- User education and awareness
  - Humans are weakest part of defenses
- Commercial products and services
  - Coordination groups
  - Spamtraps
  - Managed e-mail services
  - Fraud detection
  - Browser toolbars

User Awareness

- Users should look for telltale signs of phishing email
  - Lack of personalization, suspicious URLs, attachments, random or misspelled words, bad grammar, urgent tone
- Users should manually type URLs in browser, stay with known Websites, do not open attachments, check for known scams, use secure HTTPS connections

User Awareness (cont)

- But phishers have many tricks to fool even cautious users
  - HTML email can look like plain text and hide Javascript or invisible content
  - Similar URLs can be easily crafted by “1” instead of “l”, or “0” instead of “O”
  - Similar domain names can be registered
    - “mybank.com” could be confused with “mybank.com.us” or “mybank.fake.com”

User Awareness (cont)

- Many tricks (cont)
  - Host name obfuscation, eg, “http://mybank.com:login@210.10.3.5/index.htm” actually goes to IP address 210.10.3.5, not mybank.com
  - HTML allows graphics or complete pages to cover underlying pages
- Increasing user awareness will not be effective solution

Coordination Groups

- Anti-Phishing Working Group includes 706 financial institutions, online retailers, ISPs, law enforcement agencies
  - Collects voluntary submissions of phishing, analyzes examples, tracks statistics, raises public awareness
- Digital PhishNet includes Microsoft, AOL, Verisign, FBI, Secret Service
  - To coordinate info and shut down Websites

Coordination Groups (cont)

- Phish Report Network includes Microsoft, eBay, Visa, WholeSecurity
  - Collects submissions of new attacks, issue alerts to subscribers
- Trusted Electronic Communications Forum includes IBM, Fidelity, Charles Schwab, retailers, telecom companies
  - To find technological solutions, promote best practices, pursue legal action against

Spamtraps

- Spamtraps (e-mail honeypots) are computers loaded with fake e-mail accounts
  - Fake e-mail accounts are not used for legitimate purposes
  - Virtually all e-mail to spamtraps is spam
  - Spam is analyzed manually and automatically for new phishing attacks
  - Links lead to phishing Websites

Websense

- Websense Security Labs mines and analyzes over 24 million Websites daily
- Operates global honeynet (network of honeypots) to discover new attacks
- Software for client companies to automatically report suspicious Websites for analysis
- Classifies and reports threats to clients

Webwasher

- Operates honeypots to collect spam and analyze new phishing attacks
- Maintains database of known fraudulent sites
- Webwasher URL Filter blocks known fraudulent sites
- Webwasher AntiSpam filters e-mail for spam

NameProtect

- Working with MasterCard to detect phishing attacks in real time
- Continually monitors Websites, domain names, spam e-mail, to detect trademark or copyright infringement and fraudulent sites

Cyota

- FraudAction analyzes data from various probes, spamtraps, partners, to detect new phishing attacks
- Analysts create risk assessment reports for each attack
- Send alerts to client banks

MarkMonitor

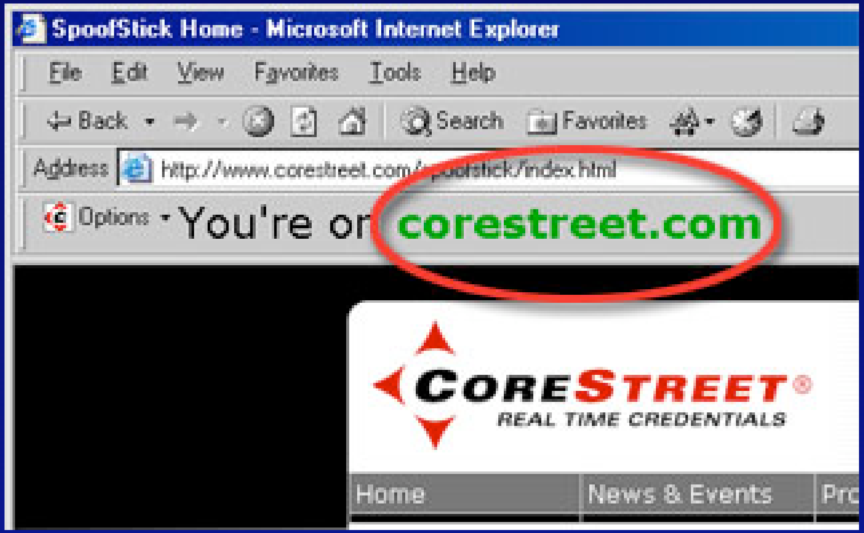
- Fraud Protection service analyzes data from honeypots to identify new attacks
- Monitors chat rooms, newsgroups, domain registries
- Correlates data to identify potential threats
- Alerts clients about high risk threats to corporate brands

WebRoot Phish Net

- Phish Net encrypts personal data on PC and alerts user if PC is transmitting personal info
- WebRoot also keeps blacklist of known fraudulent sites, compares to visited Website

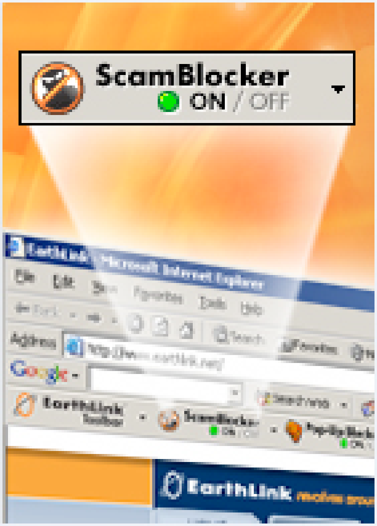
CoreStreet SpoofStick

- Toolbar prominently identifies real URL of visited Website
- Will not detect popups covering a legitimate site


SpoofStick Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.corestreet.com/spoofstick/index.html
Options You're on corestreet.com
CORESTREET
REAL TIME CREDENTIALS
Home News & Events Pro

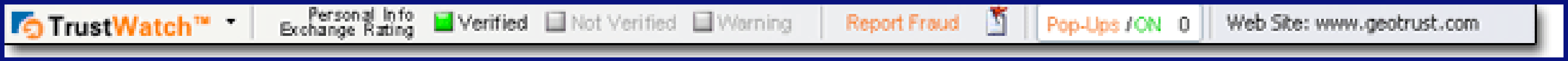
Earthlink ScamBlocker

- Earthlink keeps list of known fraudulent sites
- Browser toolbar prevents loading known sites, redirects to Earthlink's servers
- Depends on up-to-date list at Earthlink



GeoTrust TrustWatch

- GeoTrust rates Websites for trustworthiness and verifies by trusted third party
- Browser toolbar displays color code (green/yellow/red)



Conclusions

- Be very careful
  - New, more clever phishing scams can be expected
- Current defenses are educational and technological
  - Neither alone will be sufficient
  - Defenses are trying to keep up with attacks, not keep ahead