Desktop Security for Everyone

Tyler Farmer – tylerf@microsoft.com
Sr. Technology Specialist II
Education Solutions Group
Microsoft Corporation

Agenda

- State of the Industry today
- Viruses, Worms & Spies – oh my!
- How to Protect Yourself

State of the Industry Today

Threat Follows Value

The 1950s American bank robber Willie Sutton was asked why he robbed banks. He said he robbed banks because,

"That's where the money is."

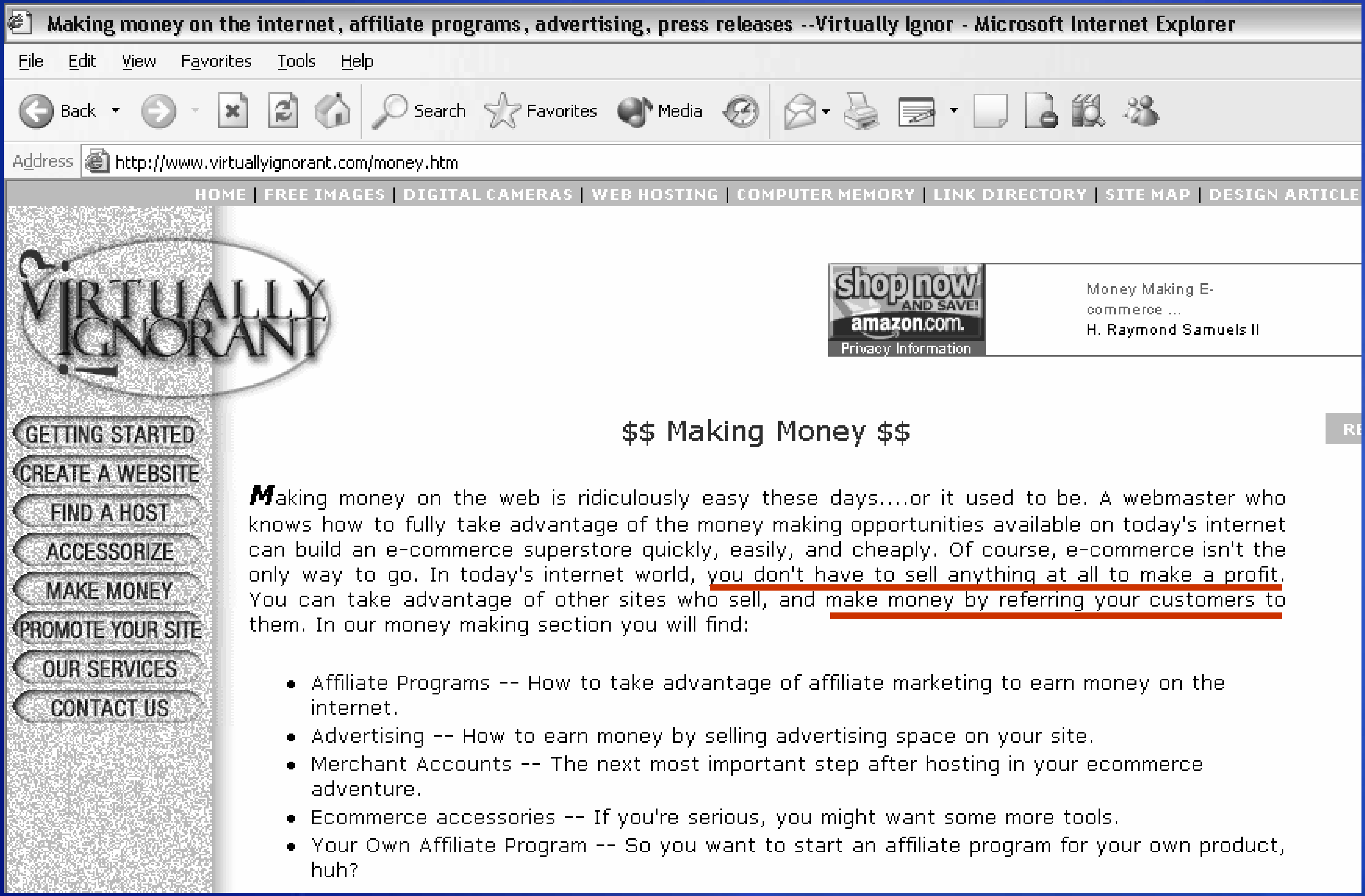
Today, the money is in Cyberspace

The Internet provides for criminals the two capabilities most required for the conduct of criminal activities: Anonymity & Mobility

Do The Math

- SoBig virus spammed mail to over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people
- If 1% of people who went to site signed up for 3-days free trial
  - = (100,000 people) x ($0.50) = $50,000
- If 1% of free trials sign up for 1 year
  - = (1,000 people) x ($144/yr) = $144,000/yr

Opportunities Are Limitless

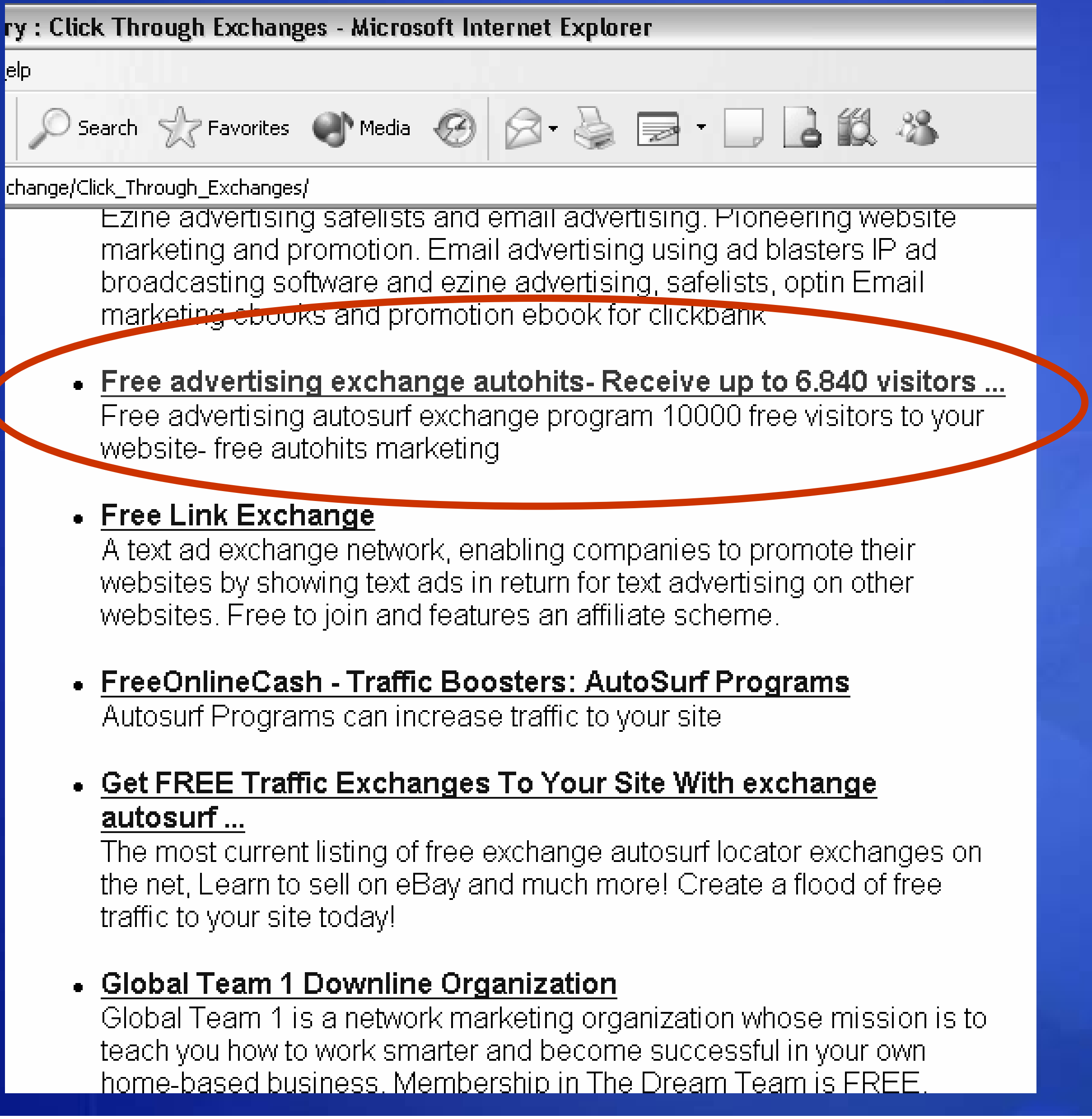

Making money on the internet, affiliate programs, advertising, press releases --Virtually Ignor - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.virtuallyignorant.com/money.htm
HOME | FREE IMAGES | DIGITAL CAMERAS | WEB HOSTING | COMPUTER MEMORY | LINK DIRECTORY | SITE MAP | DESIGN ARTICLE
VIRTUALLY IGNORANT
GETTING STARTED
CREATE A WEBSITE
FIND A HOST
ACCESSORIZE
MAKE MONEY
PROMOTE YOUR SITE
OUR SERVICES
CONTACT US
shop now AND SAVE! amazon.com.
Privacy Information
Money Making E-commerce ...
H. Raymond Samuels II
RE

$$ Making Money $$

Making money on the web is ridiculously easy these days....or it used to be. A webmaster who knows how to fully take advantage of the money making opportunities available on today's internet can build an e-commerce superstore quickly, easily, and cheaply. Of course, e-commerce isn't the only way to go. In today's internet world, you don't have to sell anything at all to make a profit. You can take advantage of other sites who sell, and make money by referring your customers to them. In our money making section you will find:

- Affiliate Programs -- How to take advantage of affiliate marketing to earn money on the internet.
- Advertising -- How to earn money by selling advertising space on your site.
- Merchant Accounts -- The next most important step after hosting in your ecommerce adventure.
- Ecommerce accessories -- If you're serious, you might want some more tools.
- Your Own Affiliate Program -- So you want to start an affiliate program for your own product, huh?

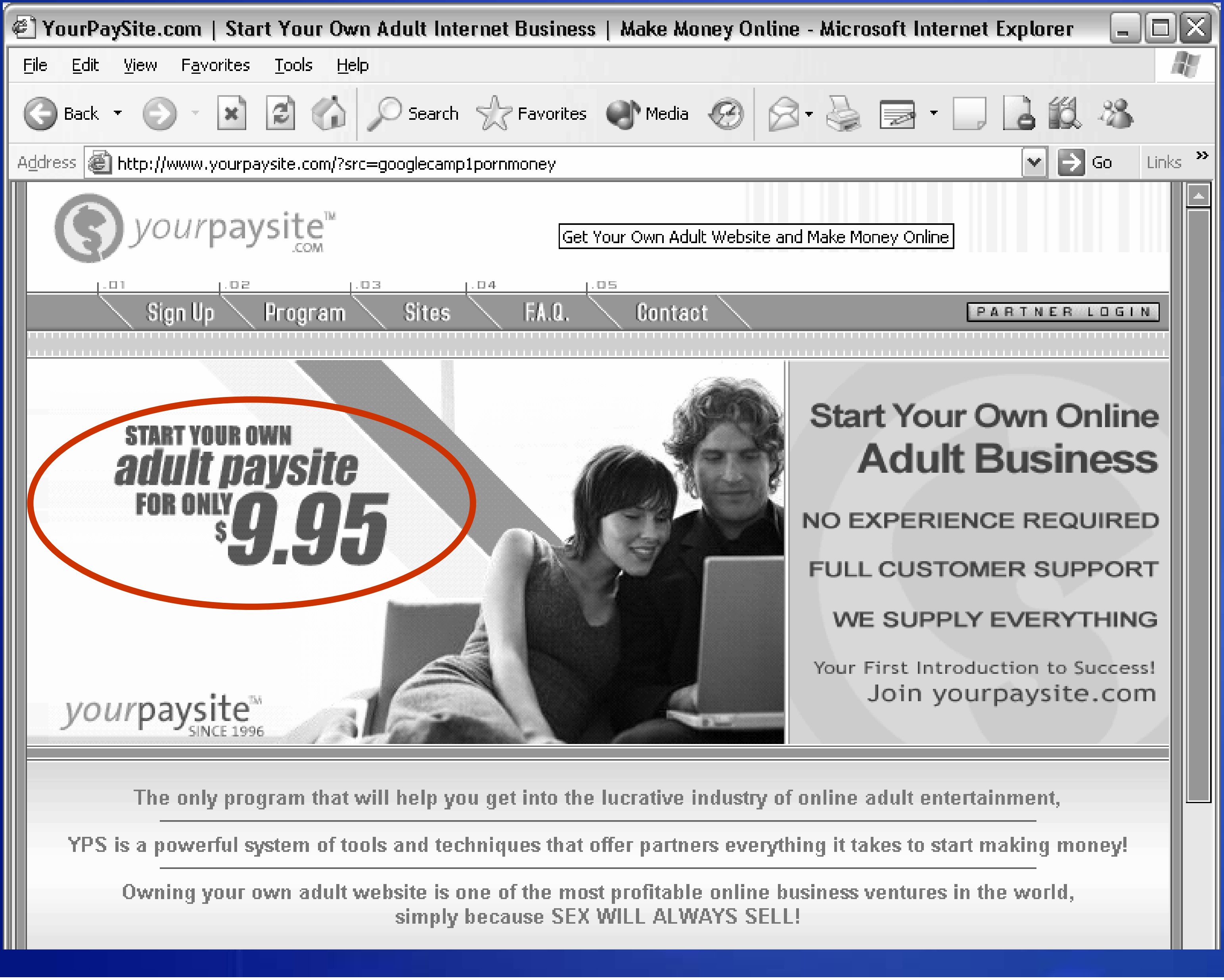
Need Traffic? Buy it!


ry : Click Through Exchanges - Microsoft Internet Explorer
elp
Search
Favorites
Media
change/Click_Through_Exchanges/

Ezine advertising safelists and email advertising. Pioneering website marketing and promotion. Email advertising using ad blasters IP ad broadcasting software and ezine advertising, safelists, optin Email marketing ebooks and promotion ebook for clickbank

- **Free advertising exchange autohits- Receive up to 6.840 visitors ...**
  Free advertising autosurf exchange program 10000 free visitors to your website- free autohits marketing
- **Free Link Exchange**
  A text ad exchange network, enabling companies to promote their websites by showing text ads in return for text advertising on other websites. Free to join and features an affiliate scheme.
- **FreeOnlineCash - Traffic Boosters: AutoSurf Programs**
  Autosurf Programs can increase traffic to your site
- **Get FREE Traffic Exchanges To Your Site With exchange autosurf ...**
  The most current listing of free exchange autosurf locator exchanges on the net, Learn to sell on eBay and much more! Create a flood of free traffic to your site today!
- **Global Team 1 Downline Organization**
  Global Team 1 is a network marketing organization whose mission is to teach you how to work smarter and become successful in your own home-based business. Membership in The Dream Team is FREE.

Need A Family Business?



YourPaySite.com | Start Your Own Adult Internet Business | Make Money Online - Microsoft Internet Explorer

Address http://www.yourpaysite.com/?src=googlecamp1pornmoney

Get Your Own Adult Website and Make Money Online

Start Your Own Online Adult Business

NO EXPERIENCE REQUIRED

FULL CUSTOMER SUPPORT

WE SUPPLY EVERYTHING

Your First Introduction to Success!
Join yourpaysite.com

The only program that will help you get into the lucrative industry of online adult entertainment,

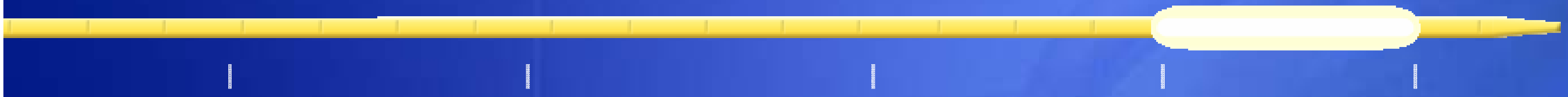
YPS is a powerful system of tools and techniques that offer partners everything it takes to start making money!

Owning your own adult website is one of the most profitable online business ventures in the world,
simply because SEX WILL ALWAYS SELL!

Situation:

It is getting scary!

Why does this gap exist?



Product ship

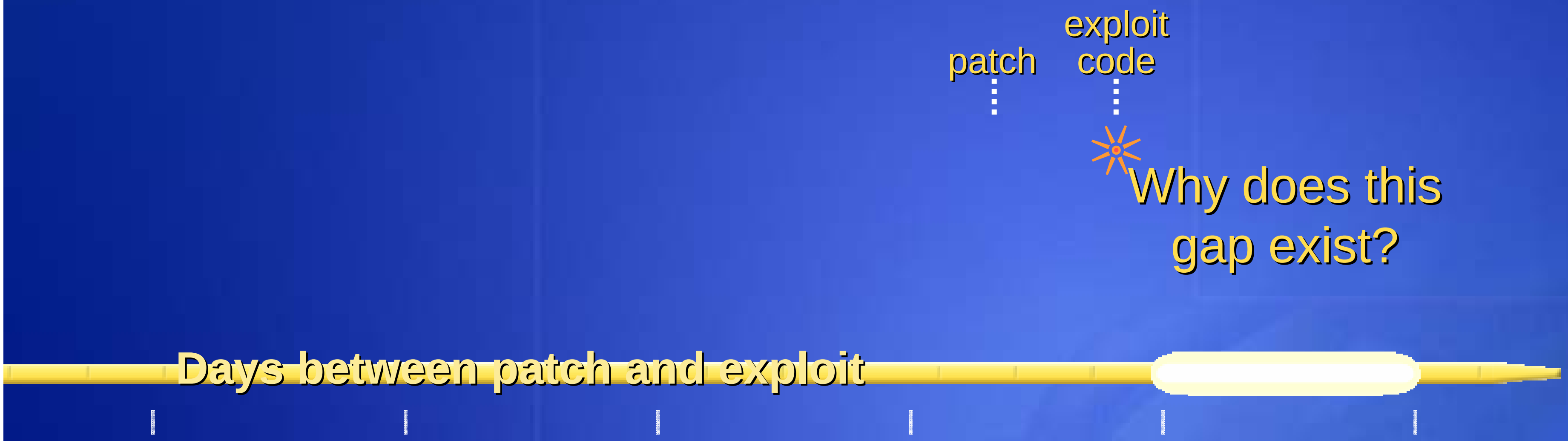
Vulnerability discovered

Component modified

Patch released

Patch deployed at customer site

Exploit Timeline

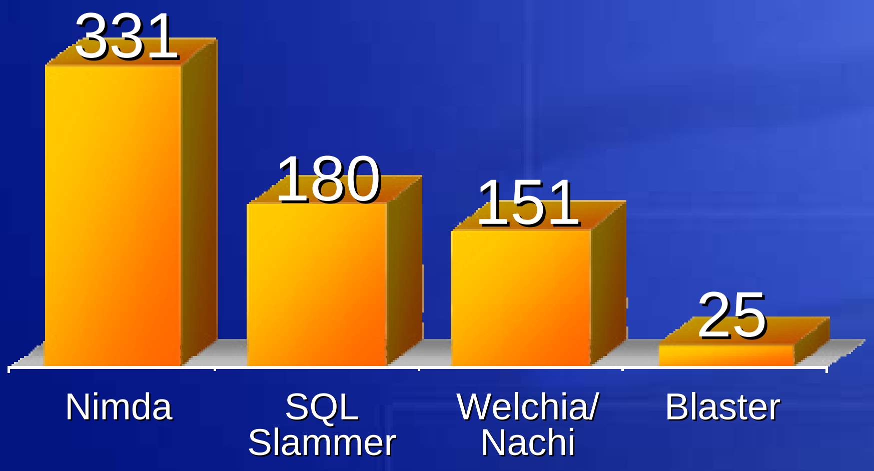


patch

exploit code

Why does this gap exist?

Days between patch and exploit



- Days From Patch to Exploit
  - The average is now nine days for a patch to be reverse-engineered
  - As this cycle keeps getting shorter, patching is a less effective defense in large organizations

The Forensics of a Virus

July 1

Vulnerability reported to us / Patch in progress

Report

- Vulnerability in RPC/DDOM reported
- MS activated highest level emergency response process

July 16

Bulletin & patch available
No exploit

Bulletin

- MS03-026 delivered to customers (7/16/03)
- Continued outreach to analysts, press, community, partners, government agencies

July 25

Exploit code in public

Exploit

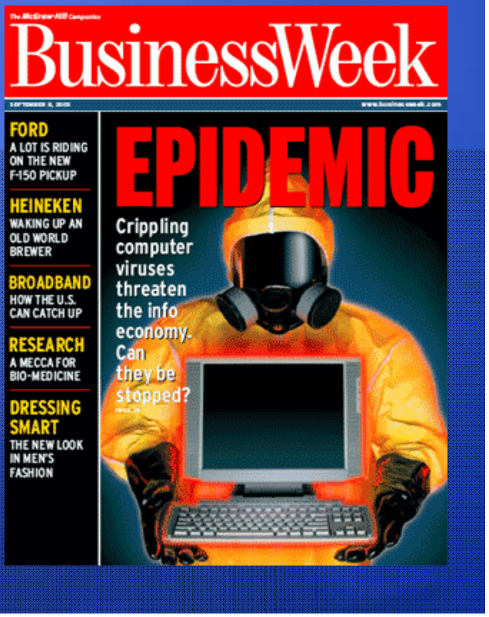
- X-focus published exploit tool
- MS heightened efforts to get information to customers

Aug 11

Worm in the world

Worm

- Blaster worm discovered –; variants and other viruses hit simultaneously (i.e. “SoBig”)


The McGraw-Hill Companies
BusinessWeek
www.businessweek.com
FORD
A LOT IS RIDING ON THE NEW F-150 PICKUP
HEINEKEN
WAKING UP AN OLD WORLD BREWER
BROADBAND
HOW THE U.S. CAN CATCH UP
RESEARCH
A MECCA FOR BIO-MEDICINE
DRESSING SMART
THE NEW LOOK IN MEN'S FASHION
EPIDEMIC
Crippling computer viruses threaten the info economy. Can they be stopped?

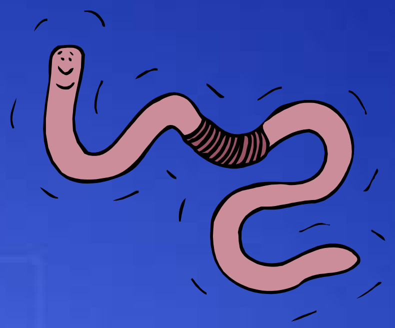
Blaster shows the complex interplay between security researchers, software companies, and hackers

Viruses, Worms & Spies

Virus:

- Old “traditional” viruses usually require human interaction
  - You have to save it, run it, share floppy disks, etc.
  - E-mailing a program / document, without knowing it is infected
- Typically just attach themselves to programs & documents, and then depend on humans to propagate
- This is changing…

Worms:



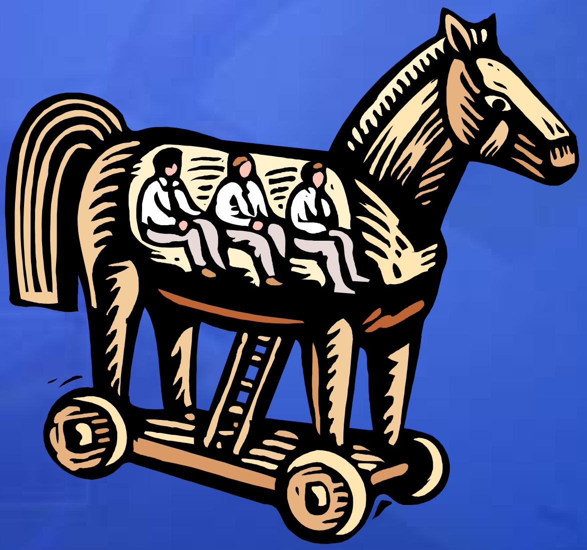
- Sub-class of Virus
- Replicated Automatically without human help
- Example is e-mail address book attack
- Bogs down networks and Internet
  - Think of a multi-level marketing company!
- Sasser, Blaster are examples

Worms:

- Scary part – you don’t have to do anything but turn your computer on!

Trojan Horse

- Program that appears to be a “good” program, but isn’t
- Might do what it is supposed to, plus more!
- Some Spyware falls in this category



Spyware:

- Defined as software that collects information about you.
- This might be OK, it might not
  - Web page collecting anonymous “click” data
  - Recording your bank # and password
- Many of these are not bad
  - You sign up for a music service, it gathers web site data, then sends you targeted advertisements that you might like

Spyware:

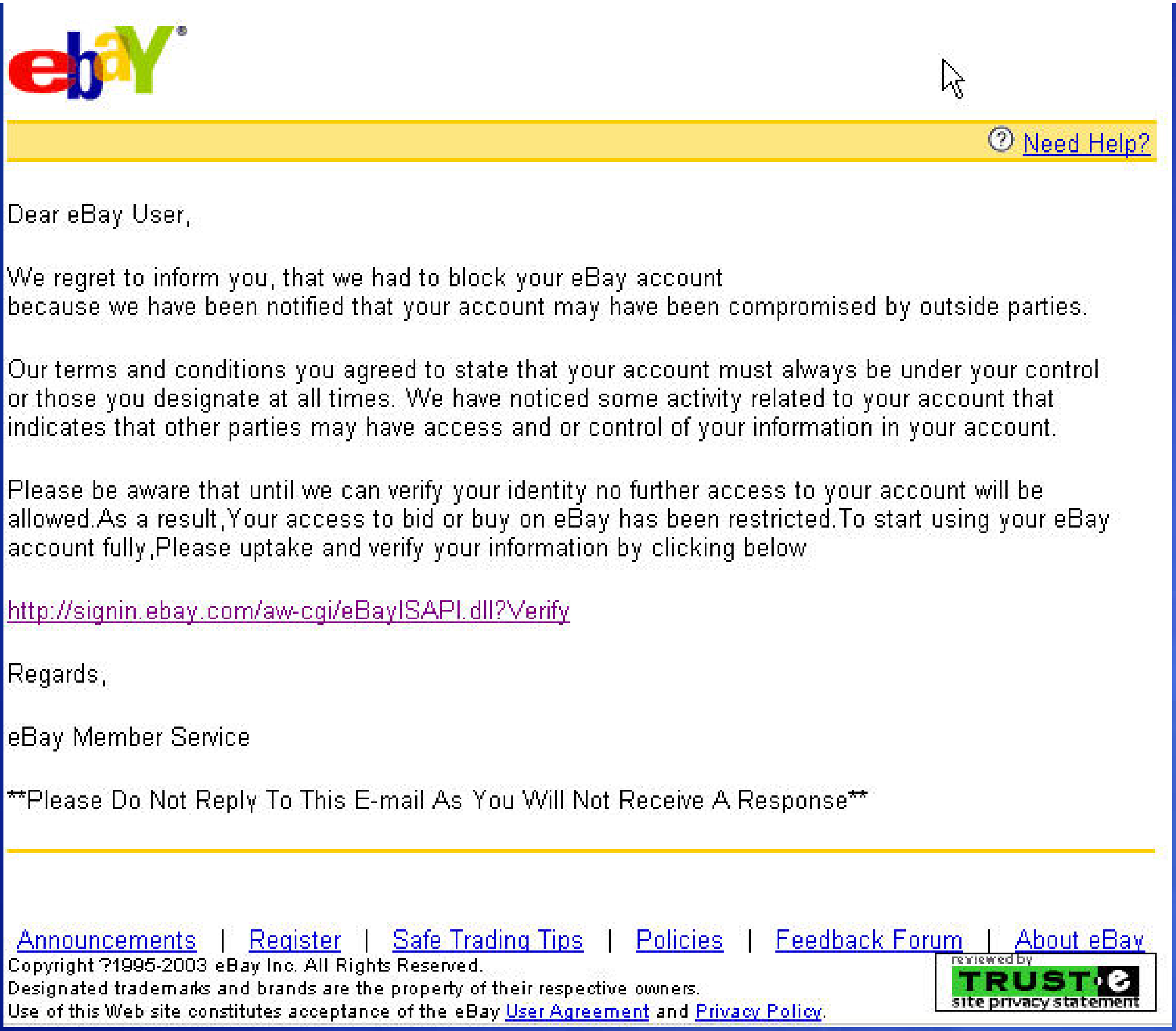
- Much of it is bad
- Example: Toolbar programs
  - Once the toolbar program is installed, it can collect anything it wants to.
  - Record your keystrokes, then “phone home”
  - Record websites, names & passwords
- Even if you remove them, they leave “bread crumbs” so that they re-install themselves

Spyware:

- Ever get pop-ups that constantly ask for you to click “OK” and won’t go away?
- This is Spyware or a virus of some sort

Phishing:

- Not a virus, but ways to trick you into giving up personal information
- See http://www.antiphishing.org for a lot of examples



Dear eBay User,

We regret to inform you, that we had to block your eBay account
because we have been notified that your account may have been compromised by outside parties.

Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have access and or control of your information in your account.

Please be aware that until we can verify your identity no further access to your account will be allowed.As a result,Your access to bid or buy on eBay has been restricted.To start using your eBay account fully,Please uptake and verify your information by clicking below

http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify

Regards,

eBay Member Service

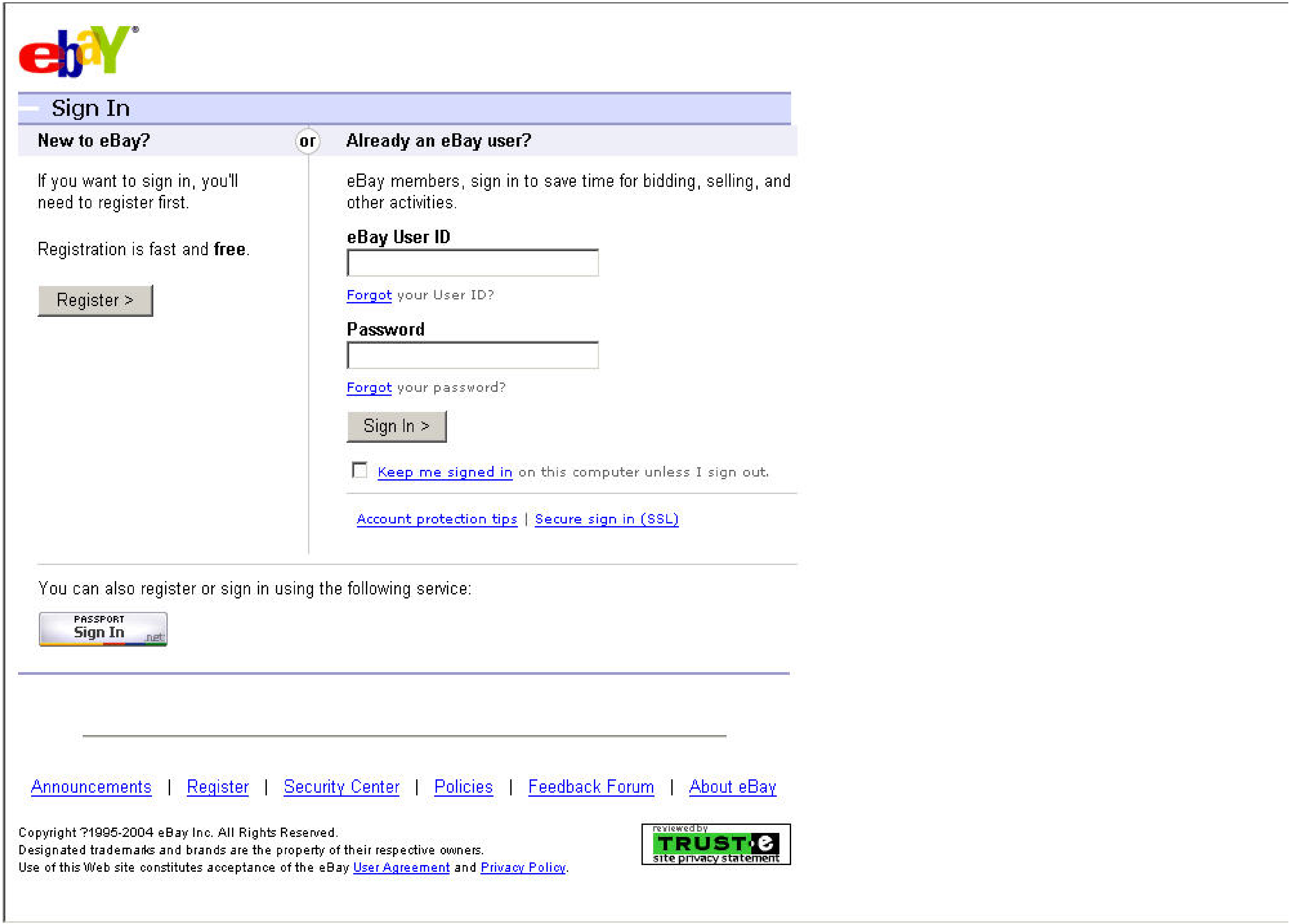
Please Do Not Reply To This E-mail As You Will Not Receive A Response

Announcements | Register | Safe Trading Tips | Policies | Feedback Forum | About eBay

Copyright ?1995-2003 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.

Visible link: http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify

Called link: http://signin_ebay_com_account.rndsystems.co.kr:7308/ebay.htm



Sign In

New to eBay?

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

Registration is fast and **free**.

Already an eBay user?

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

eBay User ID

Forgot your User ID?

Password

Forgot your password?

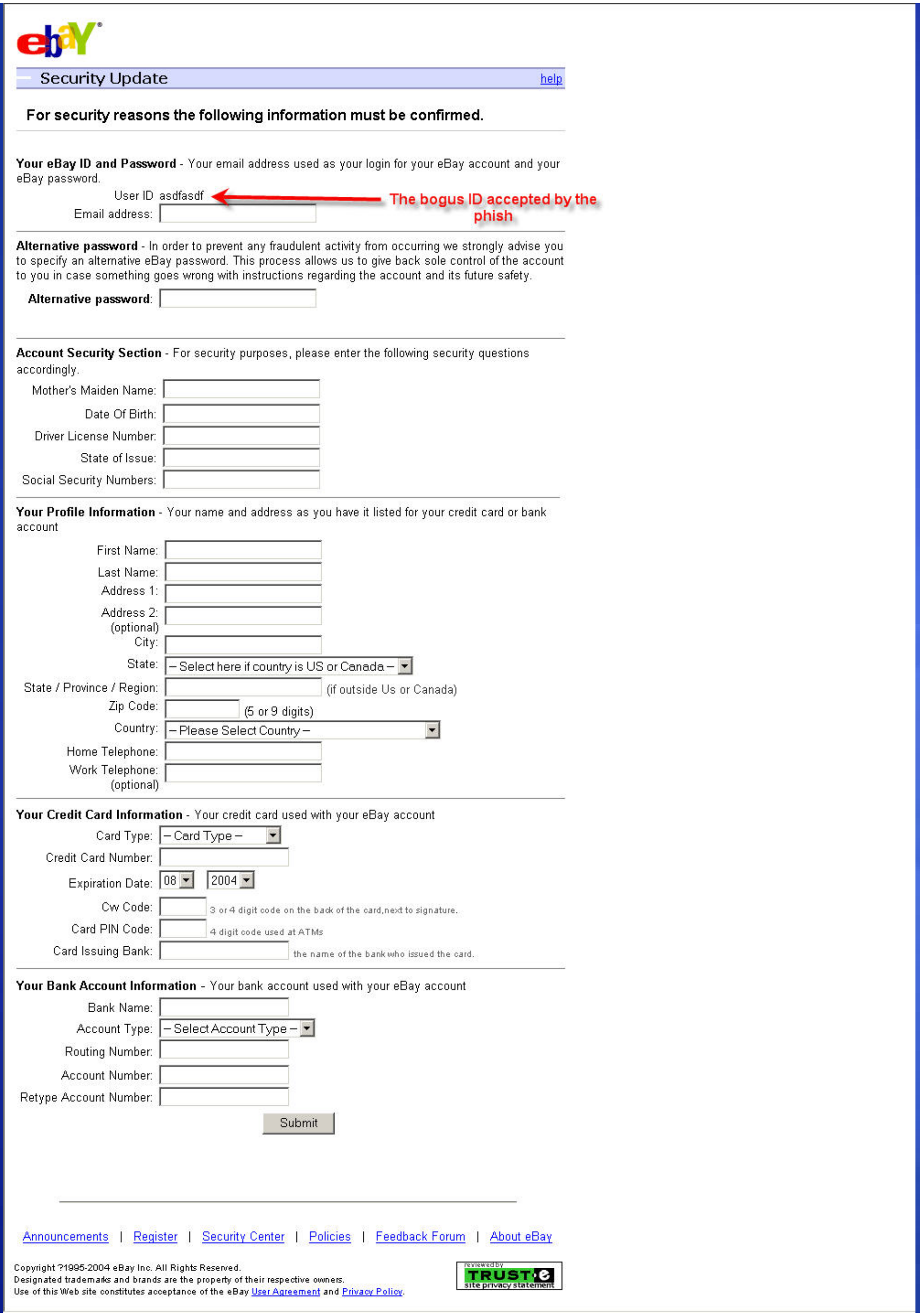
□ Keep me signed in on this computer unless I sign out.

Account protection tips | Secure sign in (SSL)

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

Announcements | Register | Security Center | Policies | Feedback Forum | About eBay

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.



The bogus ID accepted by the phish

Security Update

For security reasons the following information must be confirmed.

Your eBay ID and Password - Your email address used as your login for your eBay account and your eBay password.

User ID asdfasdf

Email address:

Alternative password - In order to prevent any fraudulent activity from occurring we strongly advise you to specify an alternative eBay password. This process allows us to give back sole control of the account to you in case something goes wrong with instructions regarding the account and its future safety.

Alternative password:

Account Security Section - For security purposes, please enter the following security questions accordingly.

Mother's Maiden Name:

Date Of Birth:

Driver License Number:

State of Issue:

Social Security Numbers:

Your Profile Information - Your name and address as you have it listed for your credit card or bank account

First Name:

Last Name:

Address 1:

Address 2: (optional)

City:

State: – Select here if country is US or Canada –

State / Province / Region: (if outside Us or Canada)

Zip Code: (5 or 9 digits)

Country: – Please Select Country –

Home Telephone:

Work Telephone: (optional)

Your Credit Card Information - Your credit card used with your eBay account

Card Type: – Card Type –

Credit Card Number:

Expiration Date: 08 2004

Cvv Code: 3 or 4 digit code on the back of the card,next to signature.

Card PIN Code: 4 digit code used at ATMs

Card Issuing Bank: the name of the bank who issued the card.

Your Bank Account Information - Your bank account used with your eBay account

Bank Name:

Account Type: – Select Account Type –

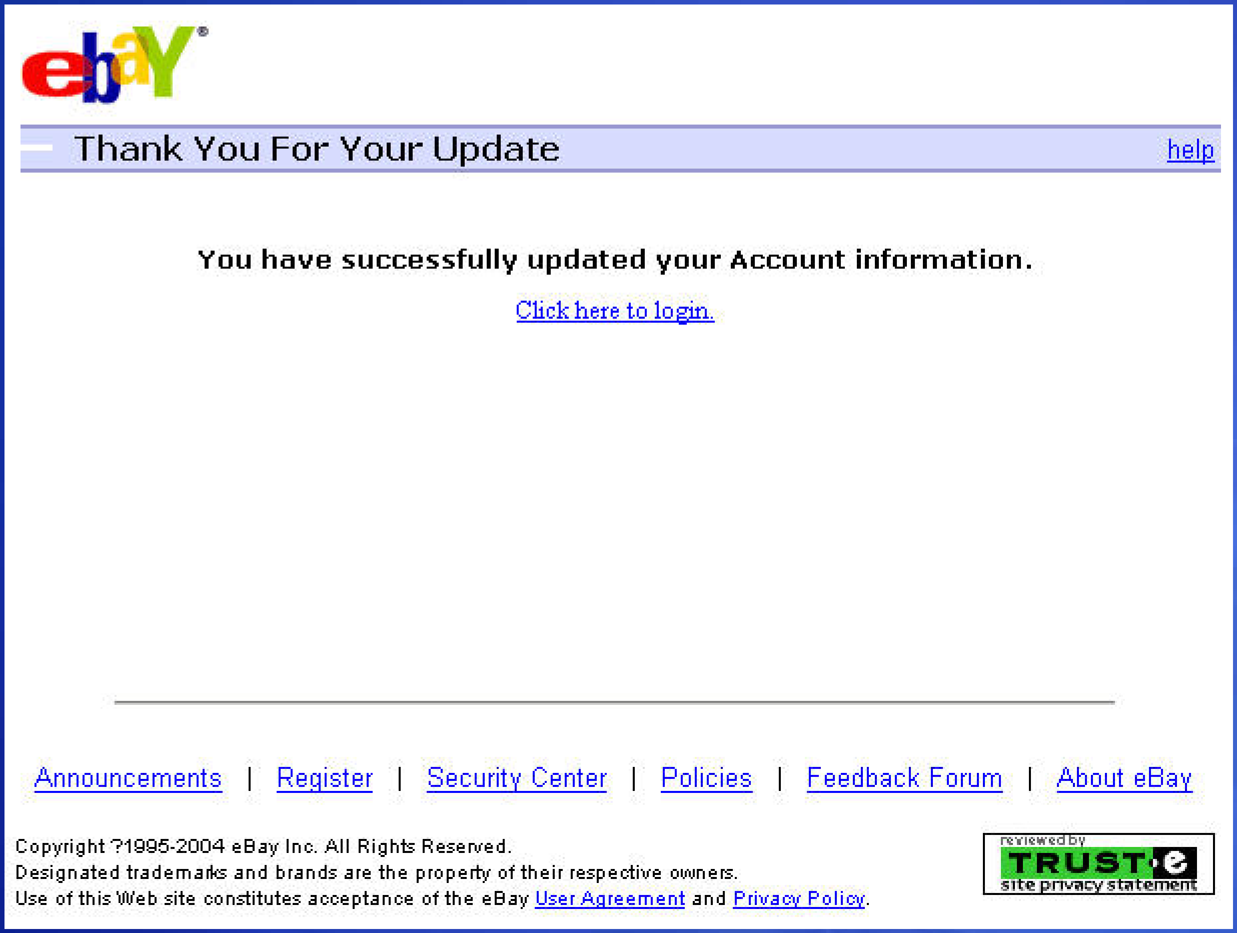
Routing Number:

Account Number:

Retype Account Number:

Submit
Announcements | Register | Security Center | Policies | Feedback Forum | About eBay

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.



Thank You For Your Update

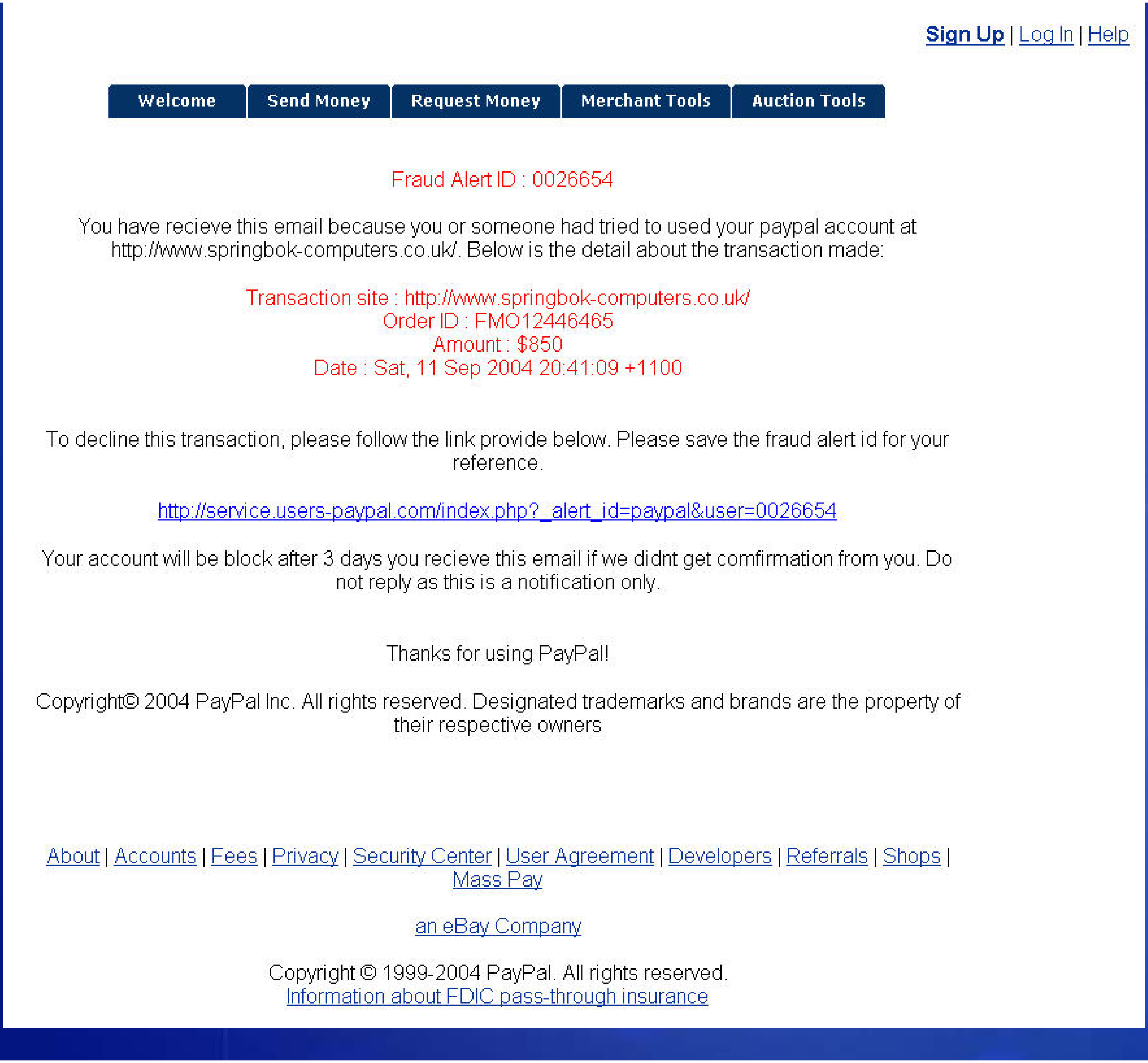
You have successfully updated your Account information.

Click here to login.

Announcements | Register | Security Center | Policies | Feedback Forum | About eBay

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



Fraud Alert ID : 0026654

You have recieve this email because you or someone had tried to used your paypal account at http://www.springbok-computers.co.uk/. Below is the detail about the transaction made:

Transaction site : http://www.springbok-computers.co.uk/
Order ID : FMO12446465
Amount : $850
Date : Sat, 11 Sep 2004 20:41:09 +1100

To decline this transaction, please follow the link provide below. Please save the fraud alert id for your reference.

http://service.users-paypal.com/index.php?_alert_id=paypal&user=0026654

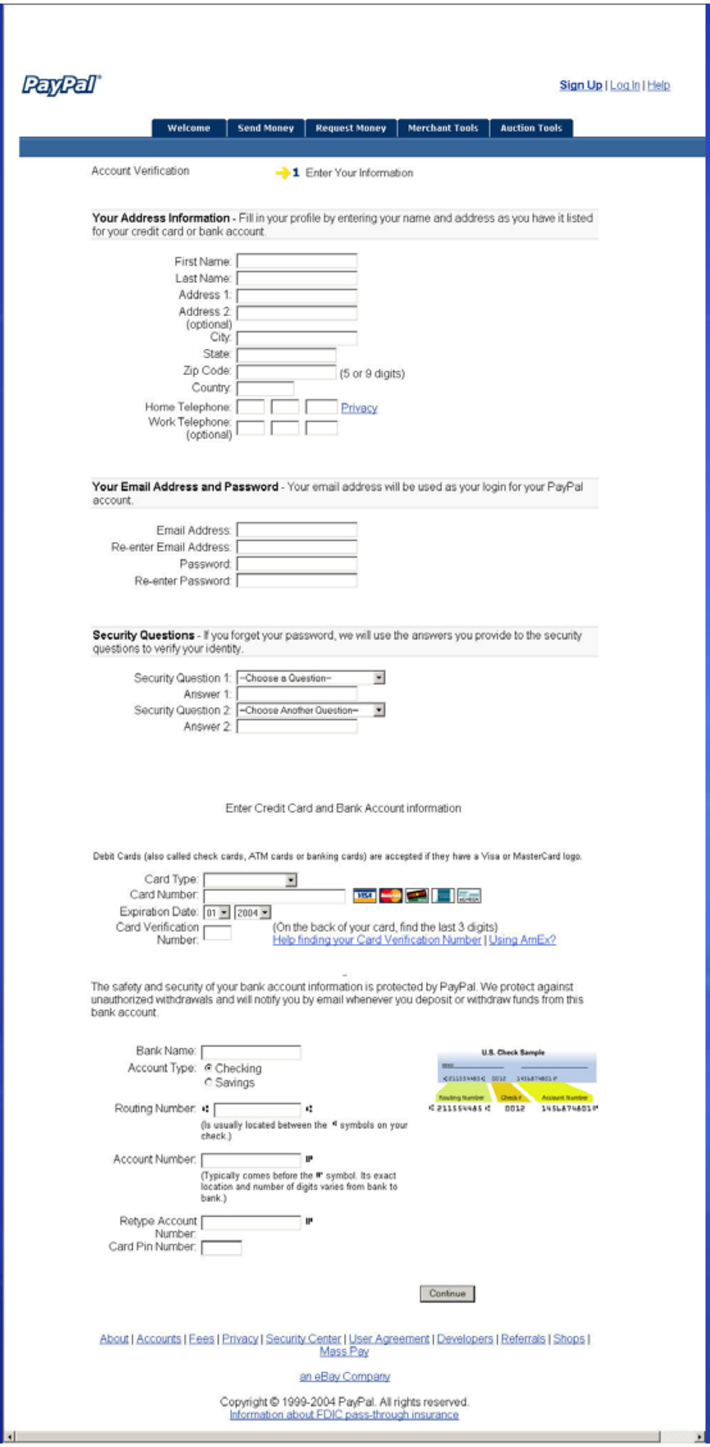
Your account will be block after 3 days you recieve this email if we didnt get comfirmation from you. Do not reply as this is a notification only.

Thanks for using PayPal!

Copyright© 2004 PayPal Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners

About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay
an eBay Company

Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance



Sign Up | Log In | Help

Account Verification

1 Enter Your Information

Your Address Information - Fill in your profile by entering your name and address as you have it listed for your credit card or bank account.

First Name:
Last Name:
Address 1:
Address 2: (optional)
City:
State:
Zip Code: (5 or 9 digits)
Country:
Home Telephone: Privacy
Work Telephone: (optional)

Your Email Address and Password - Your email address will be used as your login for your PayPal account.

Email Address:
Re-enter Email Address:
Password:
Re-enter Password:

Security Questions - If you forget your password, we will use the answers you provide to the security questions to verify your identity.

Security Question 1: --Choose a Question--
Answer 1:
Security Question 2: --Choose Another Question--
Answer 2:

Enter Credit Card and Bank Account information

Debit Cards (also called check cards, ATM cards or banking cards) are accepted if they have a Visa or MasterCard logo.

Card Type:
Card Number:
Expiration Date: 01 2004
Card Verification Number: (On the back of your card, find the last 3 digits)
Help finding your Card Verification Number | Using AmEx?

The safety and security of your bank account information is protected by PayPal. We protect against unauthorized withdrawals and will notify you by email whenever you deposit or withdraw funds from this bank account.

Bank Name:
Account Type: ● Checking
○ Savings

Routing Number: ⑆ ⑆
(Is usually located between the ⑆ symbols on your check.)

Account Number: ⑈
(Typically comes before the ⑈ symbol. Its exact location and number of digits varies from bank to bank.)

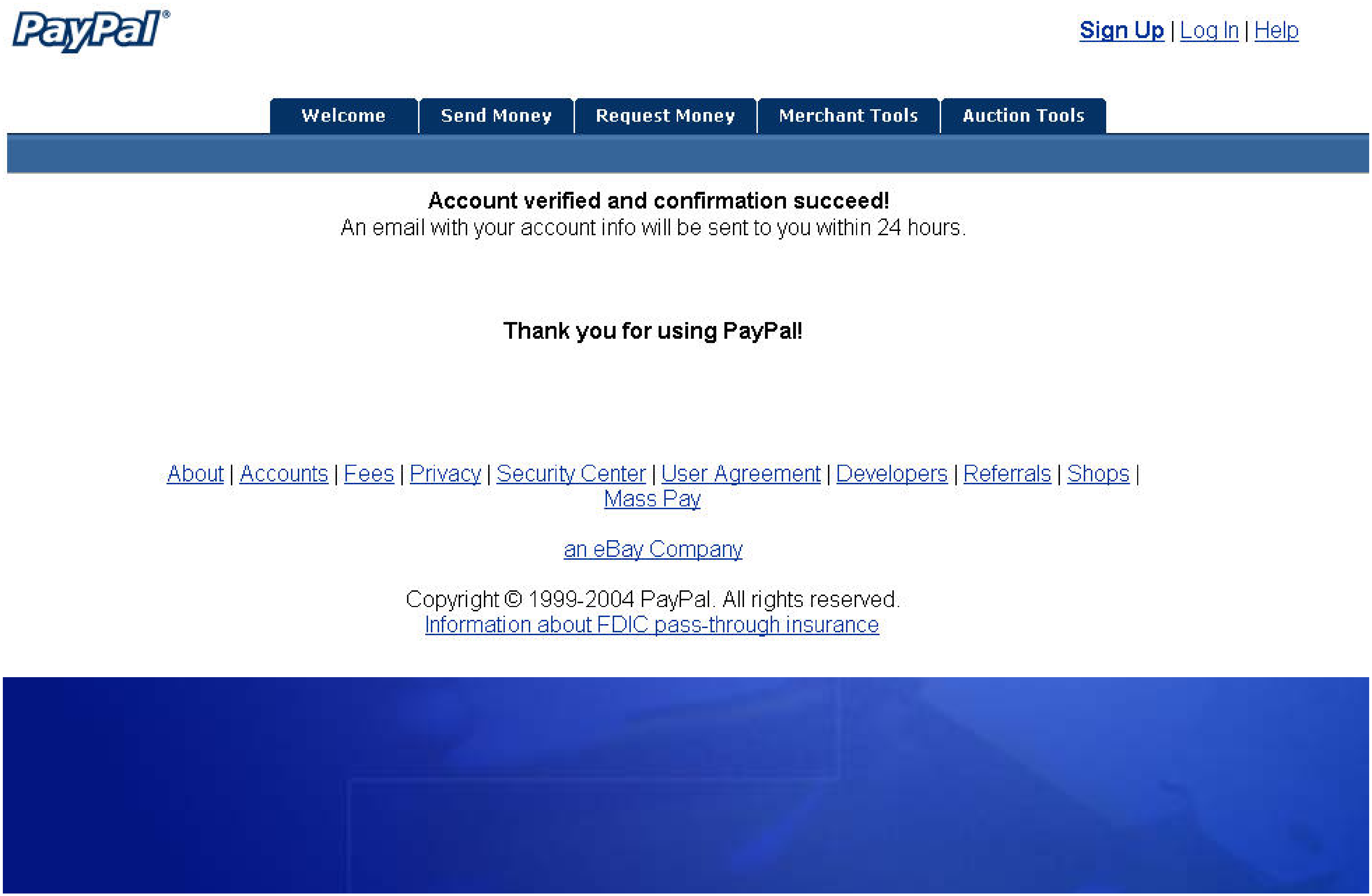
Retype Account Number: ⑈
Card Pin Number:

Continue

About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay

an eBay Company

Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance

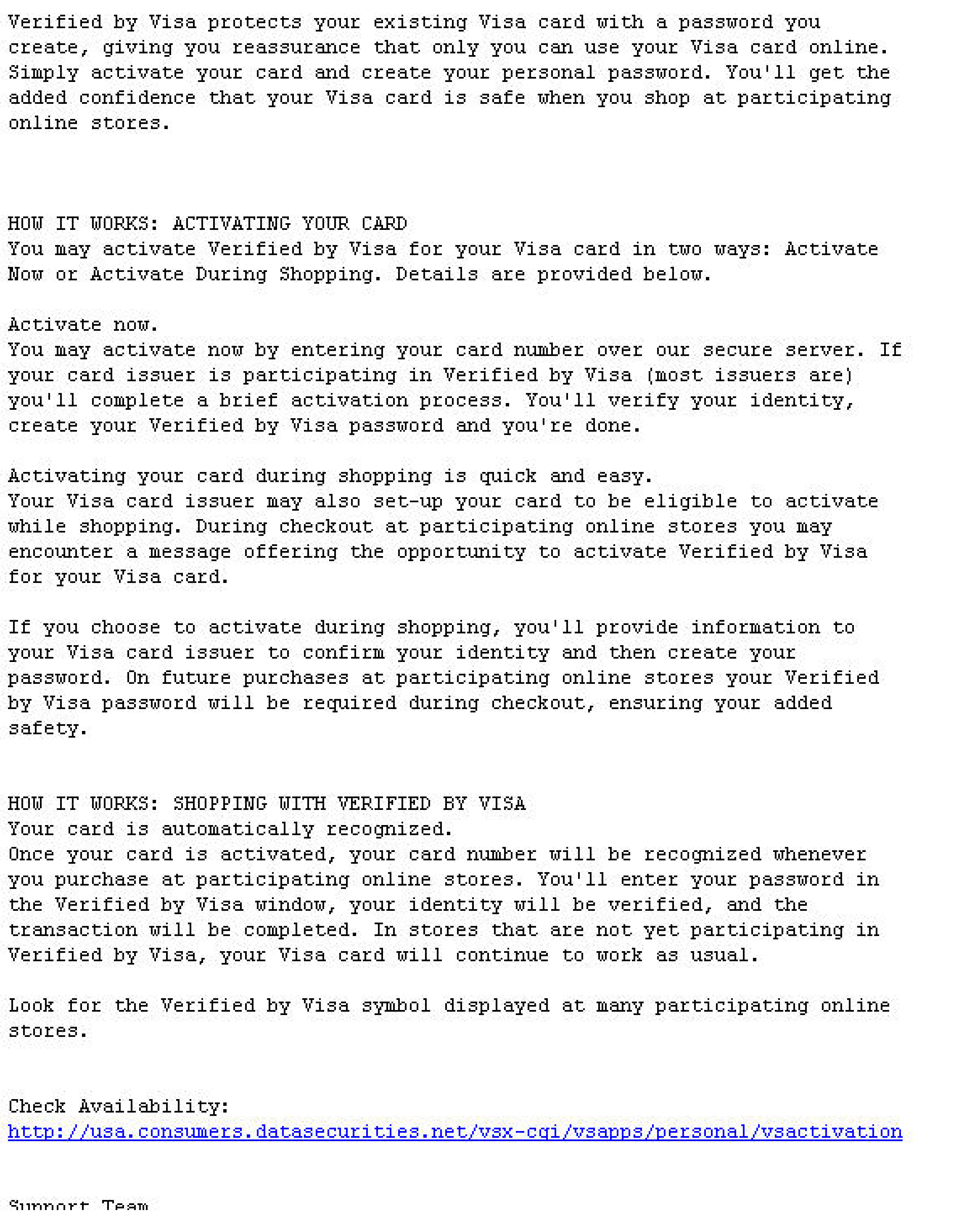

PayPal®
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools

Account verified and confirmation succeed!
An email with your account info will be sent to you within 24 hours.

Thank you for using PayPal!

About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay
an eBay Company

Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance



Verified by Visa protects your existing Visa card with a password you create, giving you reassurance that only you can use your Visa card online. Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

HOW IT WORKS: ACTIVATING YOUR CARD
You may activate Verified by Visa for your Visa card in two ways: Activate Now or Activate During Shopping. Details are provided below.

Activate now.
You may activate now by entering your card number over our secure server. If your card issuer is participating in Verified by Visa (most issuers are) you'll complete a brief activation process. You'll verify your identity, create your Verified by Visa password and you're done.

Activating your card during shopping is quick and easy.
Your Visa card issuer may also set-up your card to be eligible to activate while shopping. During checkout at participating online stores you may encounter a message offering the opportunity to activate Verified by Visa for your Visa card.

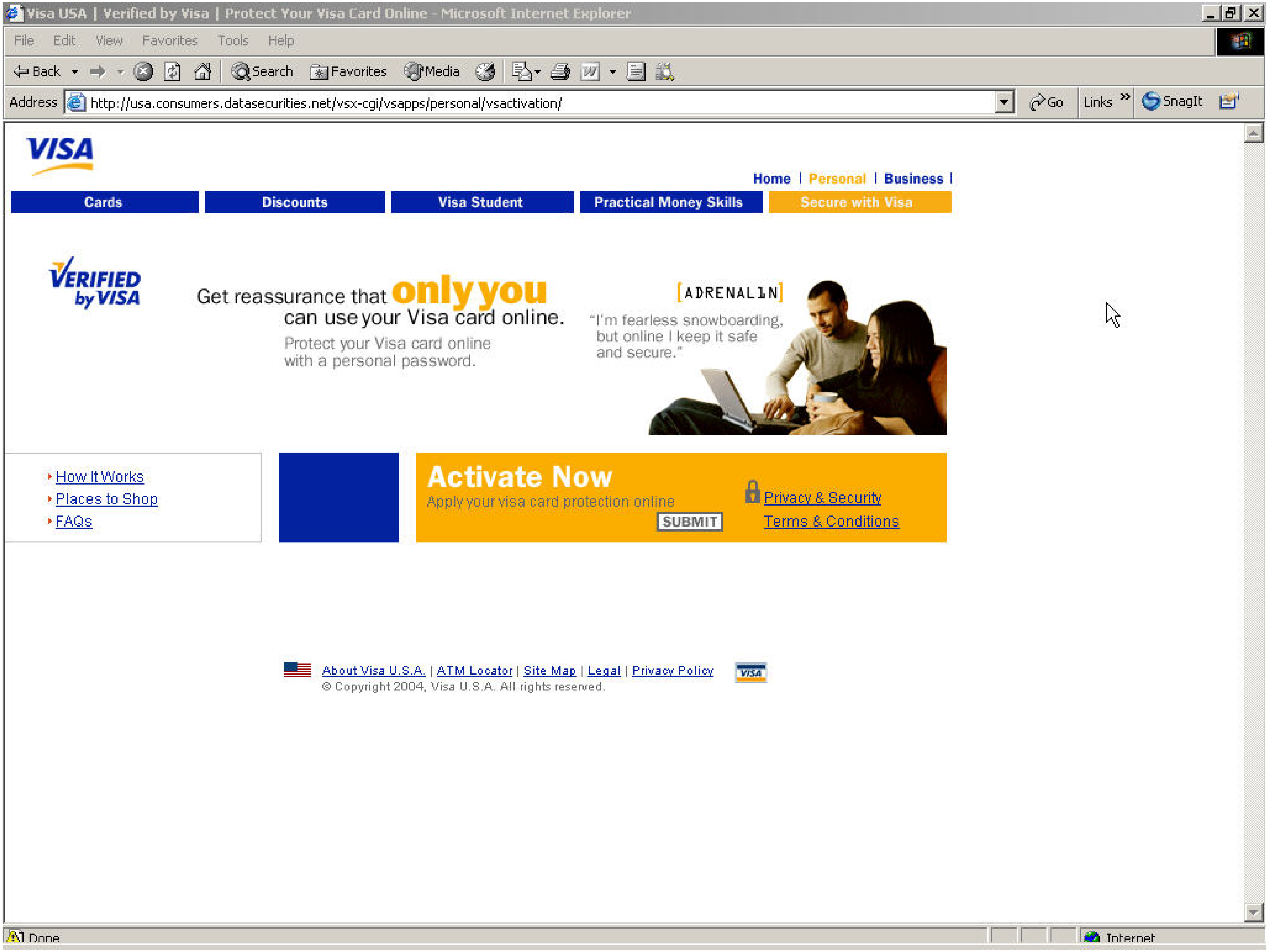
If you choose to activate during shopping, you'll provide information to your Visa card issuer to confirm your identity and then create your password. On future purchases at participating online stores your Verified by Visa password will be required during checkout, ensuring your added safety.

HOW IT WORKS: SHOPPING WITH VERIFIED BY VISA
Your card is automatically recognized.
Once your card is activated, your card number will be recognized whenever you purchase at participating online stores. You'll enter your password in the Verified by Visa window, your identity will be verified, and the transaction will be completed. In stores that are not yet participating in Verified by Visa, your Visa card will continue to work as usual.

Look for the Verified by Visa symbol displayed at many participating online stores.

Check Availability:
http://usa.consumers.datasecurities.net/vsx-cgi/vsapps/personal/vsactivation

Support Team



Visa USA | Verified by Visa | Protect Your Visa Card Online - Microsoft Internet Explorer

http://usa.consumers.datasecurities.net/vsx-cgi/vsapps/personal/vsactivation/

VERIFIED by VISA

Get reassurance that **only you** can use your Visa card online.

Protect your Visa card online with a personal password.

[ADRENAL1N]

"I'm fearless snowboarding, but online I keep it safe and secure."

- How It Works
- Places to Shop
- FAQs

Activate Now

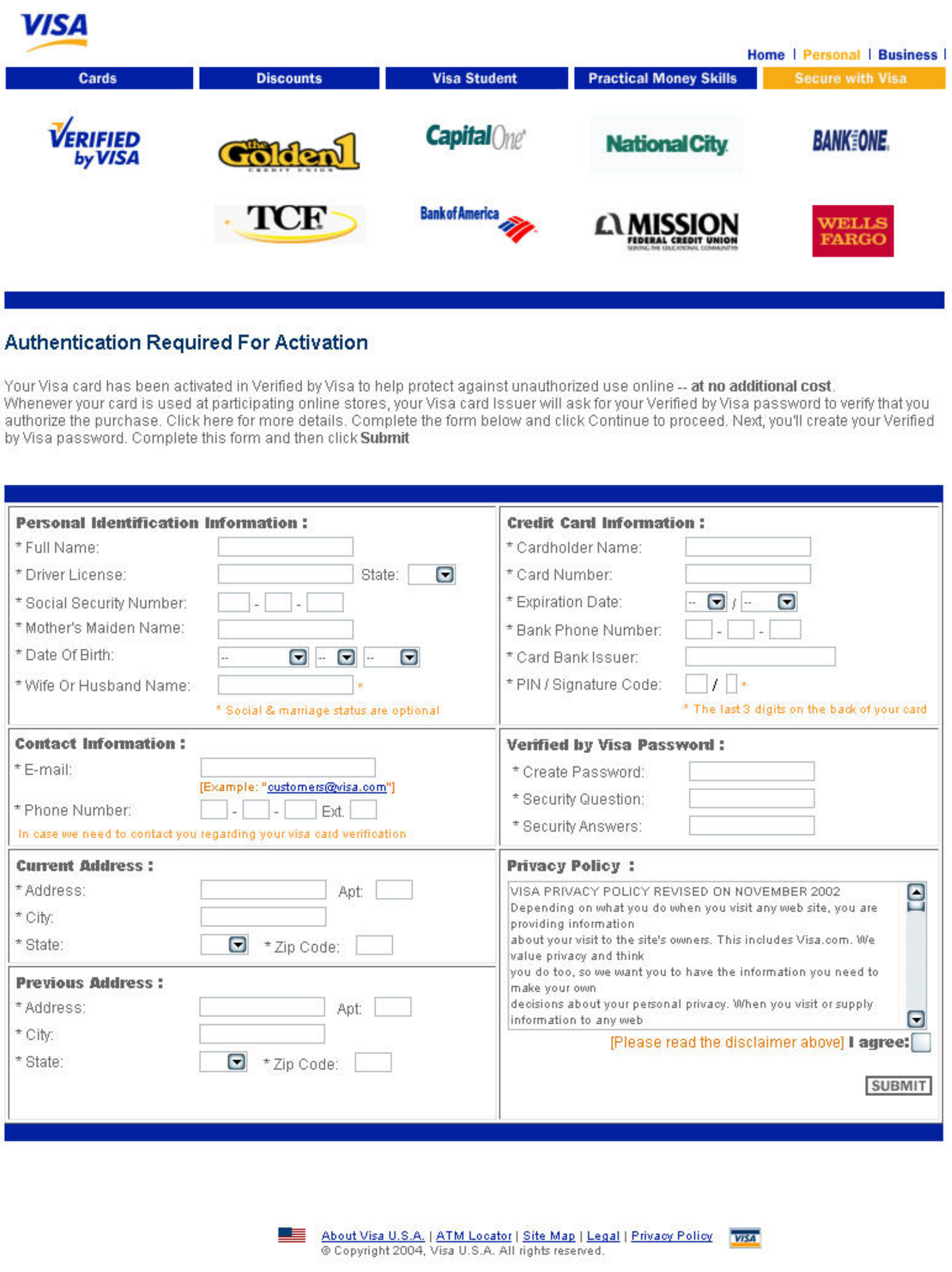
Apply your visa card protection online

Privacy & Security

Terms & Conditions

About Visa U.S.A. | ATM Locator | Site Map | Legal | Privacy Policy

© Copyright 2004, Visa U.S.A. All rights reserved.



Authentication Required For Activation

Your Visa card has been activated in Verified by Visa to help protect against unauthorized use online -- **at no additional cost**. Whenever your card is used at participating online stores, your Visa card Issuer will ask for your Verified by Visa password to verify that you authorize the purchase. Click here for more details. Complete the form below and click Continue to proceed. Next, you'll create your Verified by Visa password. Complete this form and then click **Submit**

Personal Identification Information :

* Full Name:

* Driver License: State:

* Social Security Number: - -

* Mother's Maiden Name:

* Date Of Birth: -- -- --

* Wife Or Husband Name: *

* Social & marriage status are optional

Credit Card Information :

* Cardholder Name:

* Card Number:

* Expiration Date: -- / --

* Bank Phone Number: - -

* Card Bank Issuer:

* PIN / Signature Code: / *

* The last 3 digits on the back of your card

Contact Information :

* E-mail:

[Example: "customers@visa.com"]

* Phone Number: - - Ext.

In case we need to contact you regarding your visa card verification

Verified by Visa Password :

* Create Password:

* Security Question:

* Security Answers:

Current Address :

* Address: Apt:

* City:

* State: * Zip Code:

Previous Address :

* Address: Apt:

* City:

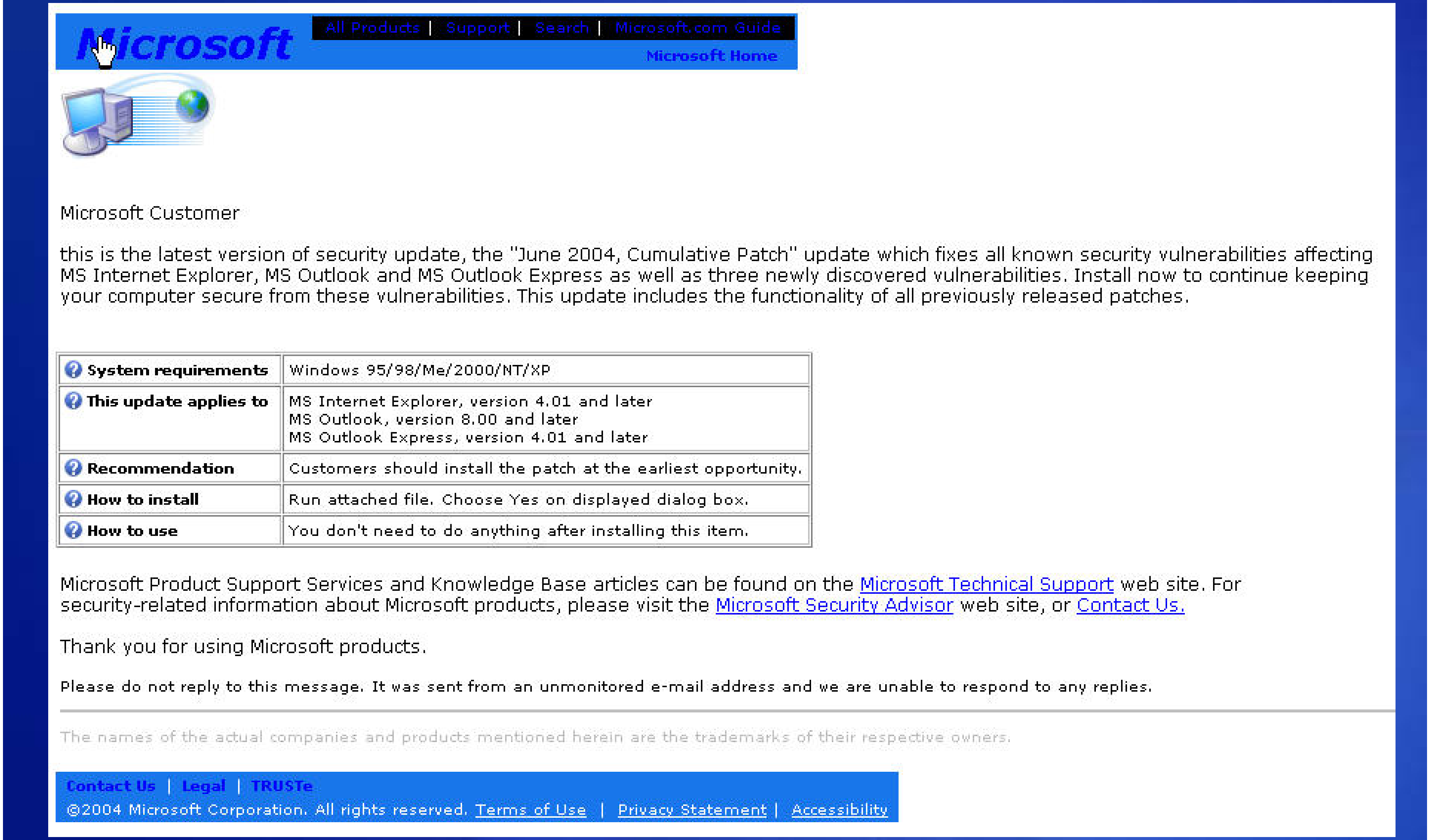
* State: * Zip Code:

Privacy Policy :

VISA PRIVACY POLICY REVISED ON NOVEMBER 2002
Depending on what you do when you visit any web site, you are providing information
about your visit to the site's owners. This includes Visa.com. We value privacy and think
you do too, so we want you to have the information you need to make your own
decisions about your personal privacy. When you visit or supply information to any web

[Please read the disclaimer above] **I agree:** □

© Copyright 2004, Visa U.S.A. All rights reserved.



Microsoft Customer

this is the latest version of security update, the "June 2004, Cumulative Patch" update which fixes all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to continue keeping your computer secure from these vulnerabilities. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us.

Thank you for using Microsoft products.

Please do not reply to this message. It was sent from an unmonitored e-mail address and we are unable to respond to any replies.

The names of the actual companies and products mentioned herein are the trademarks of their respective owners.

©2004 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement | Accessibility

How It Spreads

- Virtually all worms and trojan horses, etc. are spread through e-mail
- One person gets, they tell all their friends, they tell all *their* friends, etc.
- Ever seen “My Picture.jpg   .exe”
- Users get tricked into clicking OK

How to Protect Yourself

Practice Good Surfing Sense

- You know there are bad parts of town that you don’t go to
- The Internet is the same way – be wary!

#1 Rule

- Never download or open something, if you don't know what it is
- Even if you know the sender by name, check with them to see if they sent you something
- True company-based e-mails never send attachments
  - Make sure the link actually goes to their site & not a spoofed one!
- Only download what you trust, and even then be wary!

Points to Ponder

- Have you ever received an e-mail telling you that you have a virus?
- You might, or might not…
  - Your address could've been spoofed to someone else
  - Could be a trick to get you to install some "anti-virus" or "patch" (which is really a virus itself!)

How to Get Secure, Stay Secure

- Step 1 – Don’t change Internet Explorer “Zone” settings below “Medium”
- Step 2 – Don’t take downloads from strangers
  - Only install what you trust
  - “free” music & file sharing programs are wide open doors for hackers
- Step 3 – Try to see if you have any issues already
  - Does your browser open to a new home page, or search page?
  - Increase in advertisements & pop-ups?
  - Computer seems sluggish?

How to Get Secure, Stay Secure

- Step 4 – Get a detect & removal tool for spyware (Spybot Search & Destroy is good)
- Step 5 – Get some antivirus software (Norton, McAfee, etc.)
- Step 6 – Get a Firewall (Service Pack 2 or some other)
- Step 7 – Keep everything up-to-date!
    - Windows Automatic Updates, Anti-virus, Spyware

What is Microsoft Doing to Help?

- Block HTML in e-mail by default
- .EXE, .BAT, etc files are blocked
- Warnings when e-mail is sent automatically
- Behavior Blocking technologies
- Service Pack 2 on Windows XP
  - Firewall, pop-up blocker, others
- Working with Law Enforcement
- Reward money
  - $250,000 for Sasser paid!

Resources

- General

  http://www.microsoft.com/security

- Consumers

  http://www.microsoft.com/protect

- IT Professionals

  http://www.microsoft.com/technet/security

- Patch Management

  http://www.microsoft.com/technet/security/topics/patch

- Info on Virus, Worms, etc.

  http://www.microsoft.com/athome/security/viruses/virus101.mspx

- Info on Spyware

  http://www.microsoft.com/athome/security/spyware/devioussoftware.mspx

  http://www.microsoft.com/windowsxp/using/security/expert/honeycutt_spyware.mspx

Now for the Gentle Q&A…

Microsoft®

Your potential. Our passion.™

© 2004 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.