Test Your Tech

Crackers and cookies are:

A. Bytes to share with friends.

B. The best minor league baseball team of all time and their cheerleaders.

C. Hackers who attempt to break a program (crackers) and data stored on your computer by a Web server (cookies).

Test Your Tech

Crackers and cookies are:

A. Bytes to share with friends.

B. The best minor league baseball team of all time and their cheerleaders.

C. Hackers who attempt to break a program (crackers) and data stored on your computer by a Web server (cookies).

Security

Exploring the Dark Side of the Internet

Negative Issues

- Malware
  - Viruses, et al.
  - Spyware / Adware
- Privacy
  - Phishing
- Malicious
  - Cracking (not hacking)
  - Network service attacks

Different Types of Virii/Spyware

- Spyware
- Adware
- Embedded Programs
- Trojan Horse
- Browser Hijackers
- Dialers
- Worms

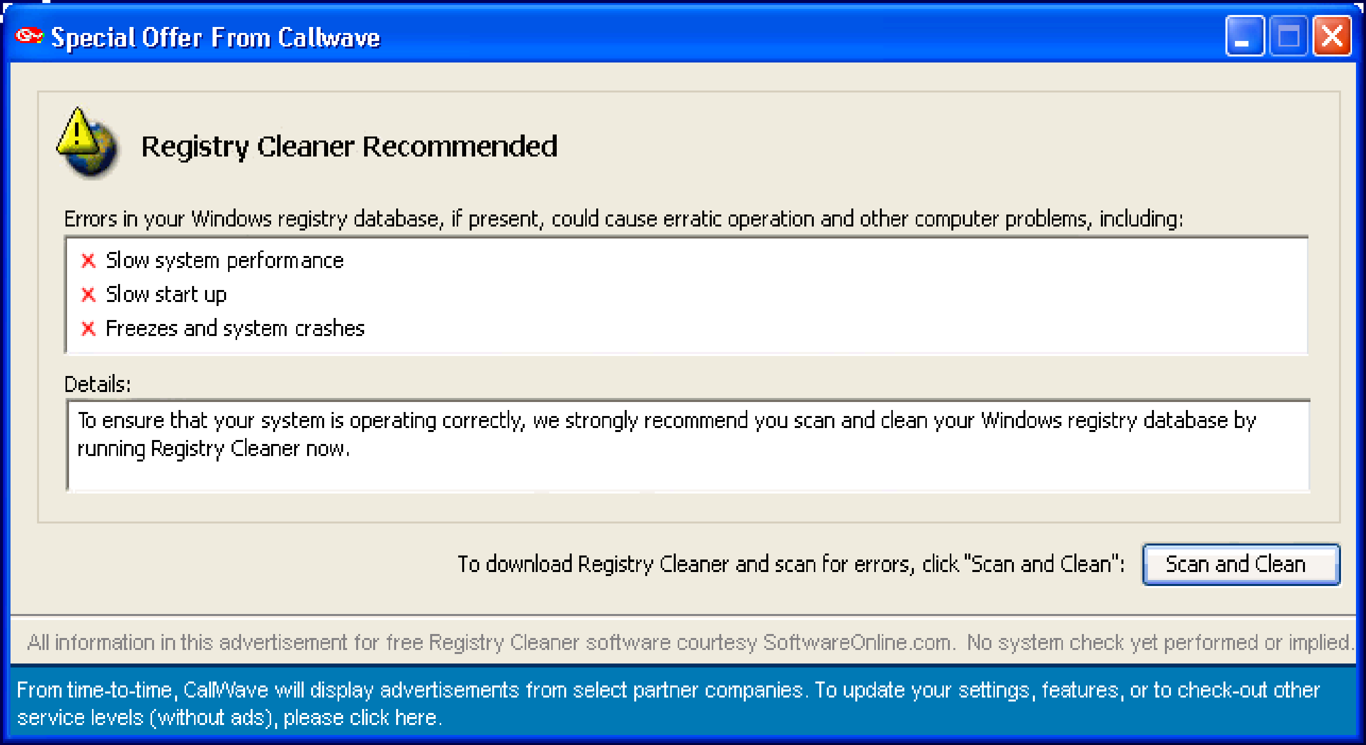
Why do people make Virii/Spyware?

- Profit
- Malice
- Boredom
- Business
- A challenge
- “Respect” from other virii writers

How do I know if I’ve got a Virus/Spyware?

- Virii
  - Programs will stop working correctly
  - Loosing data (documents disappearing)
  - Computer is running slower than normal
- Spyware
  - Popups (on or off the internet)
  - New toolbars
  - Home page changes
  - Search results look different
  - Error messages when accessing the web

What does Spyware look like?



Registry Cleaner Recommended

Errors in your Windows registry database, if present, could cause erratic operation and other computer problems, including:

- ✗ Slow system performance
- ✗ Slow start up
- ✗ Freezes and system crashes

Details:

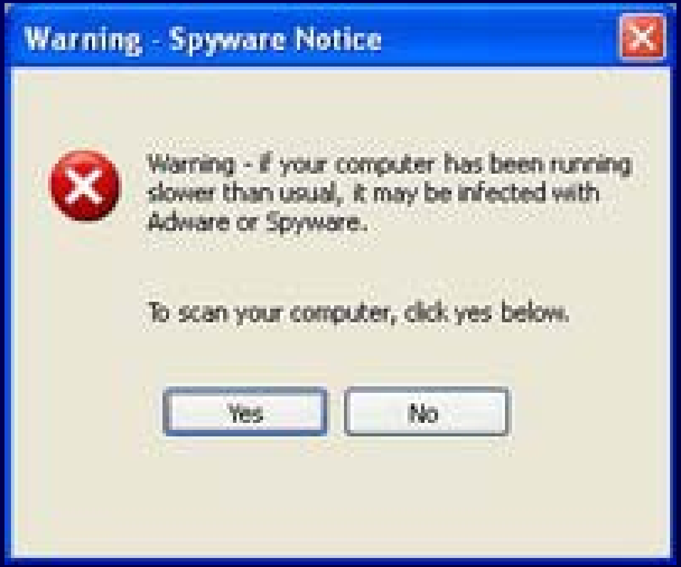
To ensure that your system is operating correctly, we strongly recommend you scan and clean your Windows registry database by running Registry Cleaner now.

To download Registry Cleaner and scan for errors, click "Scan and Clean":

All information in this advertisement for free Registry Cleaner software courtesy SoftwareOnline.com. No system check yet performed or implied.

From time-to-time, CallWave will display advertisements from select partner companies. To update your settings, features, or to check-out other service levels (without ads), please click here.

What does Spyware look like?

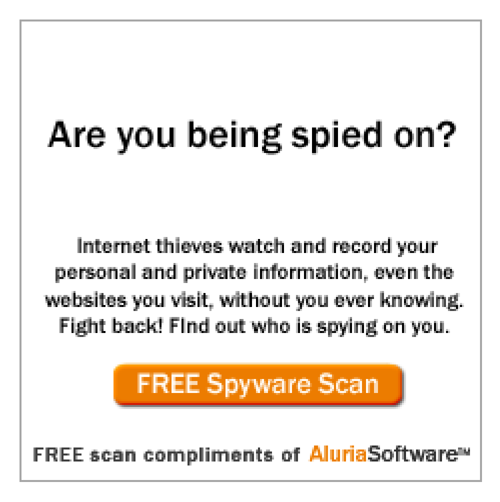


Warning - Spyware Notice

Warning - if your computer has been running slower than usual, it may be infected with Adware or Spyware.

To scan your computer, click yes below.

What does Spyware look like?

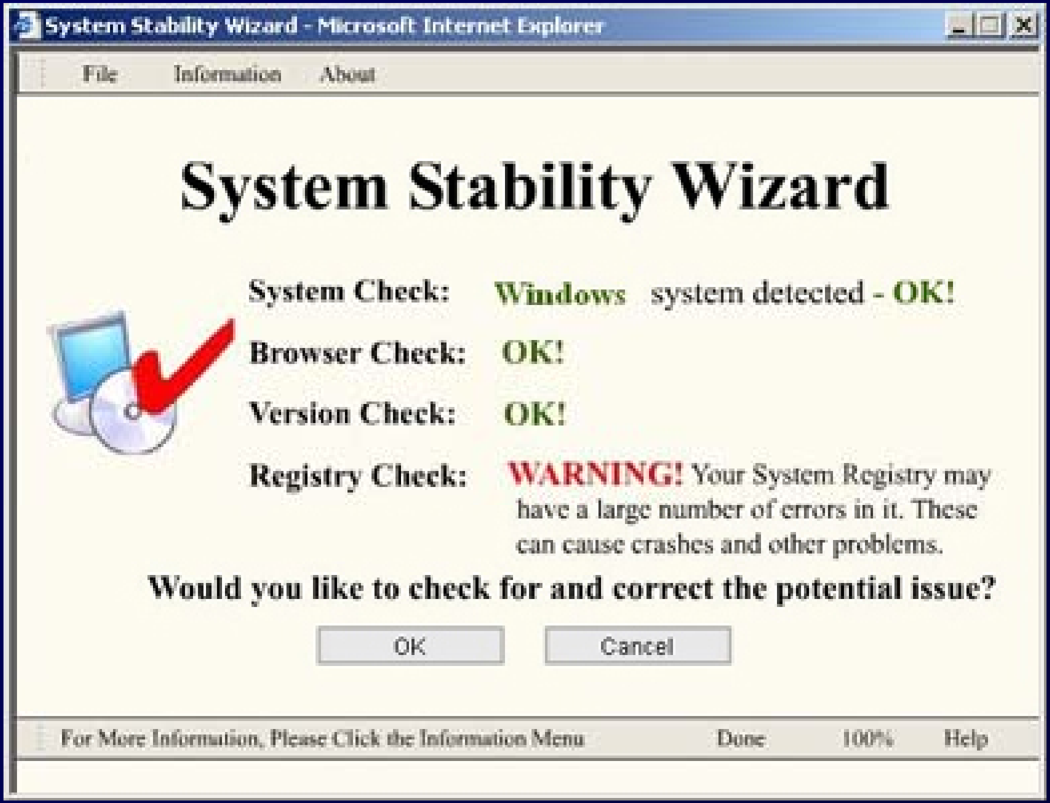


Are you being spied on?

Internet thieves watch and record your personal and private information, even the websites you visit, without you ever knowing. Fight back! Find out who is spying on you.

FREE scan compliments of AluriaSoftware™

What does Spyware look like?



System Stability Wizard - Microsoft Internet Explorer
File
Information
About
OK
Cancel
For More Information, Please Click the Information Menu
Done
100%
Help

System Stability Wizard

System Check: Windows system detected - **OK!**

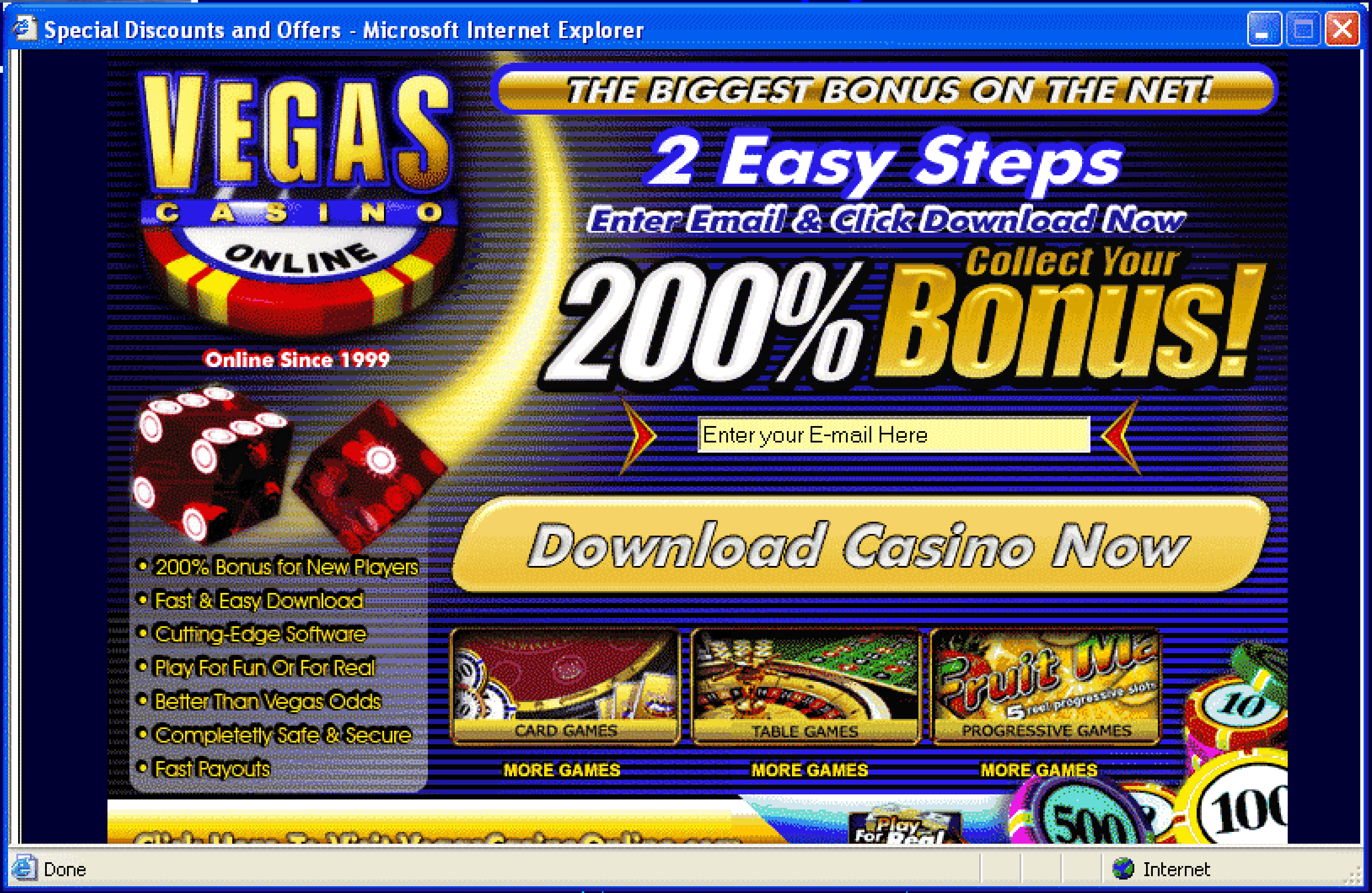
Browser Check: **OK!**

Version Check: **OK!**

Registry Check: **WARNING!** Your System Registry may have a large number of errors in it. These can cause crashes and other problems.

Would you like to check for and correct the potential issue?

What does Spyware look like?



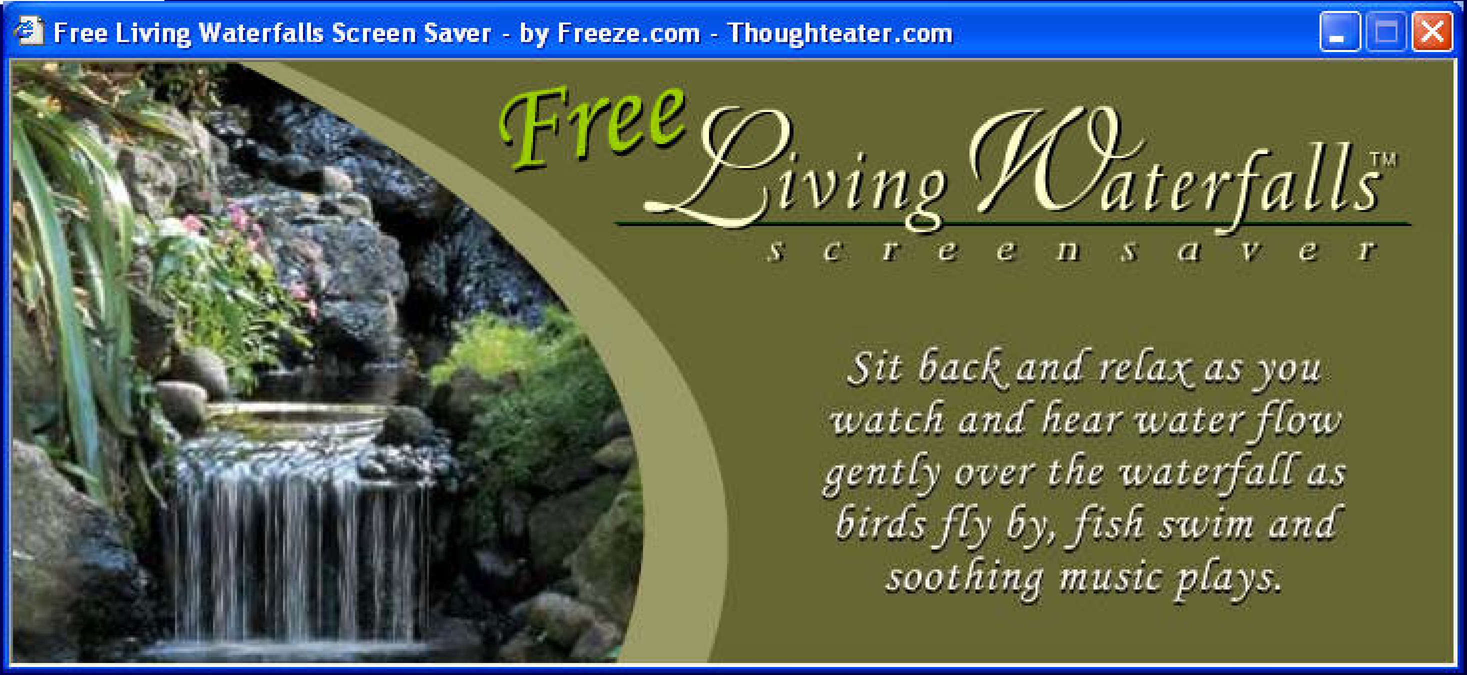
Special Discounts and Offers - Microsoft Internet Explorer

Done

Internet

of Washington

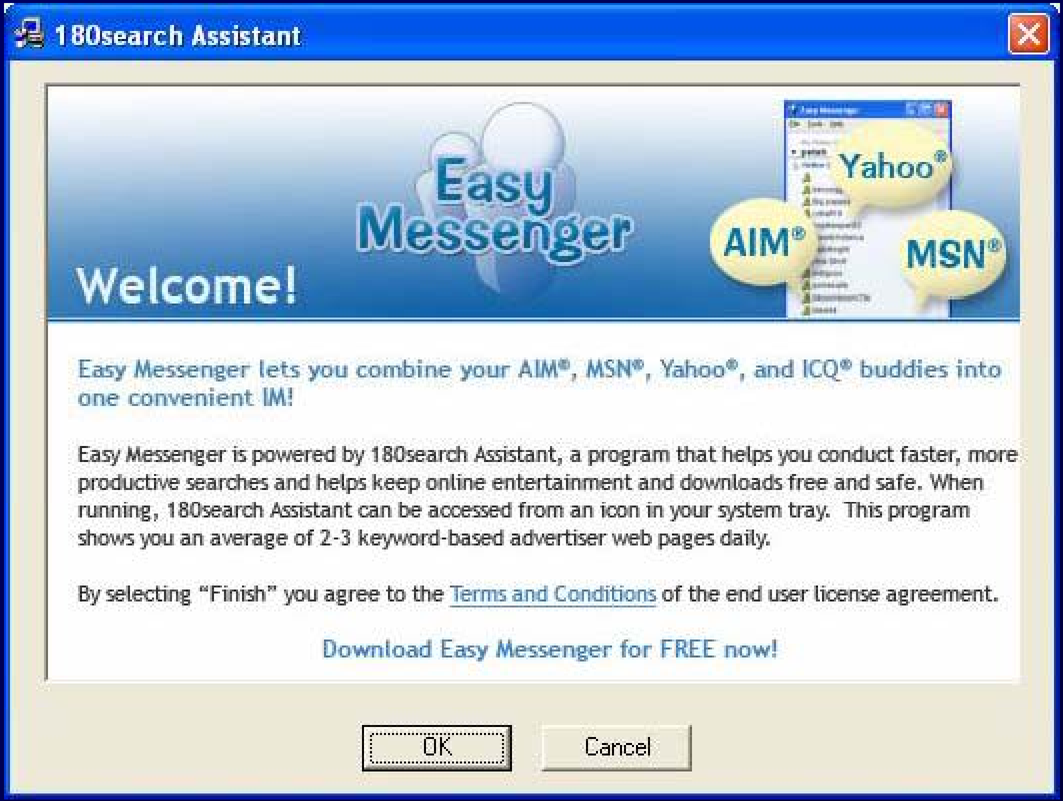
What does Spyware look like?



Free Living Waterfalls Screen Saver - by Freeze.com - Thoughteater.com

Sit back and relax as you watch and hear water flow gently over the waterfall as birds fly by, fish swim and soothing music plays.

What does Spyware look like?



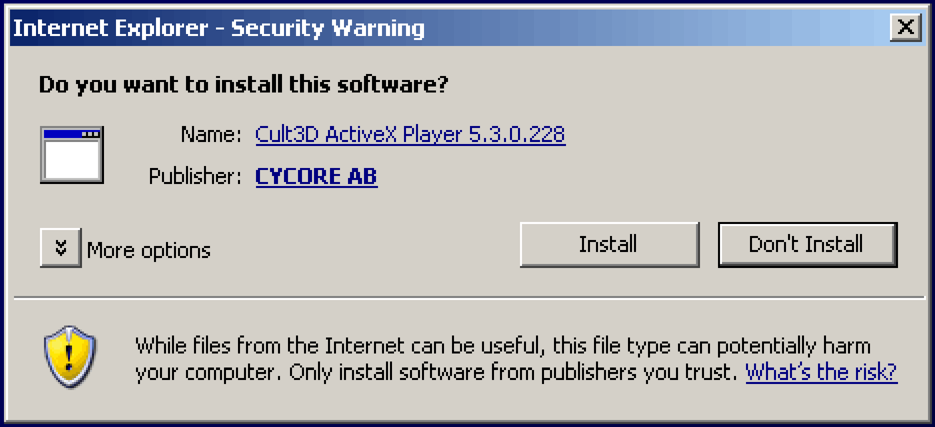
Easy Messenger lets you combine your AIM®, MSN®, Yahoo®, and ICQ® buddies into one convenient IM!

Easy Messenger is powered by 180search Assistant, a program that helps you conduct faster, more productive searches and helps keep online entertainment and downloads free and safe. When running, 180search Assistant can be accessed from an icon in your system tray. This program shows you an average of 2-3 keyword-based advertiser web pages daily.

By selecting "Finish" you agree to the Terms and Conditions of the end user license agreement.

Download Easy Messenger for FREE now!

What does Spyware look like?



Internet Explorer - Security Warning

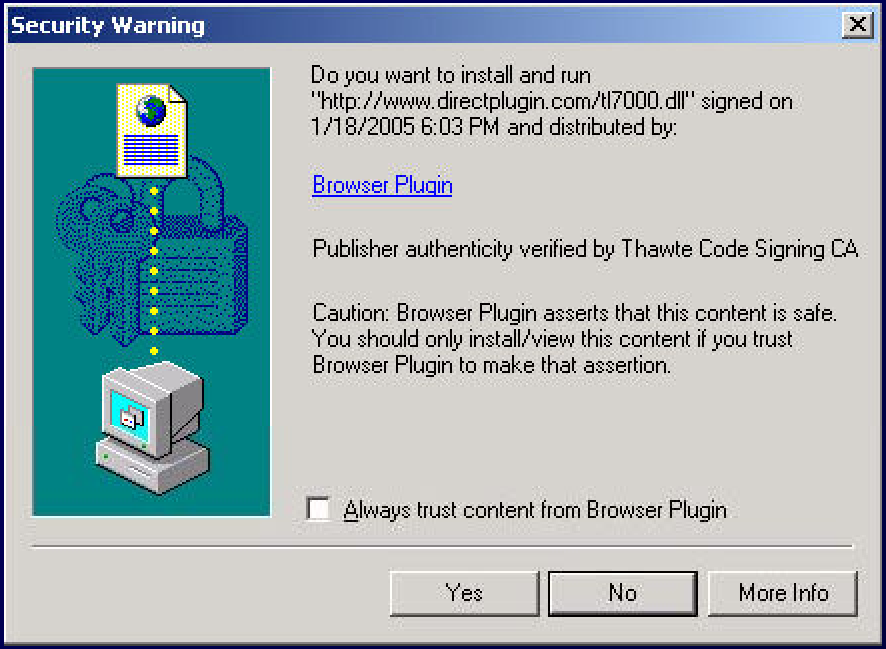
Do you want to install this software?

Name: Cult3D ActiveX Player 5.3.0.228

Publisher: **CYCORE AB**

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

What does Spyware look like?



Security Warning

Do you want to install and run "http://www.directplugin.com/tl7000.dll" signed on 1/18/2005 6:03 PM and distributed by:

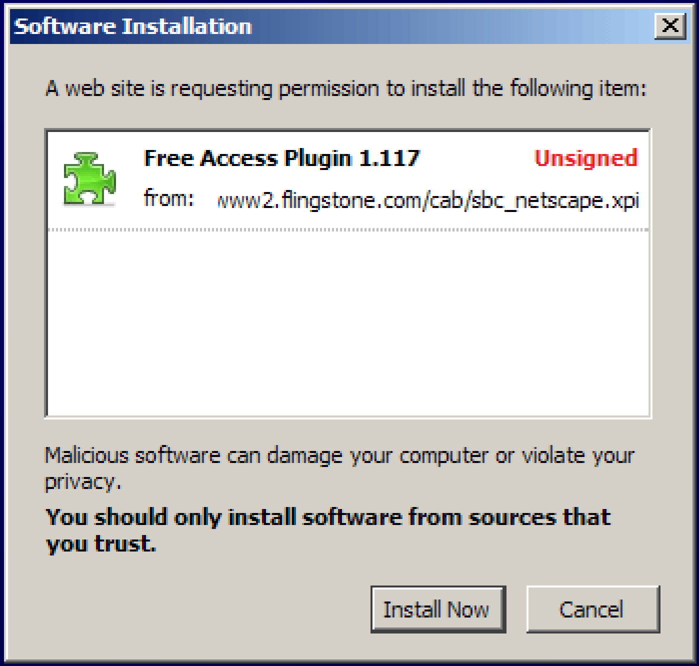
Browser Plugin

Publisher authenticity verified by Thawte Code Signing CA

Caution: Browser Plugin asserts that this content is safe. You should only install/view this content if you trust Browser Plugin to make that assertion.

□ Always trust content from Browser Plugin

What does Spyware look like?



Software Installation

A web site is requesting permission to install the following item:

Free Access Plugin 1.117 **Unsigned**

from: www2.flingstone.com/cab/sbc_netscape.xpi

Malicious software can damage your computer or violate your privacy.

You should only install software from sources that you trust.

How do I get rid of Spyware?

- Use a ***legitimate*** spyware removal program
  - Windows Defender: http://www.microsoft.com/athome/security/spyware/software/
  - Spybot: http://www.safer-networking.org/en/

How do I prevent Spyware?

- Be conscious of what you are clicking on/downloading
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it. Always look for the topmost right red X.
- Remember that things on the internet are rarely free. “Free” Screensavers etc. generally contain ads or worse that pay the programmer for their time.

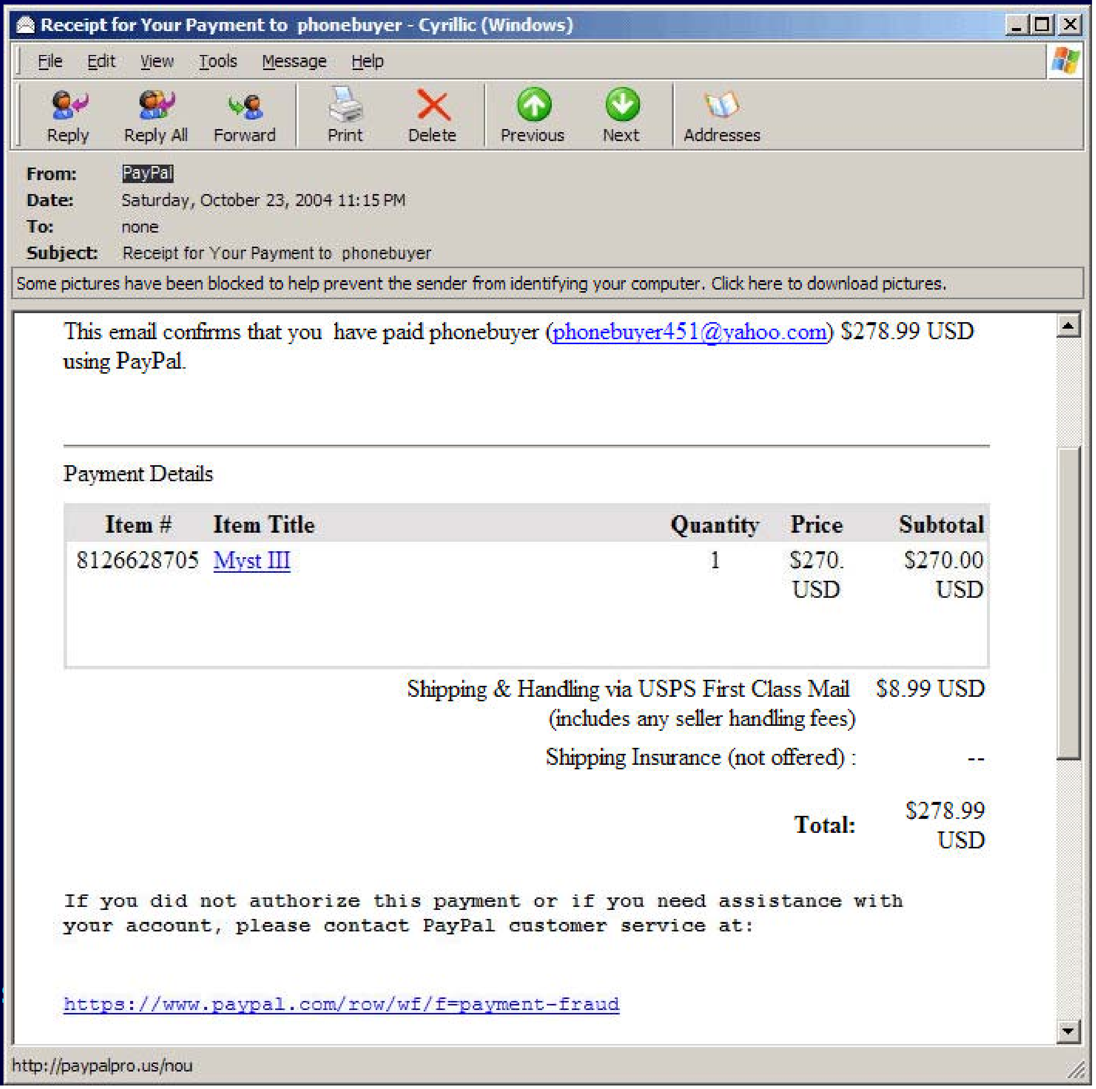
How do I get rid of/prevent Virri?

- Run antivirus software
  - http://www.washington.edu/computing/security
- Keep it up to date!
  - Virus definitions need to be updated regularly!

Phishing

- Most commonly an Email stating your account information needs updating
- Watch for URL's that are numeric or different from the link you clicked on
- Best thing to do is to type in the URL and check your account directly without following any links in the Email
- Many legitimate emails no longer contain a link (Paypal)

Phishing Examples



From: PayPal
Date: Saturday, October 23, 2004 11:15 PM
To: none
Subject: Receipt for Your Payment to phonebuyer

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

This email confirms that you have paid phonebuyer (phonebuyer451@yahoo.com) $278.99 USD using PayPal.

Payment Details

Item #	Item Title	Quantity	Price	Subtotal
8126628705	Myst III	1	$270. USD	$270.00 USD

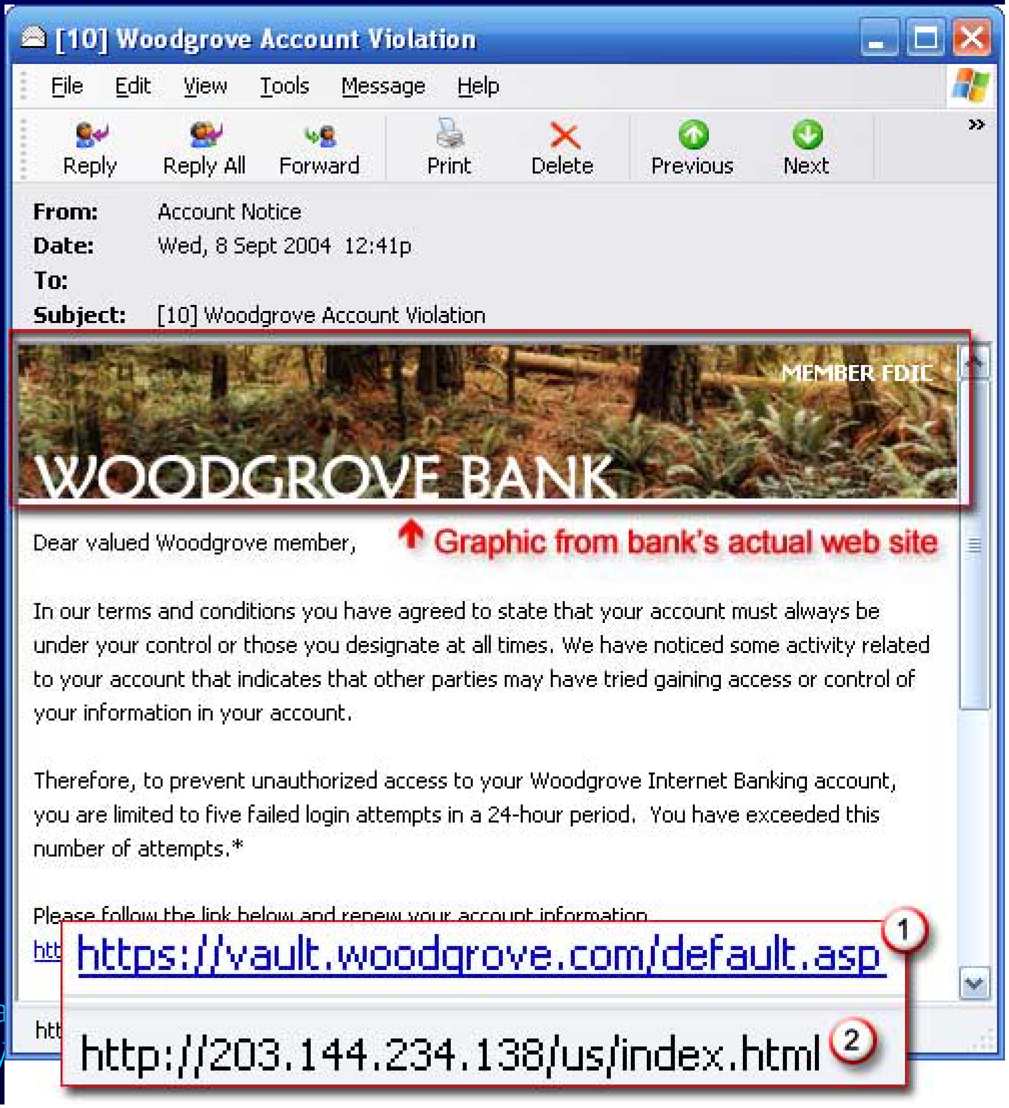
Shipping & Handling via USPS First Class Mail (includes any seller handling fees)	$8.99 USD
Shipping Insurance (not offered) :	--
Total:	$278.99 USD

```
If you did not authorize this payment or if you need assistance with
your account, please contact PayPal customer service at:
```

https://www.paypal.com/row/wf/f=payment-fraud

http://paypalpro.us/nou

Phishing Examples


[10] Woodgrove Account Violation
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
MEMBER FDIC
WOODGROVE BANK
Graphic from bank's actual web site
1
2

From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation

Dear valued Woodgrove member,

In our terms and conditions you have 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 tried gaining access or control of your information in your account.

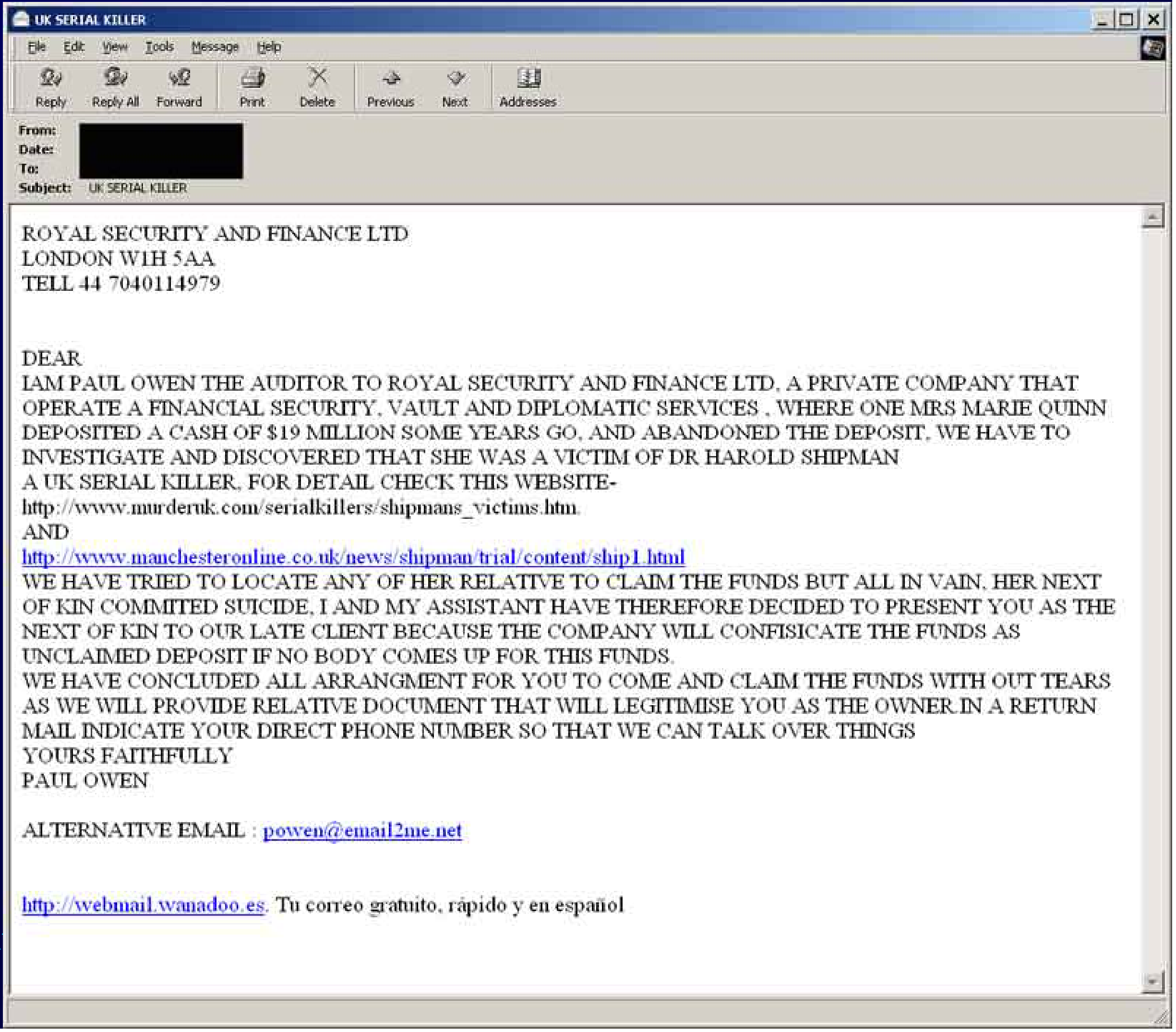
Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information.

htt https://vault.woodgrove.com/default.asp

htt http://203.144.234.138/us/index.html

Phishing Examples



From:
Date:
To:
[redacted]
Subject: UK SERIAL KILLER

ROYAL SECURITY AND FINANCE LTD
LONDON W1H 5AA
TELL 44 7040114979

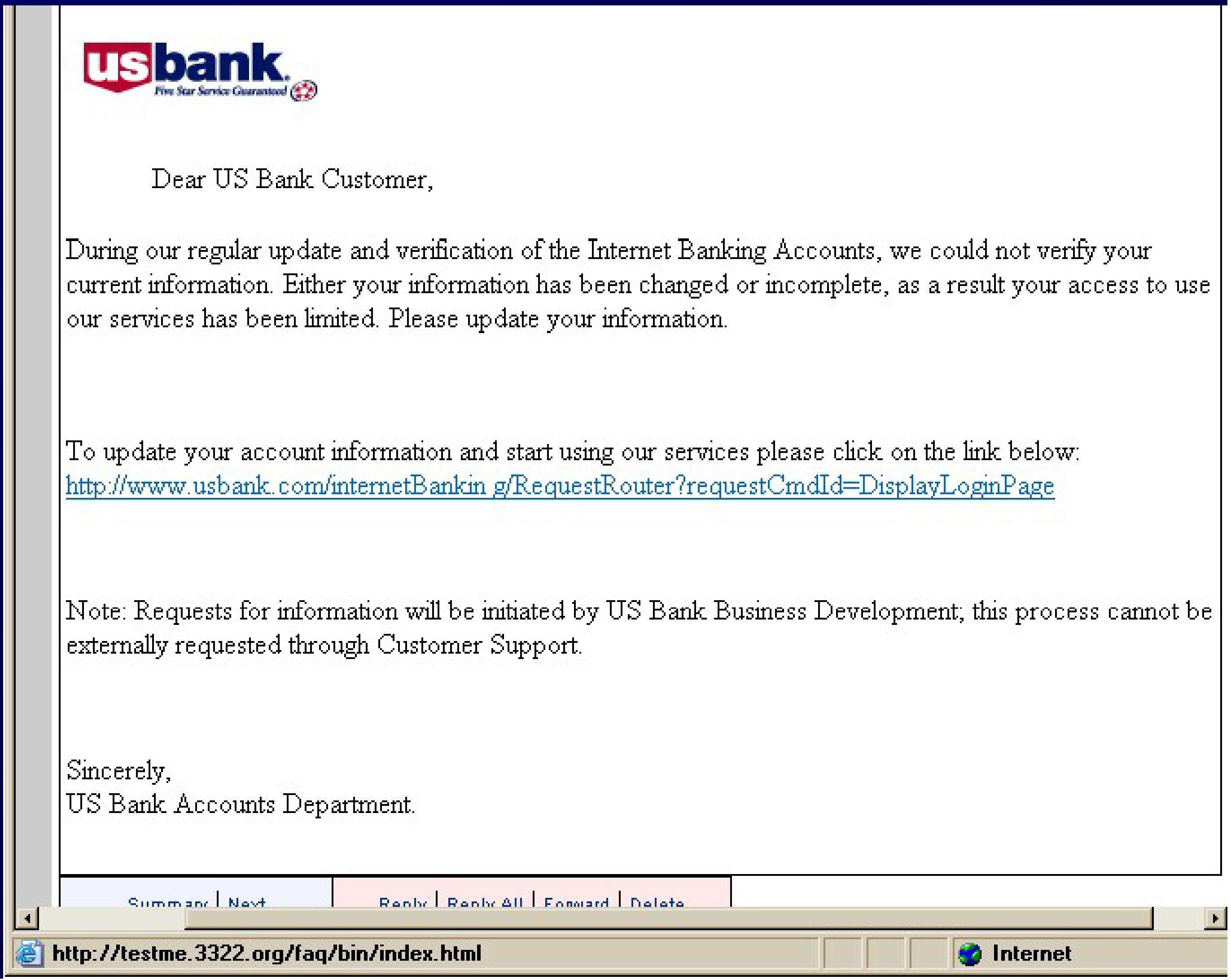
DEAR
IAM PAUL OWEN THE AUDITOR TO ROYAL SECURITY AND FINANCE LTD, A PRIVATE COMPANY THAT OPERATE A FINANCIAL SECURITY, VAULT AND DIPLOMATIC SERVICES , WHERE ONE MRS MARIE QUINN DEPOSITED A CASH OF $19 MILLION SOME YEARS GO, AND ABANDONED THE DEPOSIT, WE HAVE TO INVESTIGATE AND DISCOVERED THAT SHE WAS A VICTIM OF DR HAROLD SHIPMAN
A UK SERIAL KILLER, FOR DETAIL CHECK THIS WEBSITE-
http://www.murderuk.com/serialkillers/shipmans_victims.htm.
AND
http://www.manchesteronline.co.uk/news/shipman/trial/content/ship1.html
WE HAVE TRIED TO LOCATE ANY OF HER RELATIVE TO CLAIM THE FUNDS BUT ALL IN VAIN, HER NEXT OF KIN COMMITED SUICIDE, I AND MY ASSISTANT HAVE THEREFORE DECIDED TO PRESENT YOU AS THE NEXT OF KIN TO OUR LATE CLIENT BECAUSE THE COMPANY WILL CONFISICATE THE FUNDS AS UNCLAIMED DEPOSIT IF NO BODY COMES UP FOR THIS FUNDS.
WE HAVE CONCLUDED ALL ARRANGMENT FOR YOU TO COME AND CLAIM THE FUNDS WITH OUT TEARS AS WE WILL PROVIDE RELATIVE DOCUMENT THAT WILL LEGITIMISE YOU AS THE OWNER.IN A RETURN MAIL INDICATE YOUR DIRECT PHONE NUMBER SO THAT WE CAN TALK OVER THINGS
YOURS FAITHFULLY
PAUL OWEN

ALTERNATIVE EMAIL : powen@email2me.net

http://webmail.wanadoo.es. Tu correo gratuito, rápido y en español

fi

Phishing Examples



Dear US Bank Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

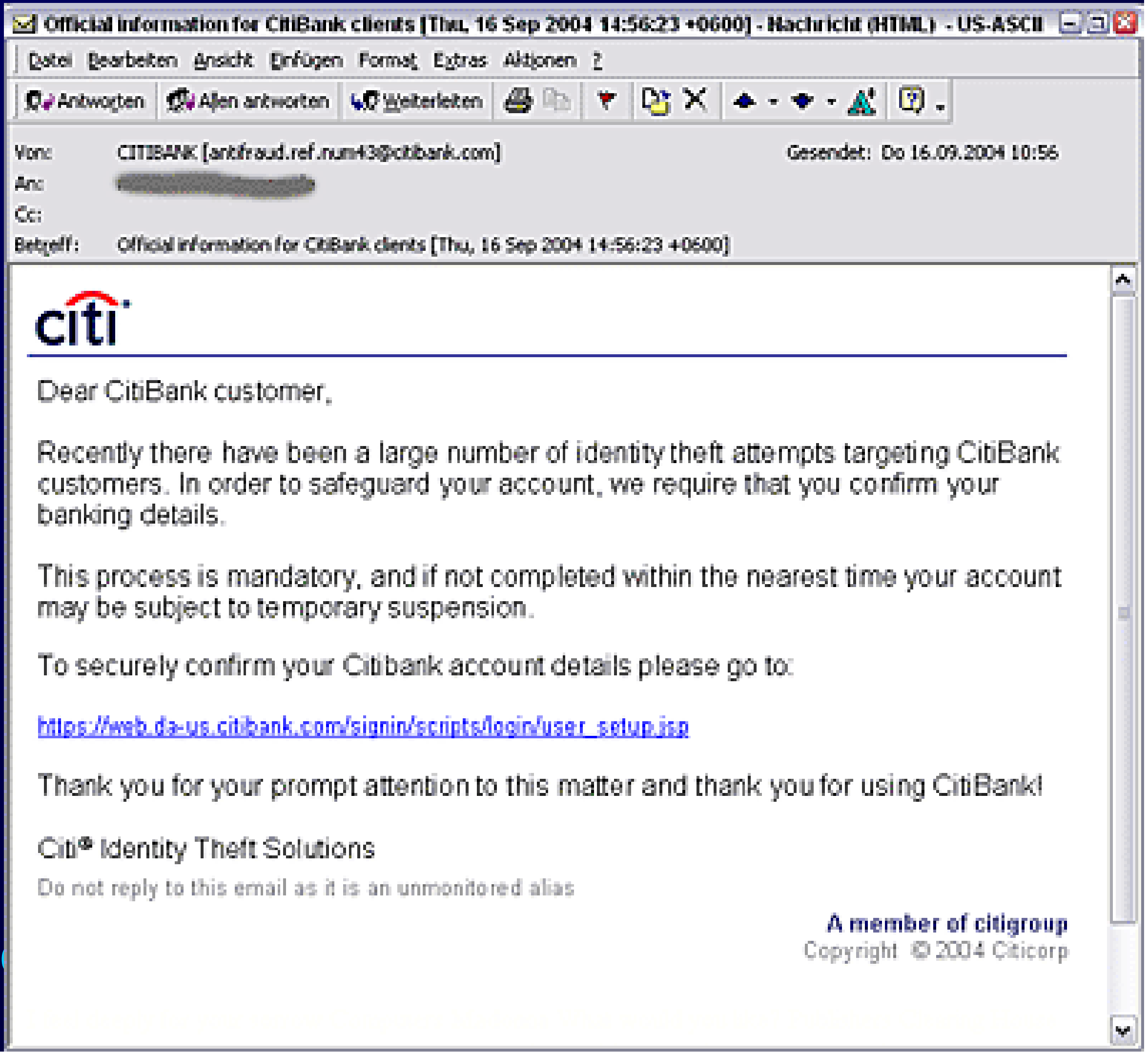
To update your account information and start using our services please click on the link below:
http://www.usbank.com/internetBankin g/RequestRouter?requestCmdId=DisplayLoginPage

Note: Requests for information will be initiated by US Bank Business Development; this process cannot be externally requested through Customer Support.

Sincerely,
US Bank Accounts Department.

http://testme.3322.org/faq/bin/index.html

Phishing Examples



Official information for CitiBank clients [Thu, 16 Sep 2004 14:56:23 +0600] - Nachricht (HTML) - US-ASCII

Von: CITIBANK [antifraud.ref.num43@citibank.com]

Gesendet: Do 16.09.2004 10:56

An: [redacted]

Cc:

Betreff: Official information for CitiBank clients [Thu, 16 Sep 2004 14:56:23 +0600]

citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

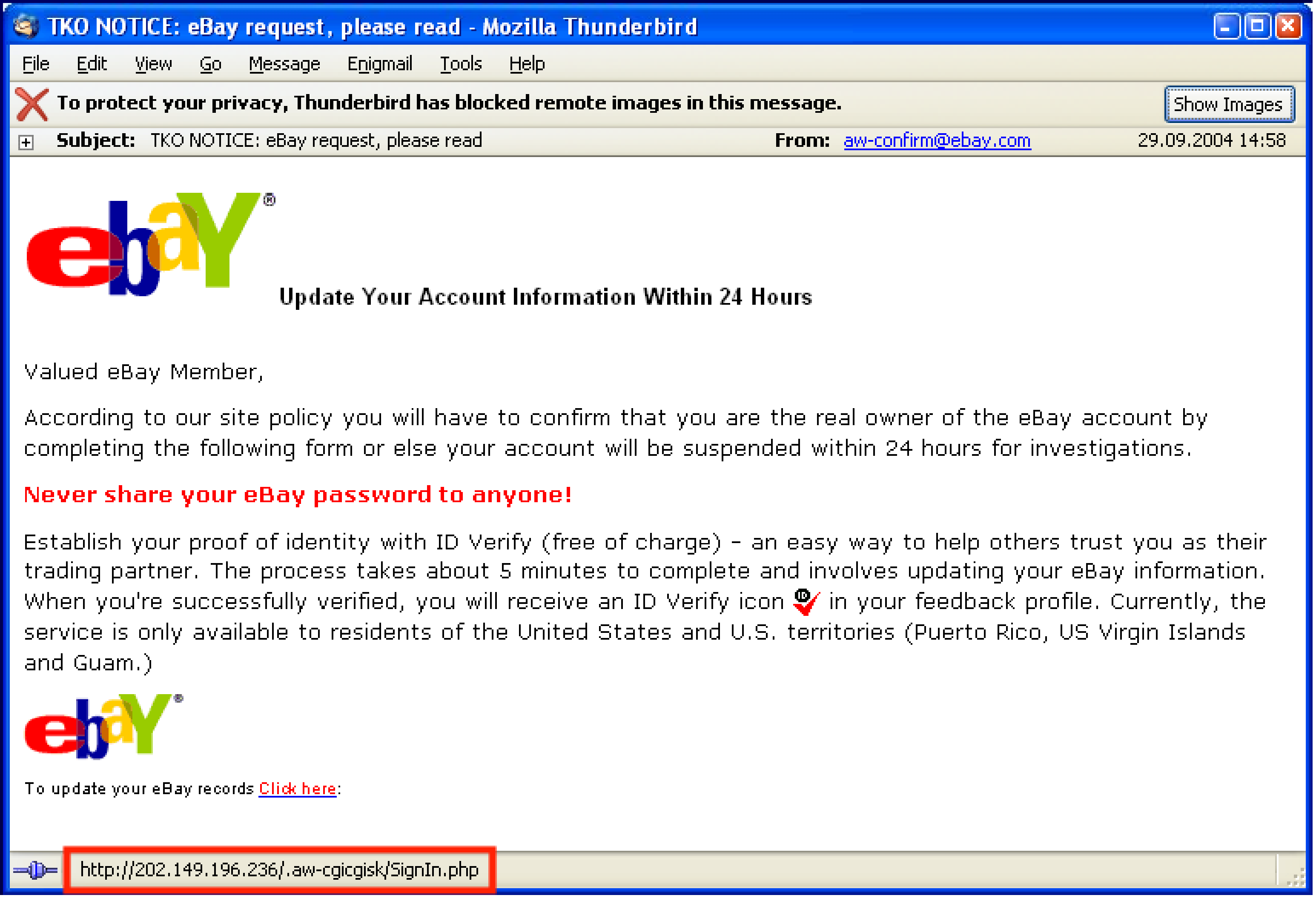
Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

Phishing Examples



To protect your privacy, Thunderbird has blocked remote images in this message.

Subject: TKO NOTICE: eBay request, please read **From:** aw-confirm@ebay.com 29.09.2004 14:58

Update Your Account Information Within 24 Hours

Valued eBay Member,

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be suspended within 24 hours for investigations.

Never share your eBay password to anyone!

Establish your proof of identity with ID Verify (free of charge) - an easy way to help others trust you as their trading partner. The process takes about 5 minutes to complete and involves updating your eBay information. When you're successfully verified, you will receive an ID Verify icon ✓ in your feedback profile. Currently, the service is only available to residents of the United States and U.S. territories (Puerto Rico, US Virgin Islands and Guam.)

To update your eBay records Click here:

http://202.149.196.236/.aw-cgicgisk/SignIn.php

How secure do you need to be?

- Be Prudent not Paranoid
- Did you initiate the action?
- Why is this free?
- Is the source trustworthy?
- When in doubt search for it!

Hackers

- White Hat
  - Very tech savvy and use powers for good
  - Security consulting, penetration testing, security audits, etc…
  - Goal is to help
- Grey Hat
  - Very tech savvy and use powers for good - sort of
  - Goal is often to help, but by doing mischievous things in the process
- Black Hat
  - Very tech savvy
  - The bad guy!
  - Goal is to “own you”

Cracking (Bad Hacking)

- Black Hats doing bad things
  - Defacing web sites
  - Stealing private information
  - Stealing money
  - Blackmail
  - Etc…

Cracking - What are their secrets?

- Social Engineering
  - Manipulating people to have them give you access
  - “Hello I am calling from tech support about the problem you submitted. Let me get your password and I will help you right away…”
- Buffer Overflow
  - Finding problems in programming code
  - Writing outside of memory location (Example - writing past the end of an array into a variable called: myPassword and saving your own password)
- Cross Site Scripting
  - One site or program is used to edit another site
  - See my example: https://faculty.washington.edu/samspade/secure/ (works in IE and Safari)

Denial of Service Attack

- Also known as a DoS attack
  - attack on a computer system or network that causes a loss of service to users
- Consuming the bandwidth of the victim network or overloading the computational resources of the victim system.
- Sort of like someone constantly calling you over and over again. You wouldn't be able to use your phone.
- If they don't affect you directly
  - May slow down your network service...
- If they do affect you directly
  - May block your network service...

Questions

- If I wanted to update a group of co-workers about a project and solicit their feedback, would I want to use a synchronous or asynchronous system?
- What communication system would work well and why?

Questions

- If I were in marketing, and wanted to “put my finger on the pulse” of a particular group of people: say candy lovers, what social technologies could I use to find out what they are thinking?