

# Maintaining Data Security in an Open Society

**Wasn't I you yesterday?**

Presenter: Jim Stickley  
TraceSecurity Inc.

[www.tracesecurity.com](http://www.tracesecurity.com)

TraceSecurity Inc Copyright 2005

# Getting Started

- Risks to your network and your members
  - Remote threats
    - Phishing
    - Man in the middle
    - Pharming
  - Internal threats
    - Breaking in while you watch

# Gone Phishing

- What is phishing?
  - URL supplied generally through an email linking to a malicious web site that impersonates a legitimate site.
  - Often times the email indicates an urgent need for the user to go to the link such as a security risk to the user.

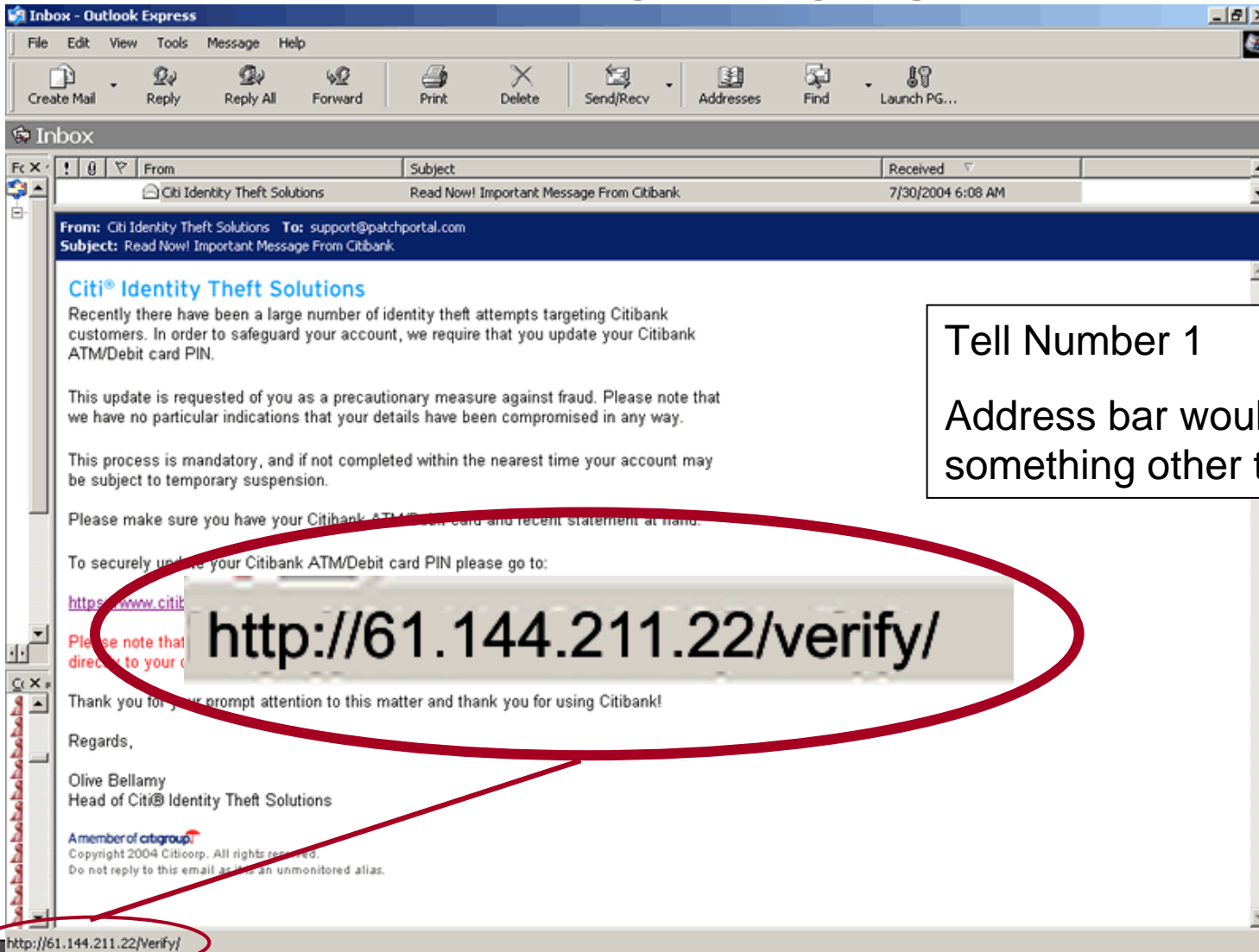
# Gone Phishing

- Malicious sites are always looking for new bait
  - Old ways to detect malicious sites have grown outdated.
  - Newer sophisticated attacks take advantage of old detection methods.
  - Many tools designed to detect phishing can be tricked.

# That was then...

- What do most people watch for?

# The "Tells"



**Inbox - Outlook Express**

File Edit View Tools Message Help

Create Mail Reply Reply All Forward Print Delete Send/Recv Addresses Find Launch PG...

**Inbox**

From	Subject	Received
Citi Identity Theft Solutions	Read Now! Important Message From Citibank	7/30/2004 6:08 AM

**From:** Citi Identity Theft Solutions **To:** support@patchportal.com  
**Subject:** Read Now! Important Message From Citibank

**Citi® Identity Theft Solutions**

Recently there have been a large number of identity theft attempts targeting Citibank customers. In order to safeguard your account, we require that you update your Citibank ATM/Debit card PIN.

This update is requested of you as a precautionary measure against fraud. Please note that we have no particular indications that your details have been compromised in any way.

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

Please make sure you have your Citibank ATM/Debit card and recent statement at hand.

To securely update your Citibank ATM/Debit card PIN please go to:

<https://www.citibank.com>

Please note that this link will direct you to your Citibank account.

**http://61.144.211.22/verify/**

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

Regards,

Olive Bellamy  
Head of Citi® Identity Theft Solutions

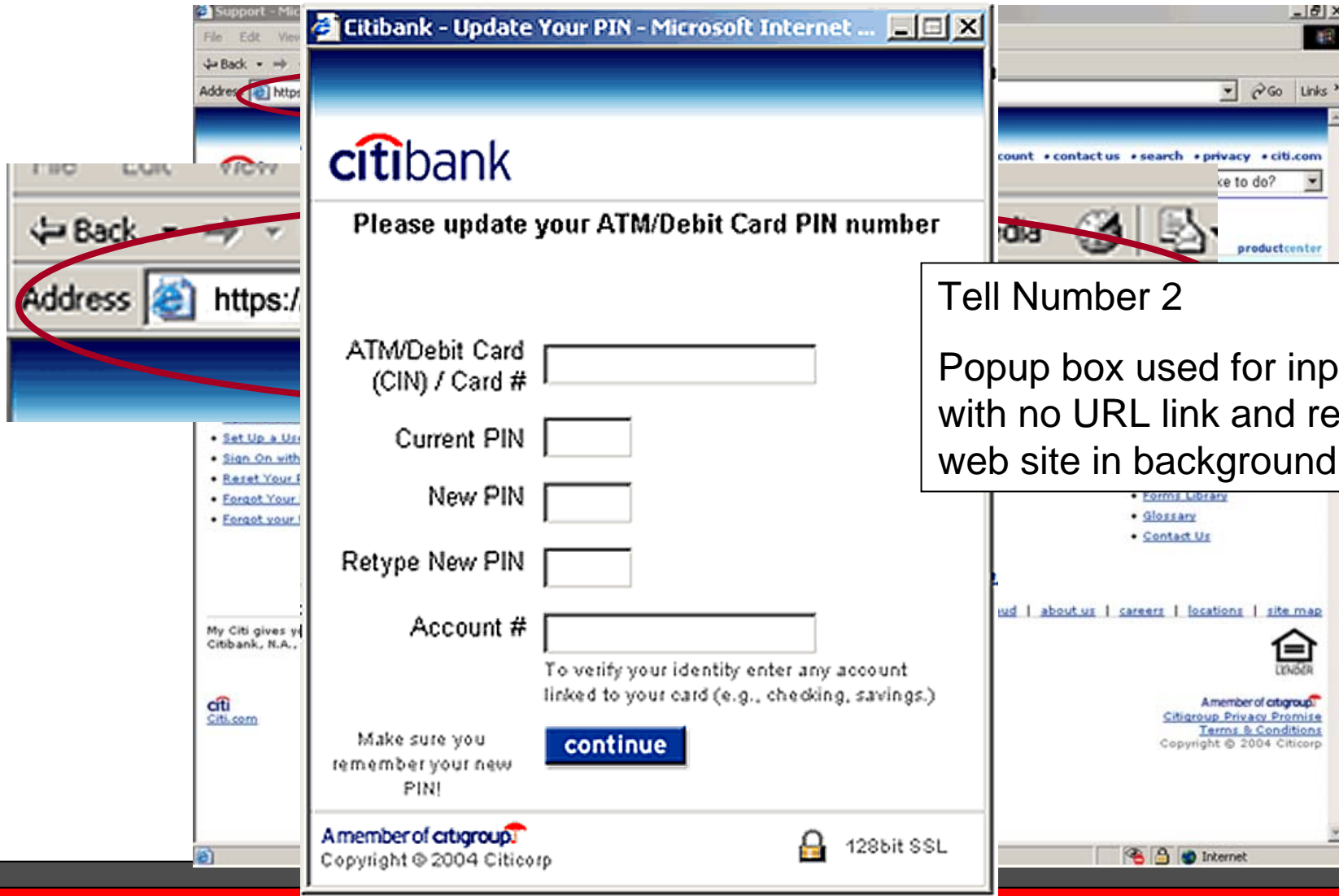
Member of citigroup  
Copyright 2004 Citicorp. All rights reserved.  
Do not reply to this email as this is an unmonitored alias.

<http://61.144.211.22/Verify/>

Tell Number 1

Address bar would point to something other than link.

# The “Tells”

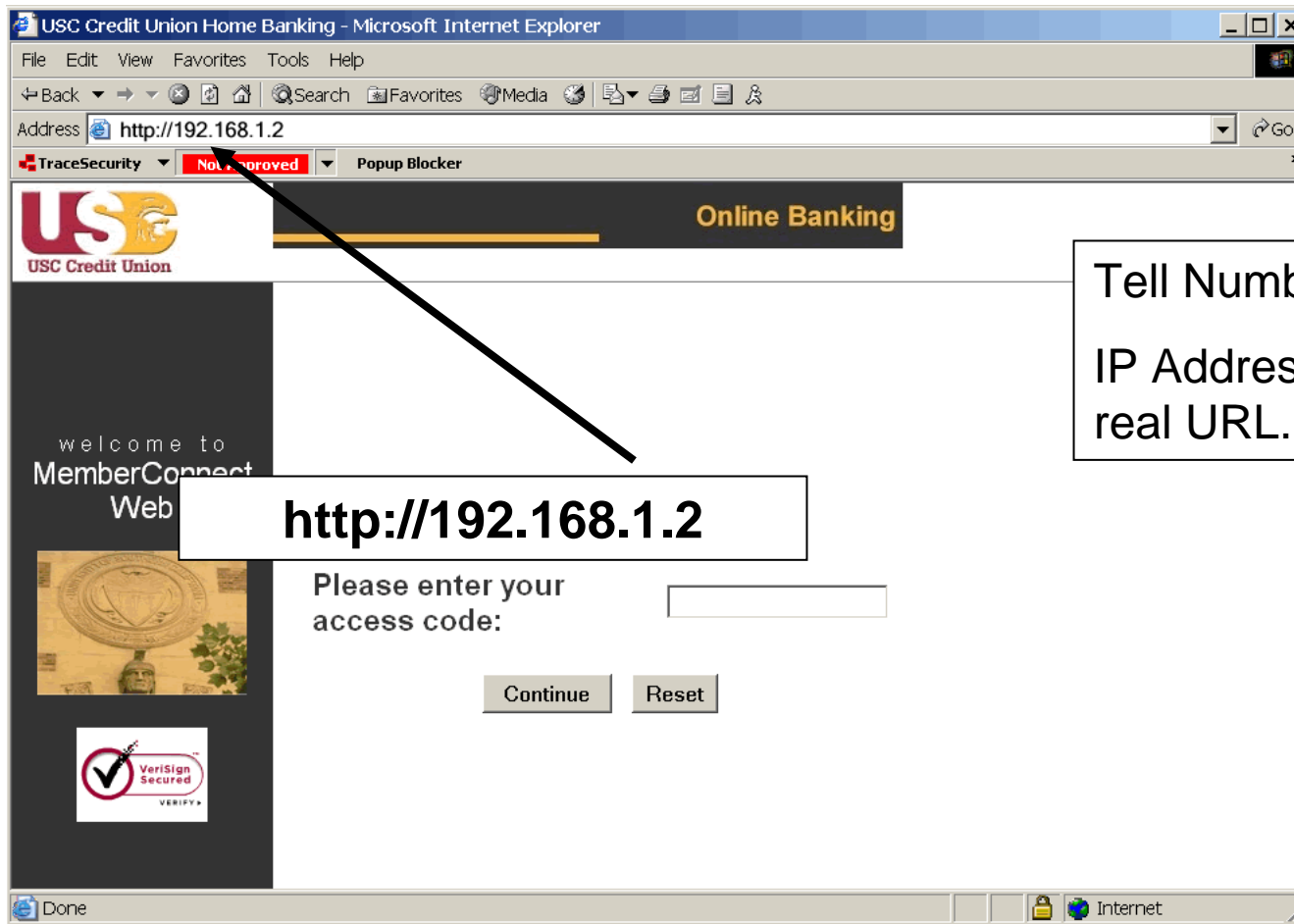


The image shows a screenshot of a Citibank web page titled "Citibank - Update Your PIN - Microsoft Internet ...". The page content includes the Citibank logo, the heading "Please update your ATM/Debit Card PIN number", and several input fields: "ATM/Debit Card (CIN) / Card #", "Current PIN", "New PIN", "Retype New PIN", and "Account #". A "continue" button is located below the "Account #" field. The page footer contains "A member of citigroup", "Copyright © 2004 Citicorp", and "128bit SSL".

Two callout boxes highlight specific elements:

- Tell Number 1:** A red circle highlights the address bar of the browser window, which contains a URL starting with "https://".
- Tell Number 2:** A white box with a black border contains the text: "Tell Number 2  
Popup box used for input with no URL link and real web site in background." A red line points from this box to the "New PIN" input field.

# The “Tells”



Tell Number 3

IP Address in place of the  
real URL.



# This is now...

- Can you still watch for the same tells?


# Seeing in believing

eBay customer notice: data confirmation [Sun, 31 Jul 2005 16:17:12 +0200]

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** eBay Inc  
**Date:** Sunday, July 31, 2005 7:17 AM  
**To:** sales@tracesecurity.com  
**Subject:** eBay customer notice: data confirmation [Sun, 31 Jul 2005 16:17:12 +0200]



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.  
To resolve this problem please visit link below and re-enter your account information:

[https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0)

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

[https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0)

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

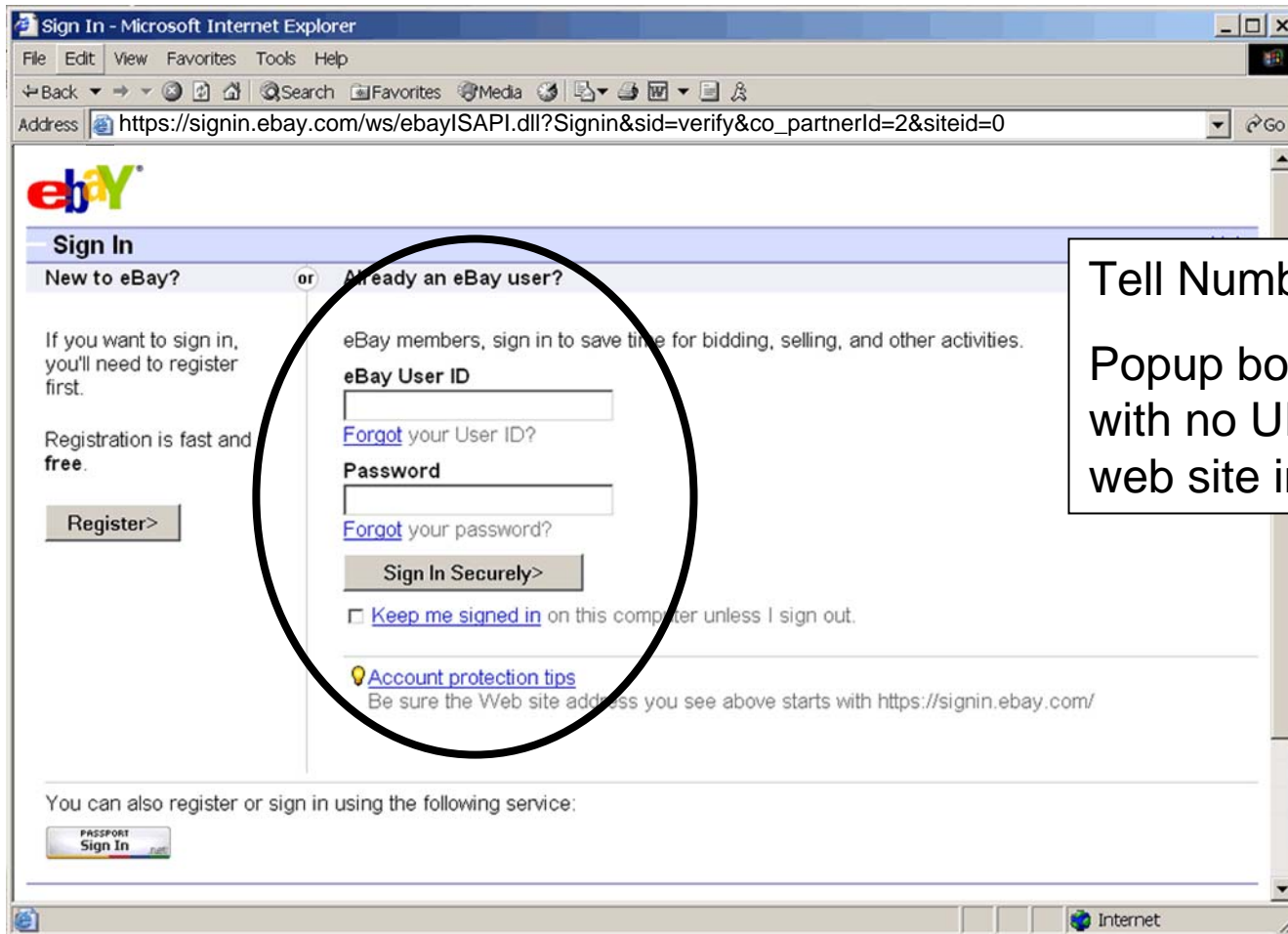
[https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0)

Tell Number 1

Address bar would point to something other than link.

[https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0)

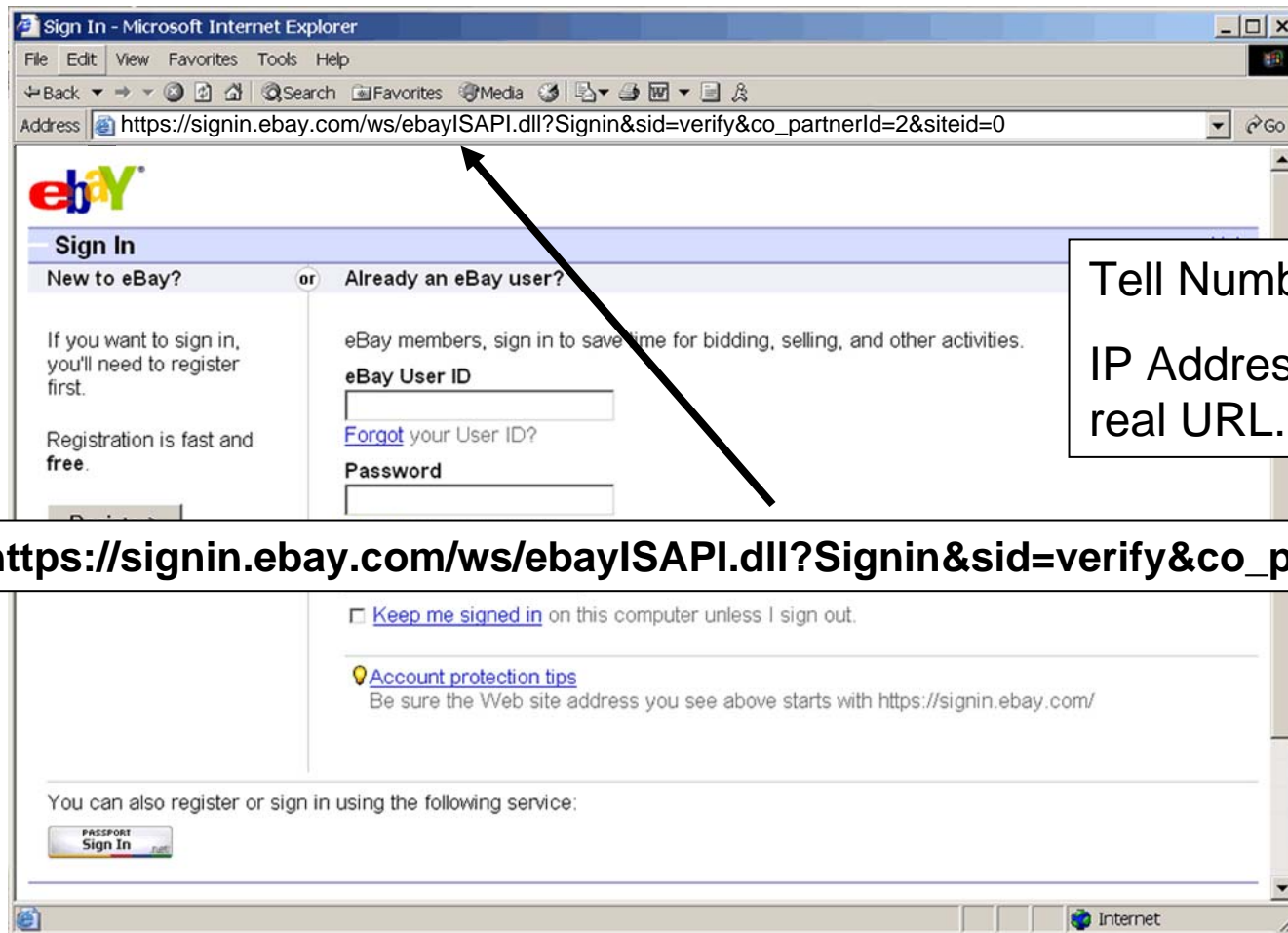
# Seeing in believing



Tell Number 2

Popup box used for input with no URL link and real web site in background.

# Seeing in believing

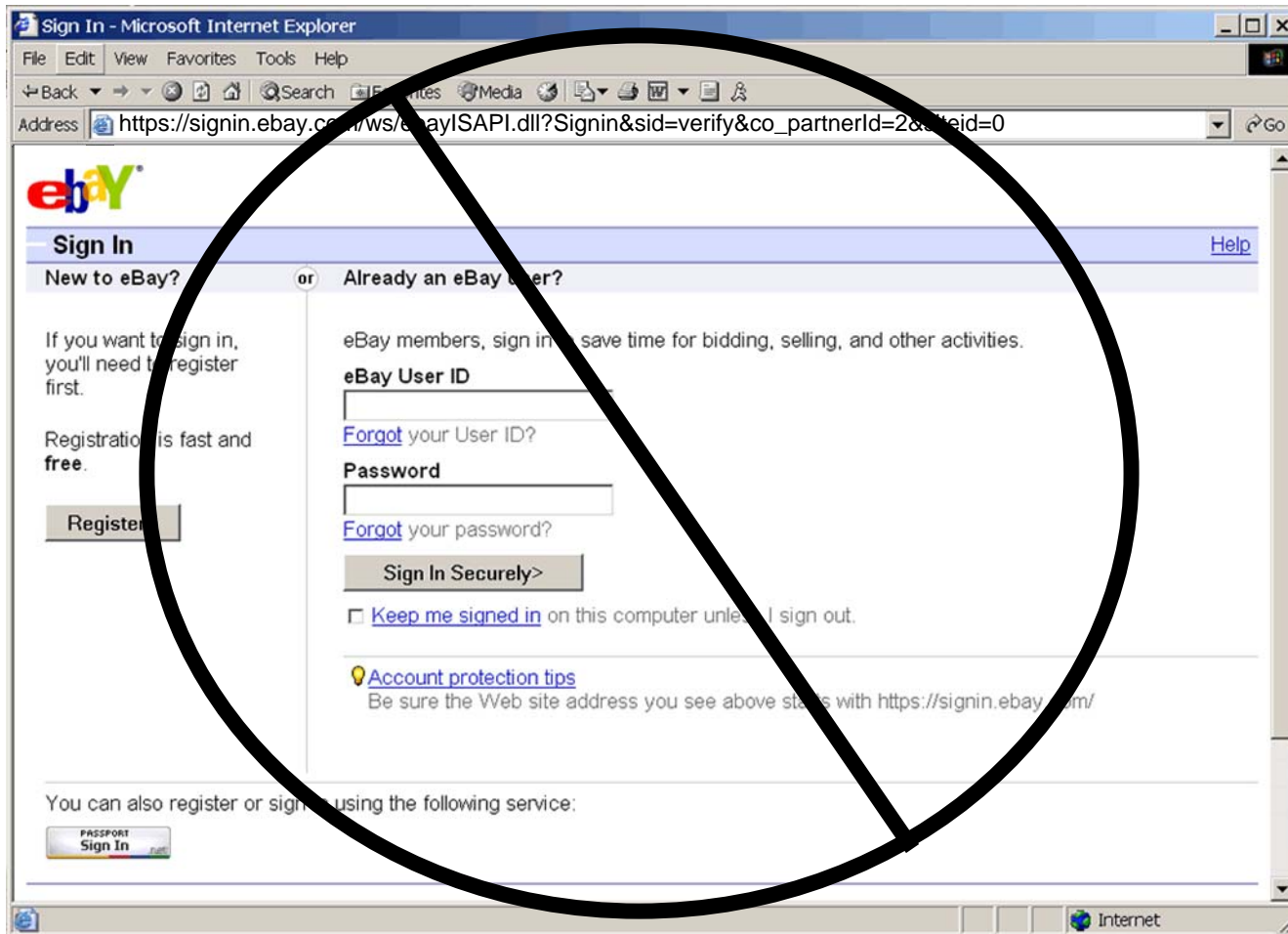


Tell Number 3

IP Address in place of the real URL.

[https://signin.ebay.com/ws/ebayISAPI.dll?Signin&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/ebayISAPI.dll?Signin&sid=verify&co_partnerId=2&siteid=0)

# Is it real?



# How was it done?

Re: eBay customer notice: data confirmation [Sun, 31 Jul 2005 16:17:12 +0200]

File Edit View Insert Format Tools Message Help

Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline

From: jlm@tracesecurity.com (Main TraceSecurity)

To: eBay Inc

Cc:

Bcc:

Subject: Re: eBay customer notice

**<MAP name=abxypml><AREA shape=RECT coords=0,0,646,569 href="http://218.1.73.209/.../e3b/"></MAP>**

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=iso-8859-1"><MAP
name=abxypml><AREA shape=RECT coords=0,0,646,569
href="http://218.1.73.209/.../e3b/"></MAP>
<META content="MSHTML 6.00.2900.5512" />
<STYLE></STYLE>
<A
href="https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0"><IMG
src="cid:part1.01010202.00000906@support_num_663046@ebay.com"
useMap=#abxypml border=0></A>
</HEAD>
<BODY>
<DIV>
<DIV><BR></DIV>
<P><FONT face=Arial><A
href="https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0"><IMG
src="cid:part1.01010202.00000906@support_num_663046@ebay.com" useMap=#abxypml
border=0></A></A></FONT></P>
<P><FONT color=#ffffff>Java Tennis Web The British Open Just tonight
</FONT></P></BLOCKQUOTE></BODY></HTML>
  
```

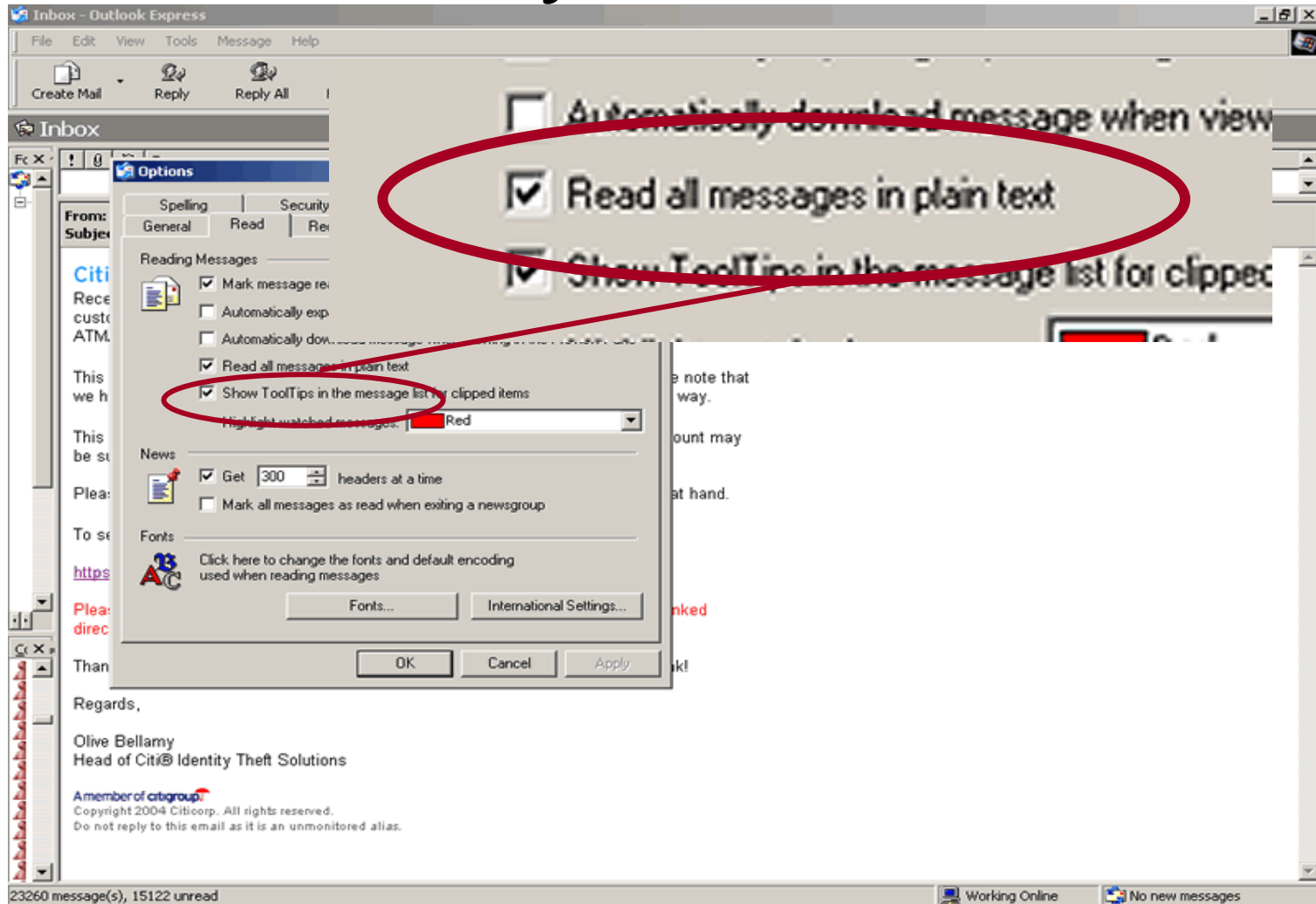
**<A href="https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\_partnerId=2&siteid=0"><IMG src="cid:part1.01010202.00000906@support\_num\_663046@ebay.com" useMap=#abxypml border=0></A>**

Edit Source Preview

# How was it done?

- Html page includes java script that creates a popup menu that displays over the real URL.
- The web page uses real images from ebay.
- After entering in confidential information, page is redirected to real ebay site.

# How do you catch it?





# How do you catch it?

- Outlook 2000
  - Must have SR-1
    - Set read as plain text
- Outlook 2002
  - Set read as plain text
- Outlook 2003
  - Convert HTML to plain text

# How do you catch it?

- Attempt to type in the URL box.
  - Will not function properly
- Minimize browser
  - Bogus URL will remain on the desktop in upper corner
- Some anti-phishing software will catch it

# How do you catch it?

- Most Important!
  - Never trust a link in an email.
- When sending emails to members that contain links, recommend that they manually type the link into their browser.

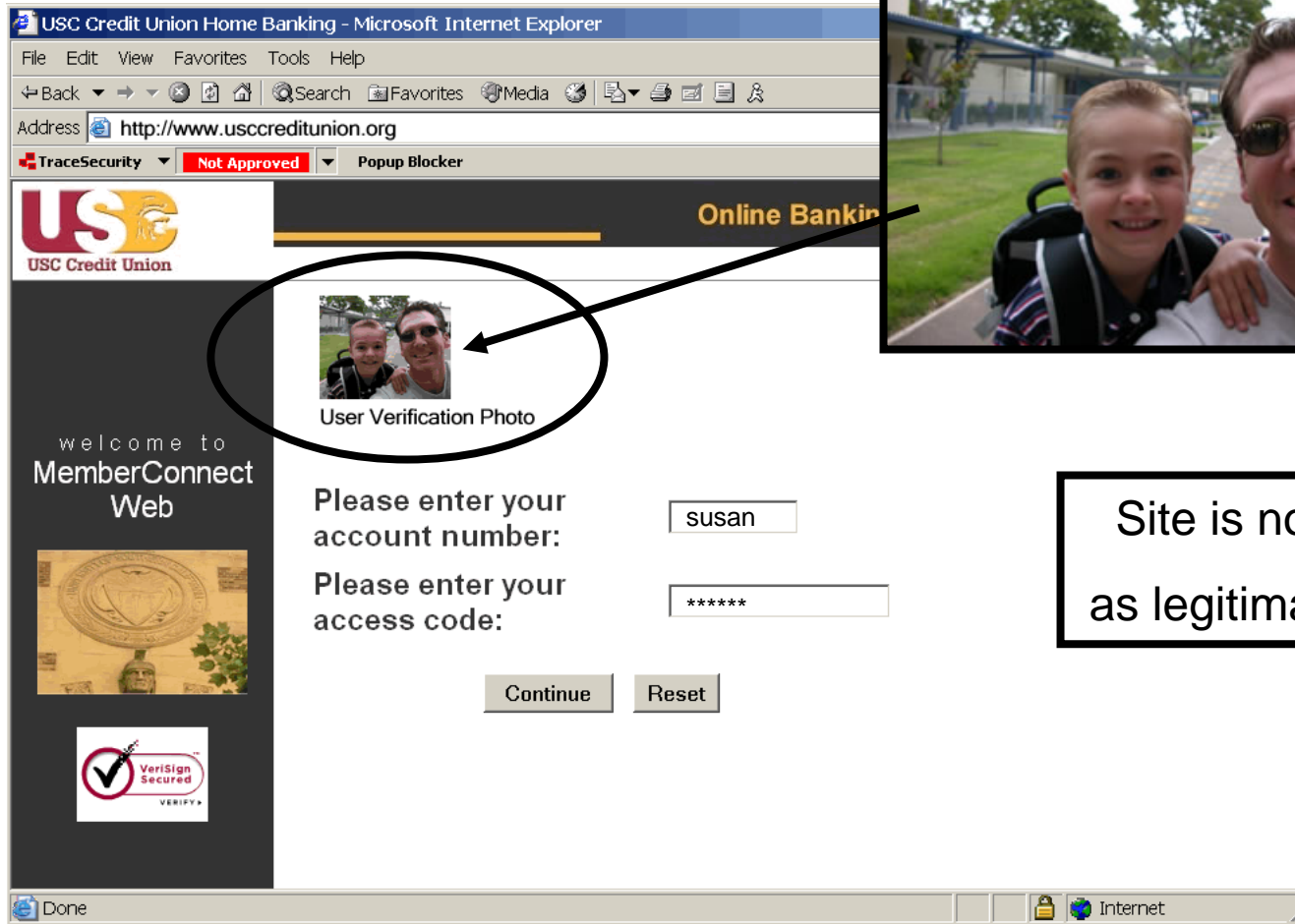
# What about Anti-Phishing?

- Many organizations are offering solutions to phishing schemes.
  - Site recognition

# Site Recognition

- The user chooses a picture, most often from a limited list on the web site that they want to see when they connect to the site.
- The idea is that a malicious site won't know what image to display and therefore the user will know they are at a malicious site.
- For this to work, a cookie is placed on the user's computer.

# Site Recognition




USC Credit Union Home Banking - Microsoft Internet Explorer


File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS

Address <http://www.usccreditunion.org>

TraceSecurity **Not Approved** Popup Blocker


 **Online Banking**


 User Verification Photo

welcome to  
**MemberConnect  
Web**

Please enter your account number:

Please enter your access code:

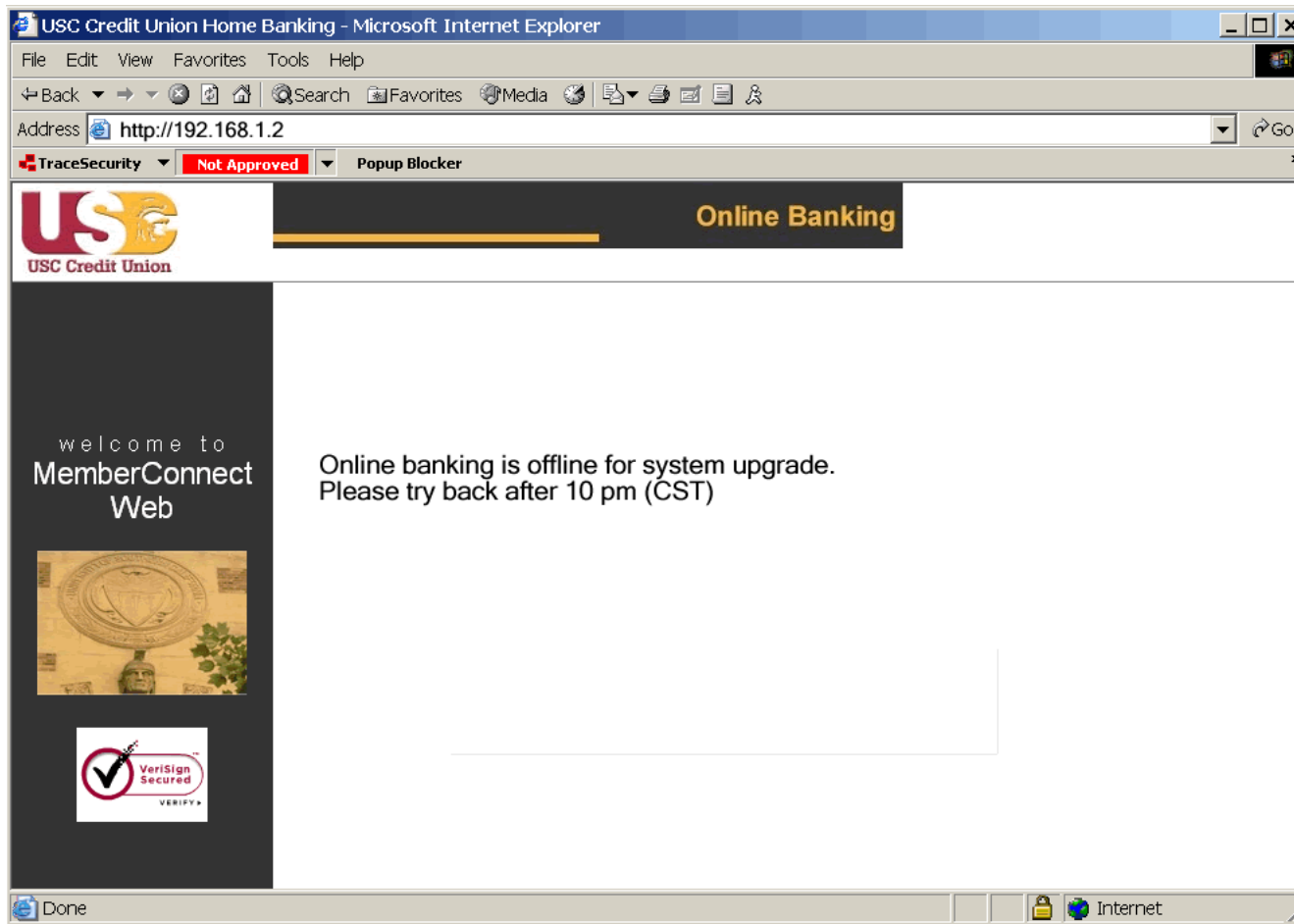


Done 

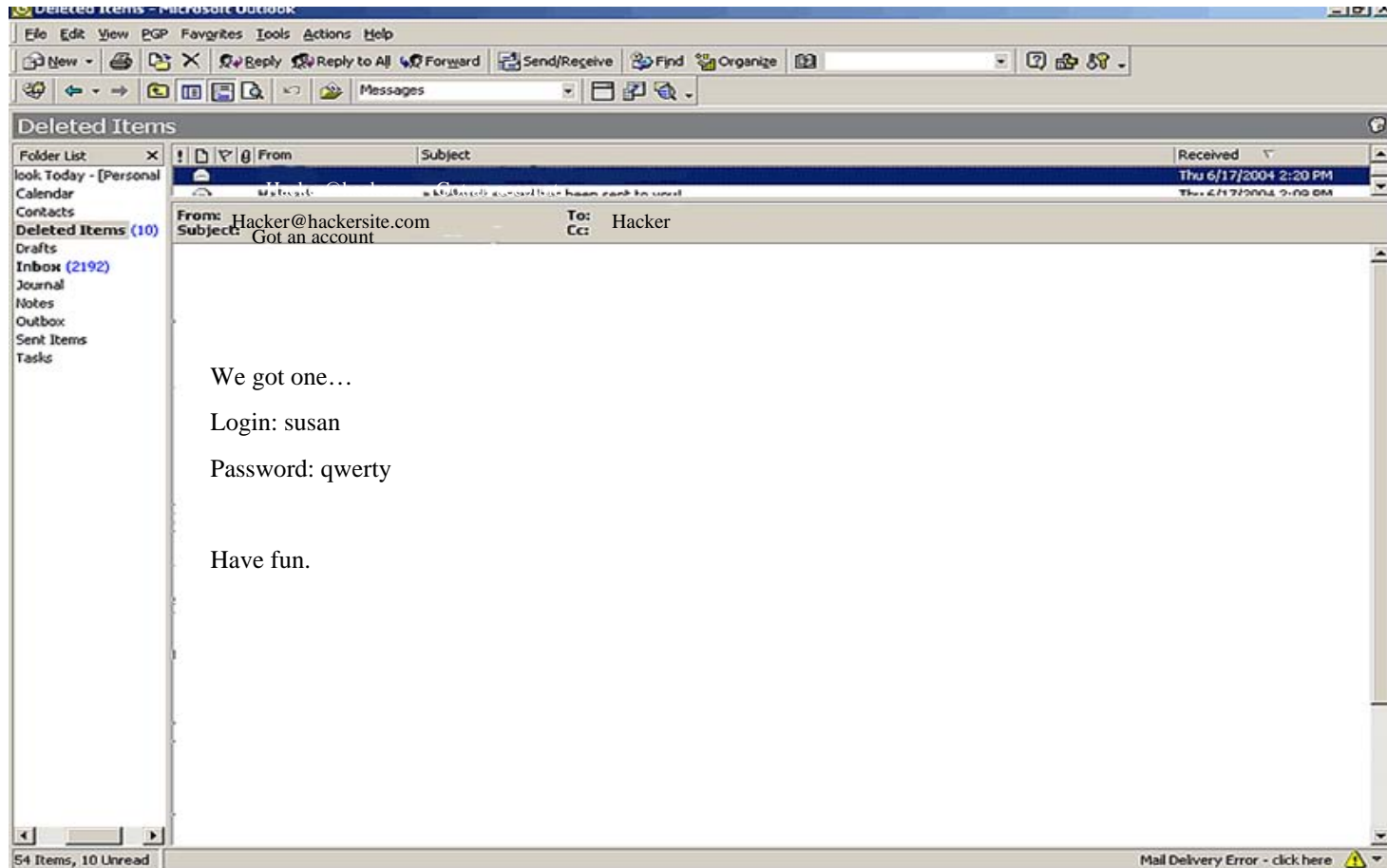


Site is now verified  
as legitimate by user

# Site Recognition



# Site Recognition

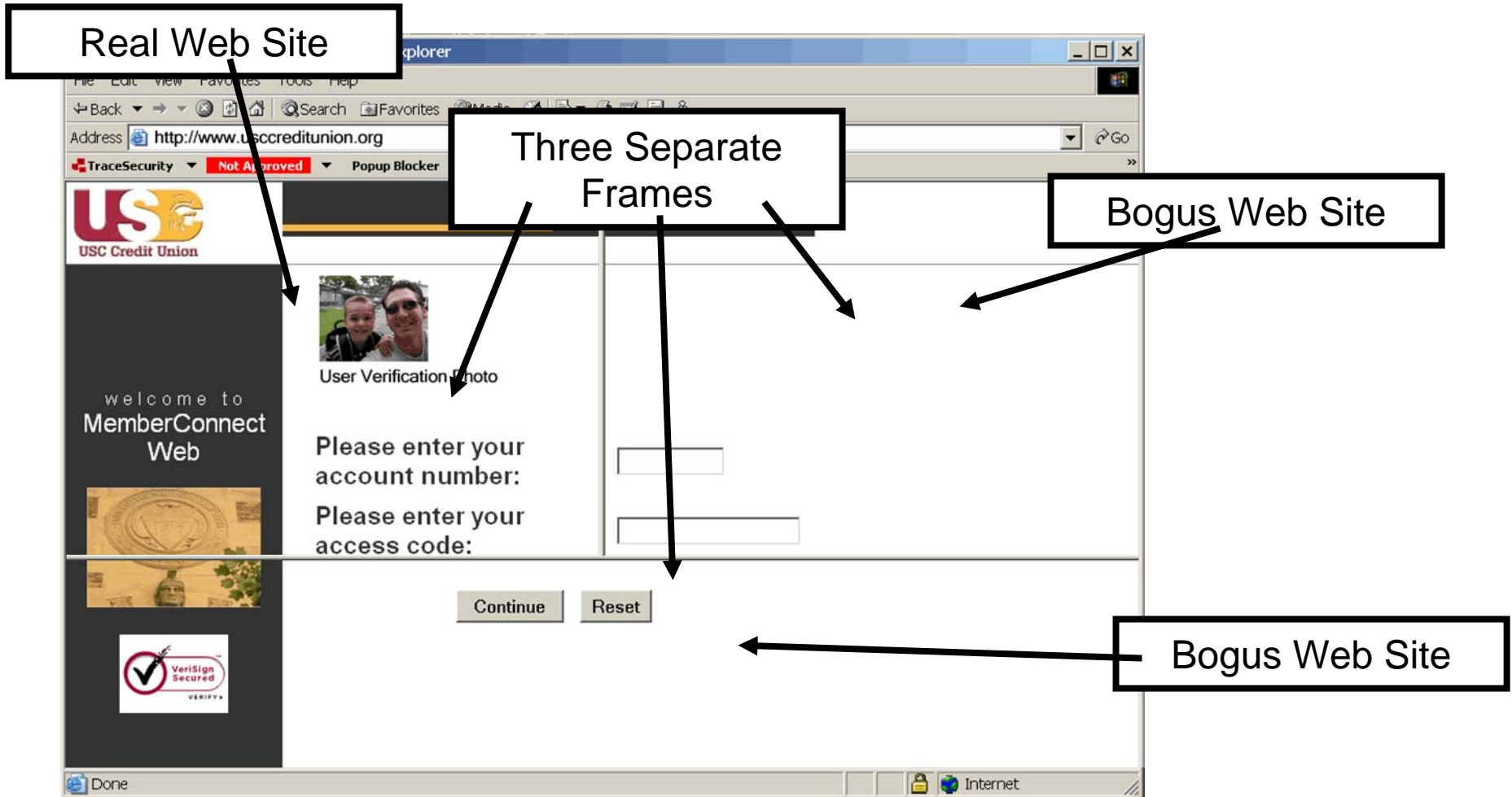




# Site Recognition

- How can that be?
  - The site had the proper URL.
  - The site showed the image that we expected.
  - The cookie on our computer was definitely used.
  - The site showed did not have any pop-ups.
- Obviously this must be the correct site..?

# Site Recognition Flaws



# What happened?

- Frames loaded the real web site
  - Tricked site into showing image via cookie
- Malicious web site used for input of data
- All pages go through SSL pages, less suspicious

# How do you catch it?

- Never allow your web page to be loaded in a frame.

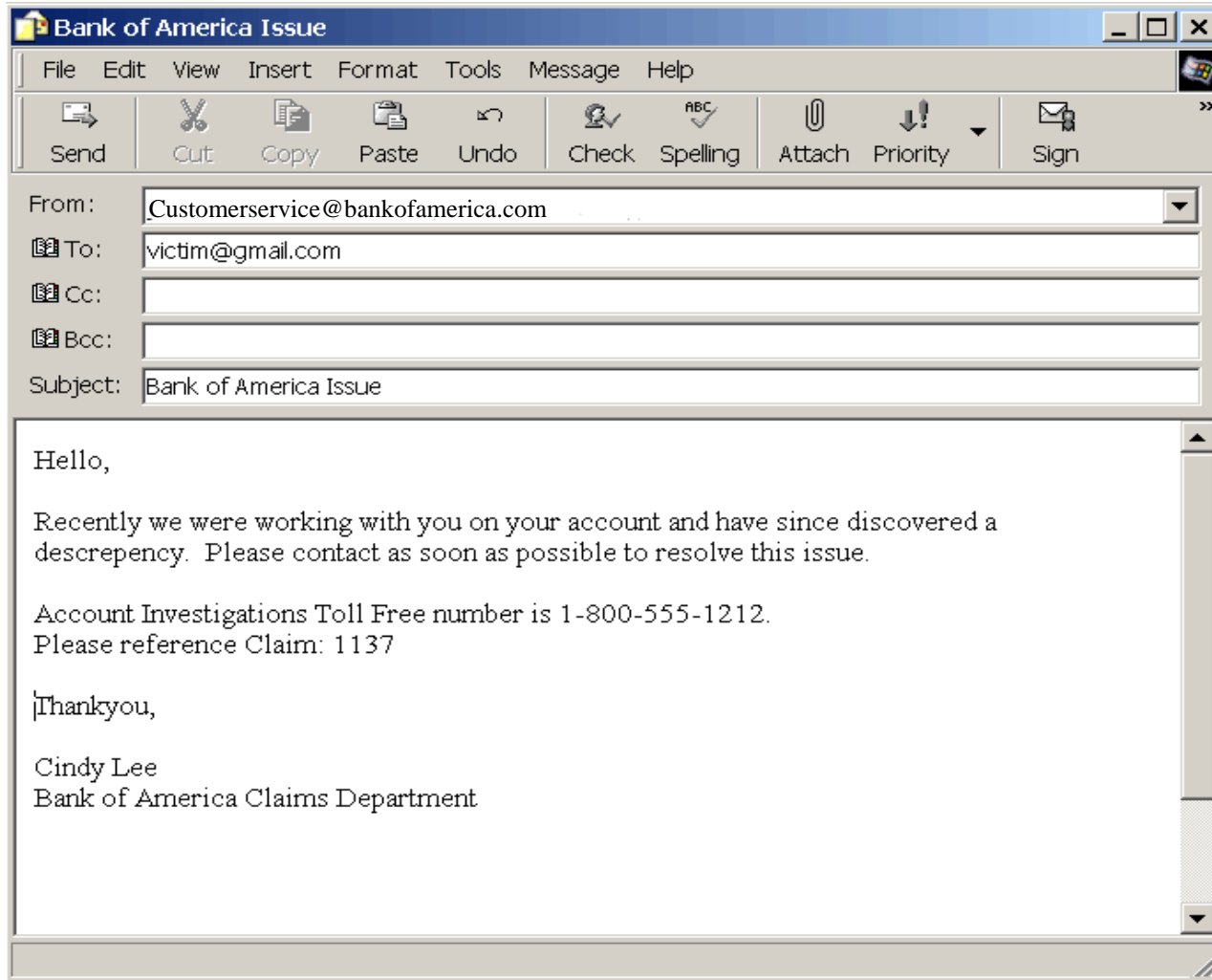
```
<script language=javascript  
  type="text/javascript"> <!-- if  
  (parent.frames.length) top.location.href=  
  document.location; // --> </script>
```

- Place image to right of input boxes.
  - More difficult to pull site into specific location

# Strategic Phishing

- Use discovered information for intimate communication.
  - Email
  - Phone Number
- Does not require knowledge of real name of victim.
- Easy and risk free to perform.
- Less risk of notification to organization.
  - Relatively few people contacted and all should be involved with organization.

# Strategic Phishing



# Strategic Phishing

- Risk
  - Customer responds to email via phone call
  - Customer tricked into revealing confidential information including last four of social, place of birth and mothers maiden name.
  - Also can be tricked into logging into bogus web site through phone call.

# Strategic Phishing

- How do you catch it?
  - Do not throw away post it notes or any other document that might contain this information.
  - Always Shred.
  - Never trust emails and information contained in emails.



# Tired of Phishing? Try Pharming

- Pharming
  - Modification of DNS to route legitimate domains to malicious web sites.

# Pharming

- DNS cache poisoning
  - Hack or modify DNS server to post malicious results.
  - Often times DNS server hosts by ISP.
  - Once server has been compromised, all hosts that resolve off server are at risk.
  - User attempts to browse to legitimate site but IP is returned pointing to malicious site often impersonating the legitimate site.

# Pharming

- **Spyware**
  - Modifies local system files to change DNS.
  - Users thinks they are connecting to real URL but system is redirected to malicious site.
  - Active X and freeware product most notorious for these kinds of attacks.
  - Used for man in the middle attacks or logging accounts.

# Pharming

- DNS Similarities
  - Register Internet Domains with similar look.
  - Often times people will guess domains.
  - Examples
    - acmeco.com
    - acmecomp.com
  
    - acmecu.org
    - acmecreditunion.org

# Pharming

- Search Engine Poisoning
  - Register similar domain.
  - Place posts in every blog that can be found
    - Make sure blogs allow <A> tags.
  - These posts will be picked up by search engine bots.
  - Over time your web site will move higher in rank than the real web site.

# Local / Onsite attacks

- *Gaining access to the network*
  - Tricks used to gain remote access to the network

# Everyone wants to be loved

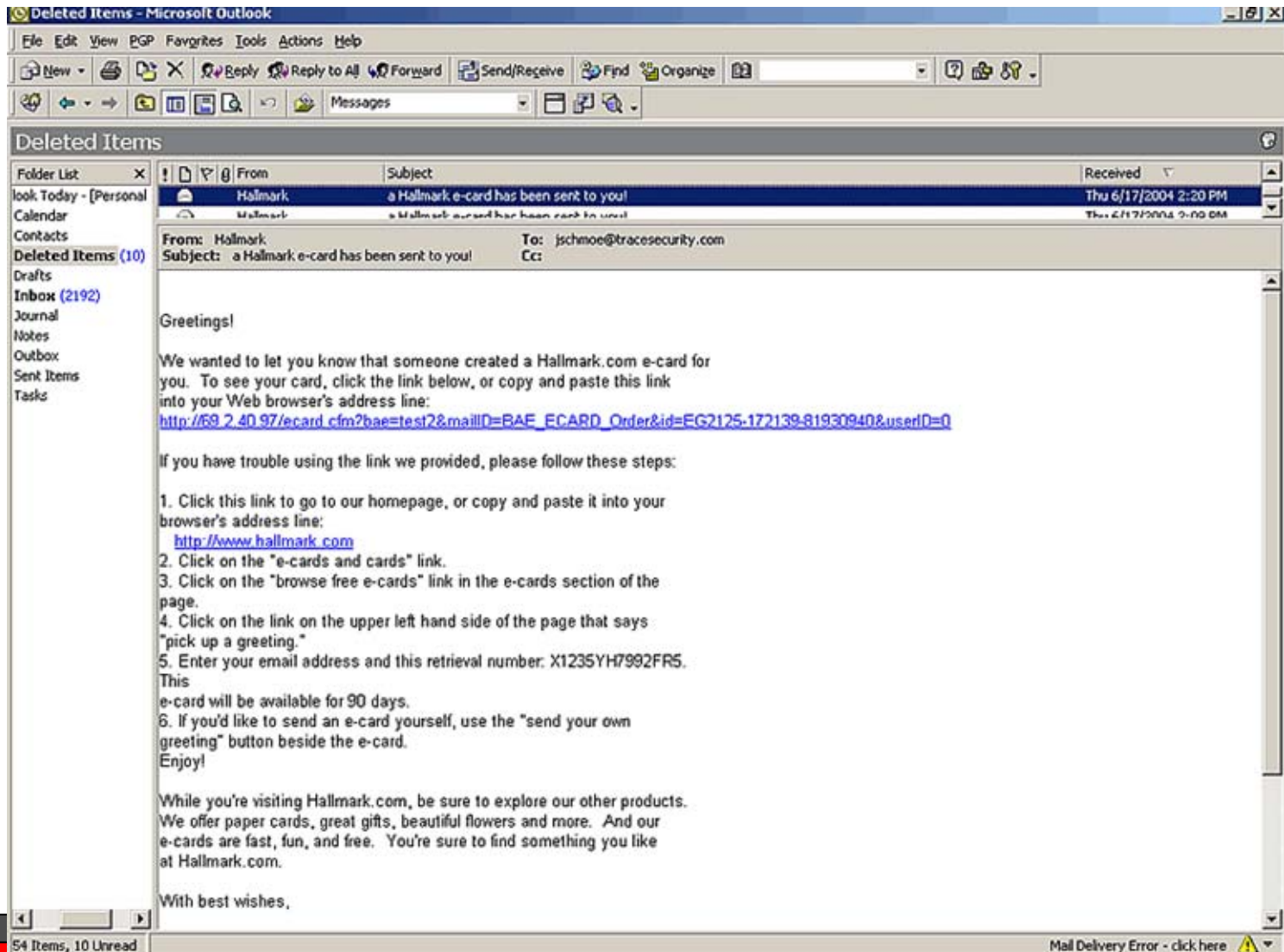
- Starting with the employees
  - Employees are often customers too
  - Employees trust other employees
  - Employees are often more willing to break the rules on themselves than on a customer
  - Employees follow managerial requests
  - Employees already have access to the internal network
  - Employees outside of systems admins often have limited technical experience

# Everyone wants to be loved

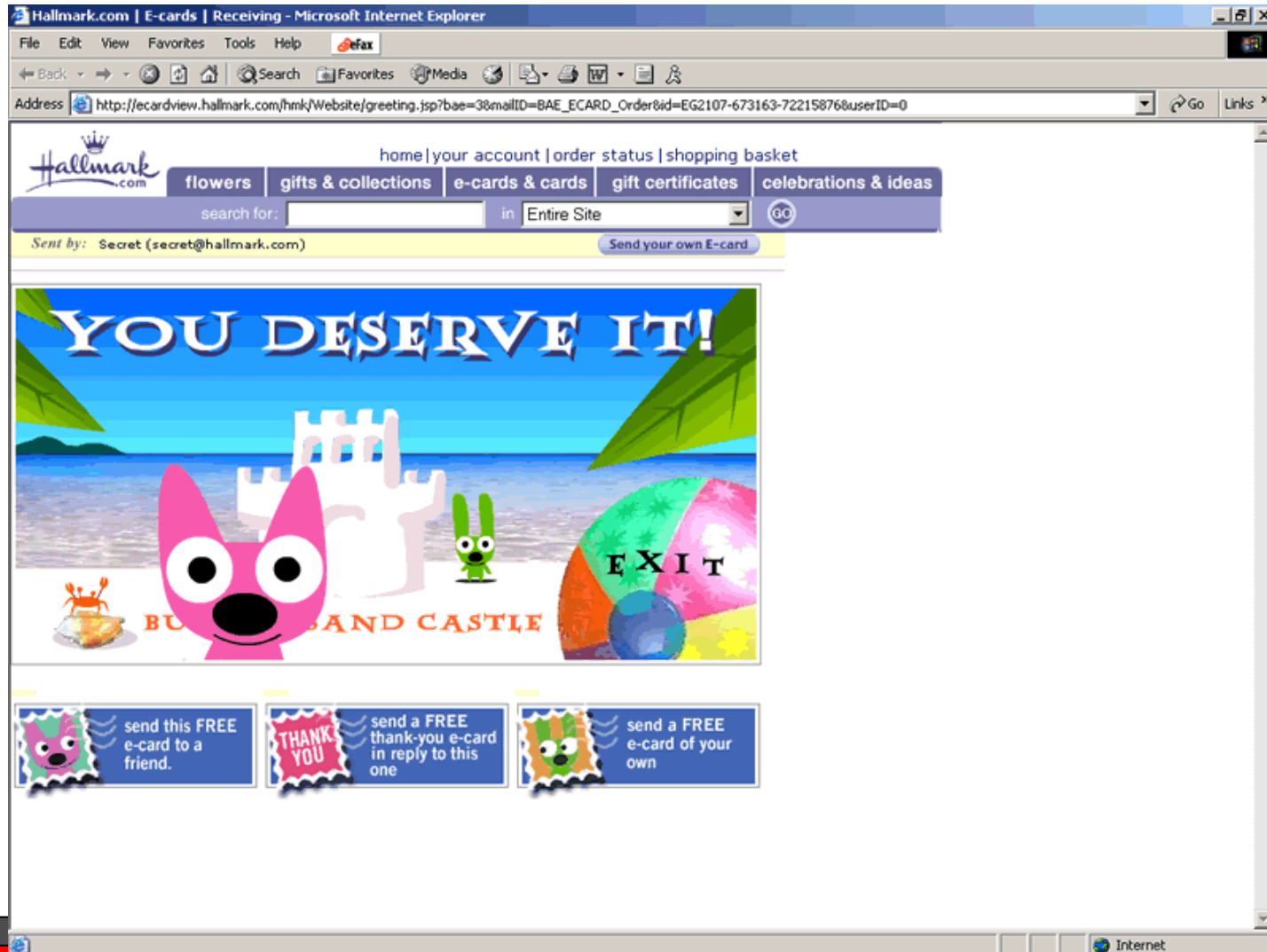
- Gaining access to the internal network
  - Target: Organization Employees
  - Type: Malicious web site attack
    - Send email on behalf of legitimate source
    - Include URL to malicious web site
    - Entice employee to click the URL
    - Execute attack through new vulnerability
  - Goal: Organization internal network access
  - Use: Gain access to employee computer installing trojans and reverse telnet software allowing remote attacks directly to the internal network
  - Difficulty: **Low**
  - Resolution: **Difficult**



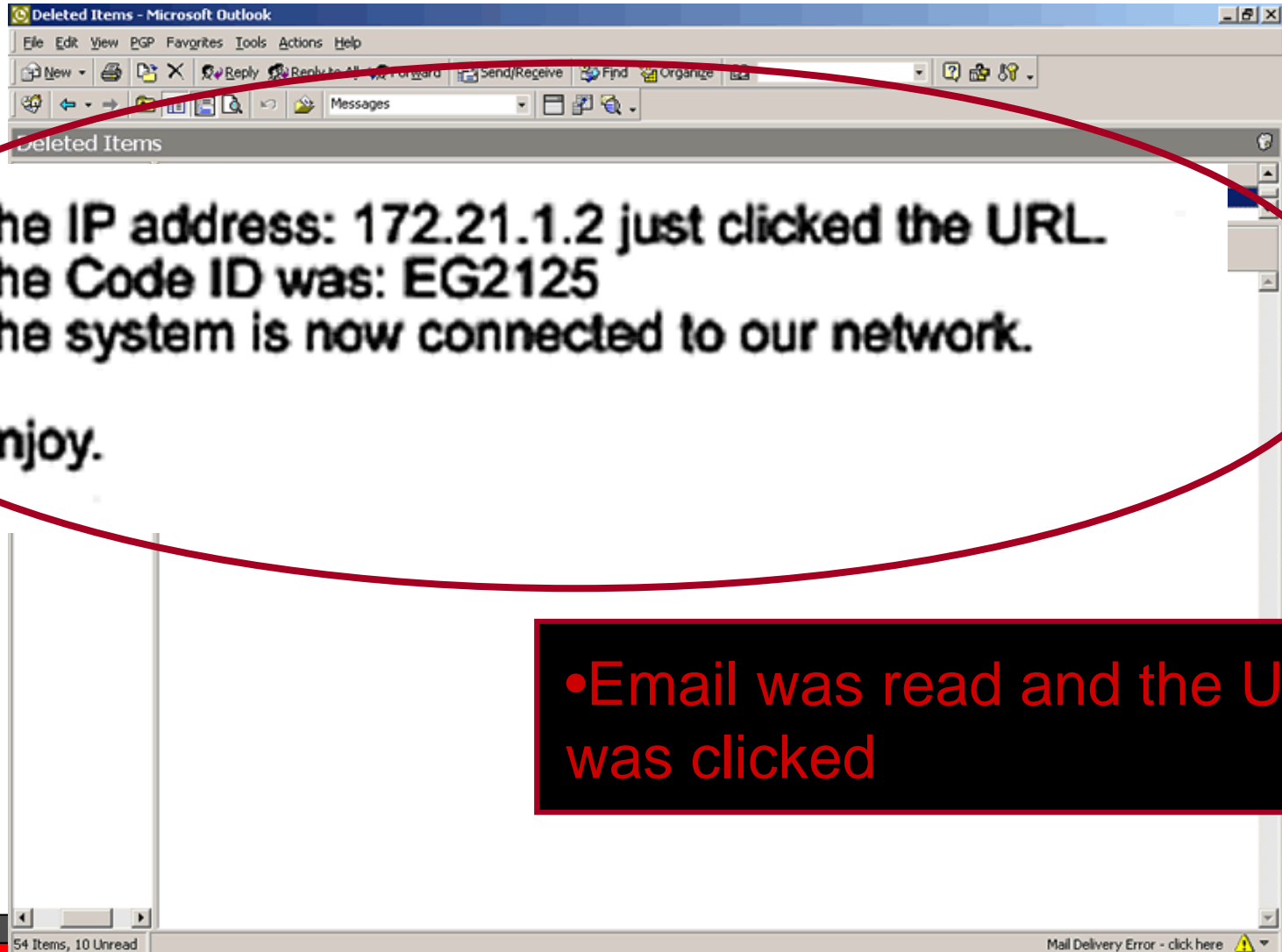
# Everyone wants to be loved



# Everyone wants to be loved

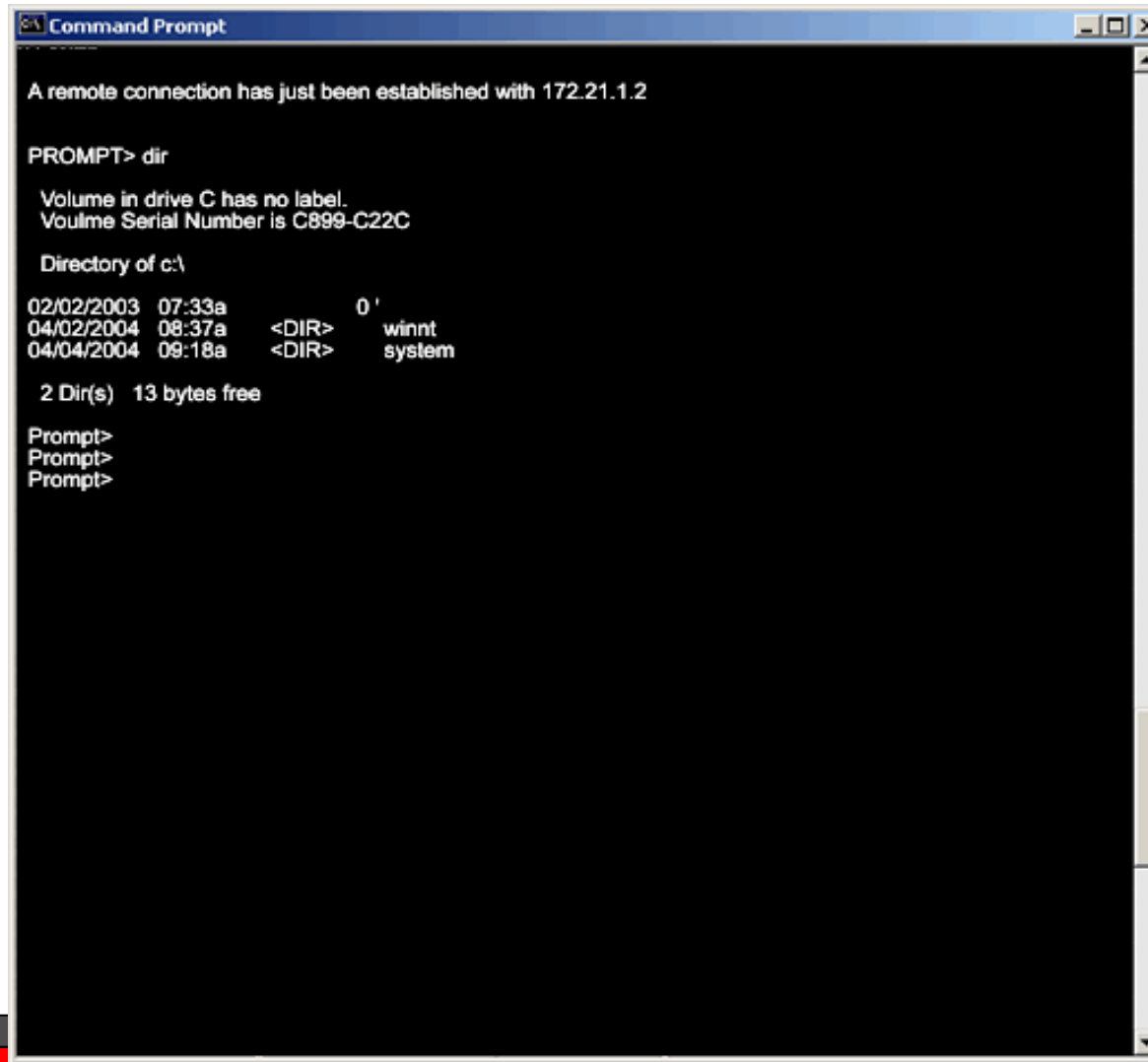


# Everyone wants to be loved



- Email was read and the URL was clicked

# Everyone wants to be loved



```
Command Prompt

A remote connection has just been established with 172.21.1.2

PROMPT> dir

Volume in drive C has no label.
Volume Serial Number is C899-C22C

Directory of c:\

02/02/2003  07:33a           0 '
04/02/2004  08:37a     <DIR>      winnt
04/04/2004  09:18a     <DIR>      system

2 Dir(s)  13 bytes free

Prompt>
Prompt>
Prompt>
```

# How was it done?



# Everyone wants to be loved

- Bypassing security devices
  - Connection is created from the internal users computer out to internet
  - Connection opens on standard port such as 443 (SSL)
  - Exploit is not known to IDS signatures so is not flagged
  - Not seen as a known virus so AV does not block
  - Some personal firewalls will see this as potential security issue but common executable names often trick users
  - Review of logs simply shows secured web traffic on network

# Everyone wants to be loved

- Risk and Resolution

- **Risk**

- Complete and total compromise of internal network by remote hacker
    - Launch point for other internal attacks including against core processor
    - Launch point to create additional trojans on internal network
    - Can establish link that “calls home” at scheduled times
    - Even if e-mail is only read but the URL is not clicked, useful information has been gathered

# Everyone wants to be loved

- Risk and Resolution
  - **Resolution**
    - Disable auto-preview
    - Never trust links in email with IP address
    - Personal firewalls at each desktop
    - User training and awareness
    - Proxy web browsing (Both HTTP and SSL)



# Local / Onsite attacks

- *Guess who stopped in for visit...*
  - Tricks used to gain physical access to your organization

# Did you shred?

**Employee Schedules**

**Loan Applications**

**Confidential documents / procurements**

**Doctors Prescriptions**

**Post-it notes with member information**

**Bank Statements**

**Personal Bills such as phone bill, credit card bill, etc.**

**Social Security Numbers**

**Internal emails**

**Overdrawn Reports**

**Teller drawer receipts with teller ID number**      **Balance Sheets**

# Local / Onsite attacks

- **Vendor Sales**

- Arrive as doing a sales call
- Bring associate
- Associate leaves every chance they get
  - Cell phone calls
  - Bathroom
  - Smoke
- Send product for testing
  - Software
    - Free software can come with a price
  - Hardware
    - Beware of the free keyboard



# Local / Onsite attacks

- **The Wanderer**
  - Wander the office gathering information
  - Act like you belong and no one asks questions
  - Get caught, drop name of employee
    - Better if they are not there
  - Take what you can grab

# Local / Onsite attacks

- Fire Marshall

- Everyone loves a man in a uniform
- Complete access to facility by law
- Left alone most of the time
- Demands respect and is seen as trusted figure



# Local / Onsite attacks

- **Pest Control**

- Complete access to facility
- Left alone most of the time
- Seen as low brow and not a threat
- Easy access to cables and phone lines
- Expected to be snooping around under desks



# Local / Onsite attacks

- **Second Day Visit**

- Arrive the first day for scheduled reason (sales call)
- Come back second day and walk past all security
  - Say you are meeting same person as before
- Have complete run of the building



# Local / Onsite attacks

- OSHA
  - Send letter informing of inspection
  - Arrive on site and inspect the facility
  - Before leaving facility install logged keyboards



# Local / Onsite attacks

- **Air Conditioning Repair**
  - Complete access to the building
  - Always left unattended
  - Seen as low level threat
  - Bump ceiling tiles a lot to make dust and get person to leave office
  - Always carry bags for equipment



# Local / Onsite attacks

- Local ISP or Phone Company
  - Create Issues
  - Contact on behalf of company
  - Visit location and gain access to network
  - Visit location and gain access to phone closet
  - Ask for information over phone



# Local / Onsite attacks

- Media / News Agency
  - Everyone wants their 15 seconds of fame
  - Gain trust
  - Bring “photographer”
  - Keep busy while “Photographer” wanders



# Physical Layout

- The layout of a facility can make a major difference.
  - Blind corners
  - Wall files
  - Easy access printers
  - Public restrooms near open cubicles
  - Insecure server rooms
  - Easy access conference rooms
  - Unattended areas with easy access

# Did you shred?



# Prevention

- Simple solutions
  - Be Alert
  - Make sure all employees know policy
  - Ask for Picture ID
  - Be a shadow
  - Don't let a group separate
  - Make it clear they are being watched
  - Never trust software
  - Cross reference everything
  - Strong policy enforcement
  - Shred Shred Shred

# Useful Links

- [www.tracesecurity.com](http://www.tracesecurity.com) (TraceSecurity Inc)
  - Products include Trace Audit, Trace Regulation Compliance, PatchPortal and Trace Policy Manager
  
- [www.sans.org](http://www.sans.org) (SANS)
  - Organization dedicated to the advancement of security
  
- [www.itdefensemag.com](http://www.itdefensemag.com) (IT Defense Magazine)
  - Monthly Magazine focused solely on network security. Be sure to check out the column “Cyber Sideline”.

# TraceSecurity Inc.

**Comprehensive Security Assessments**

**Penetration Testing**

**Comprehensive Regulation Compliance Review**

**Online Banking Application Testing**

**Remote and Onsite Social Engineering**

**Policy Development and Review**

**Unlimited On Demand Internal / External Scanning**

**Numerous Training Courses available (On site and remote)**

**Anti Phishing, Man in the Middle and Pharming solution**

**Multi Factor Authentication Solution**