Global Knowledge®

Securing the Weakest Link

Instructor

Jay Ferron

CEHI, CISM, CISSP, CWSP, MCITP, MCT, MVP, NSA-IAM …

jayson.ferron@globalknowledge.com

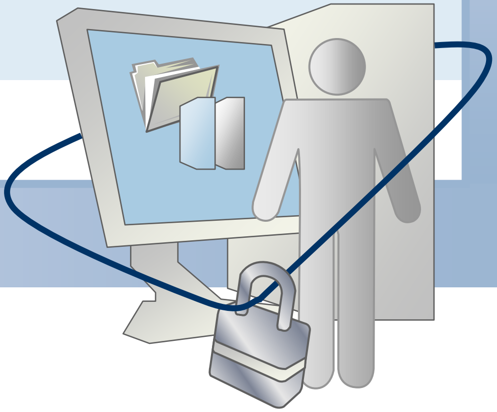
Section Objectives

After completing this section, you will be able to:

- Discuss the issue of social media in security
- Describe and show examples of phishing
- Show methods of discovering and processing online attacks

Security Importance

- To protect your finances
- To protect your data
- To protect your country
- To protect your job
- To protect your way of life
- To protect your life



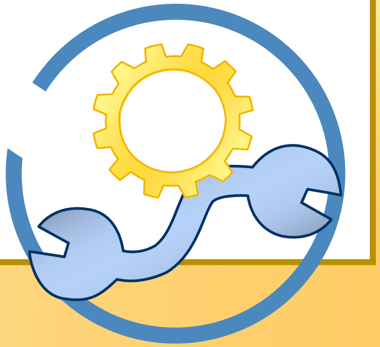
Human Influence in Security

“People are the underlying cause of the need for security.”

Donn Parker, *Fighting Computer Crime*

Social Engineering

- Dumpster diving and shoulder surfing
  - Organizational charts, passwords, access codes, and log files
- Use of tools
  - Google, Bing, Yahoo!, etc.
  - www.learnwebskills.com/company
  - www.whitepages.com
  - Hoover’s, Inc.
  - EDGAR Online, Inc.



Demo

Discussion

How [illegible] one.
[illegible] often?
([illegible] -up)?

Types

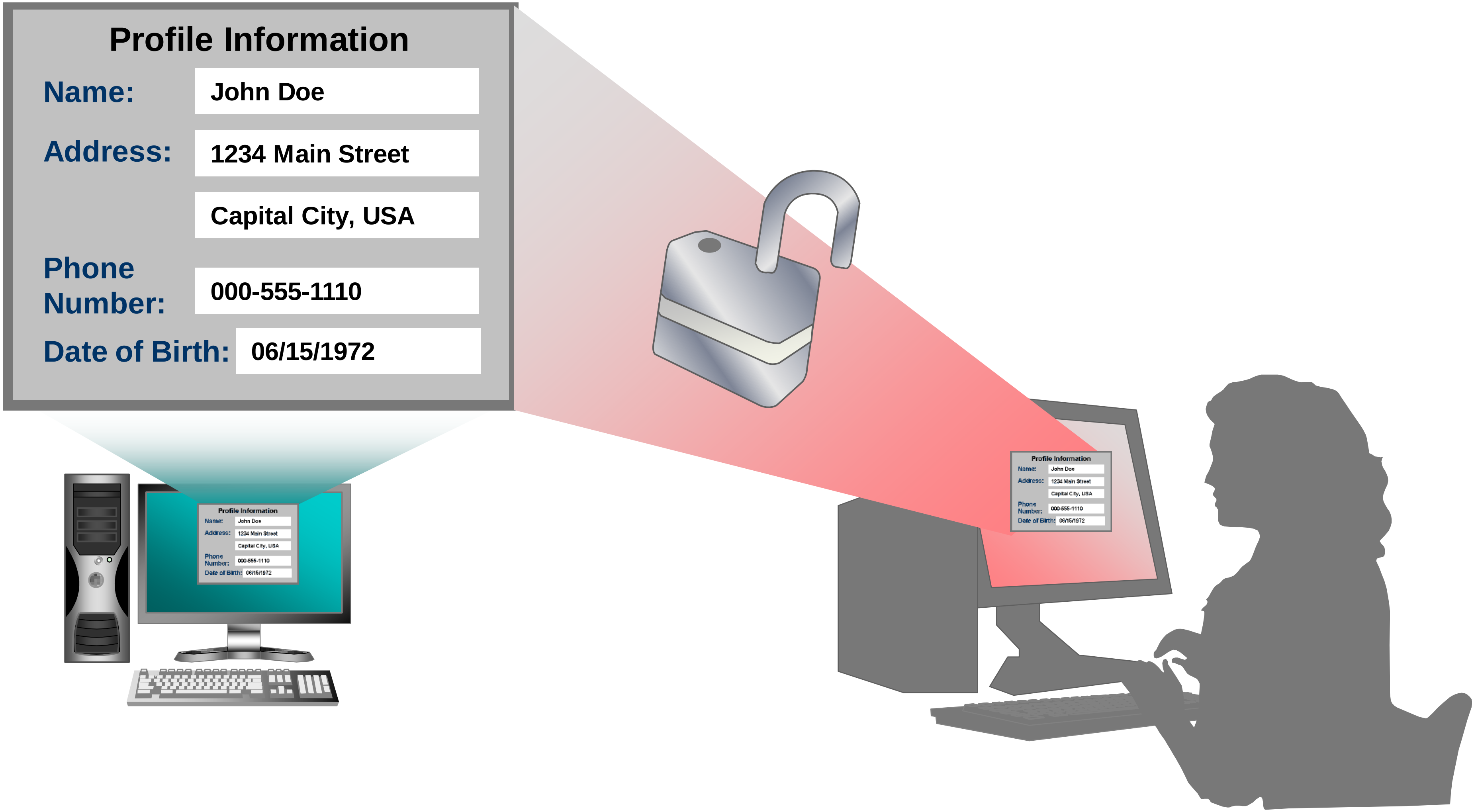
- Social networking sites
  - Facebook
  - Twitter
- Blogging sites
  - Xanga
  - LiveJournal

- Video sharing
  - YouTube
- Bookmarking sites
  - Digg
- Photo sharing
  - Flickr

Demonstration

Social Networking: Help Desk

Vulnerabilities

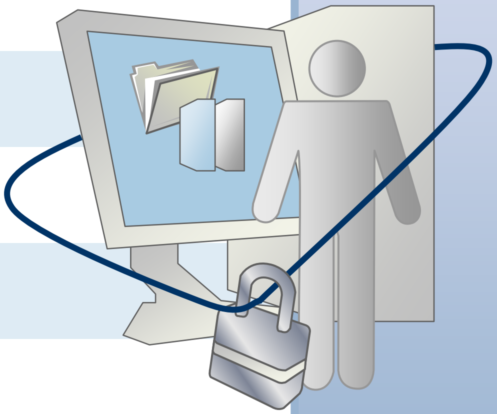


Profile Information

Name:	John Doe
Address:	1234 Main Street Capital City, USA
Phone Number:	000-555-1110
Date of Birth:	06/15/1972

Items At Stake

- Social security number
- Mother’s maiden name
- Birth date
- Billing addresses
- E-mail addresses
- Account numbers
- Password
- System information
- Company or government data
- Who, what, and where you work

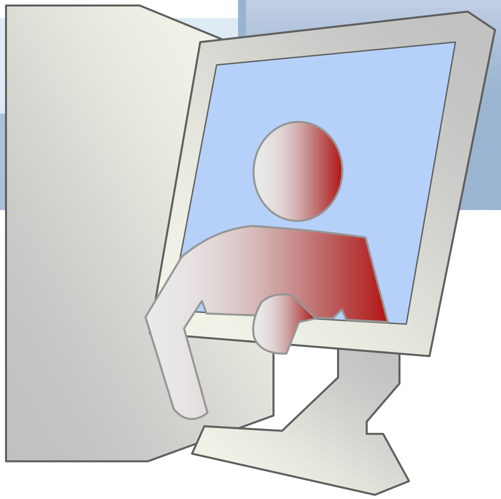


Now that I have your ID

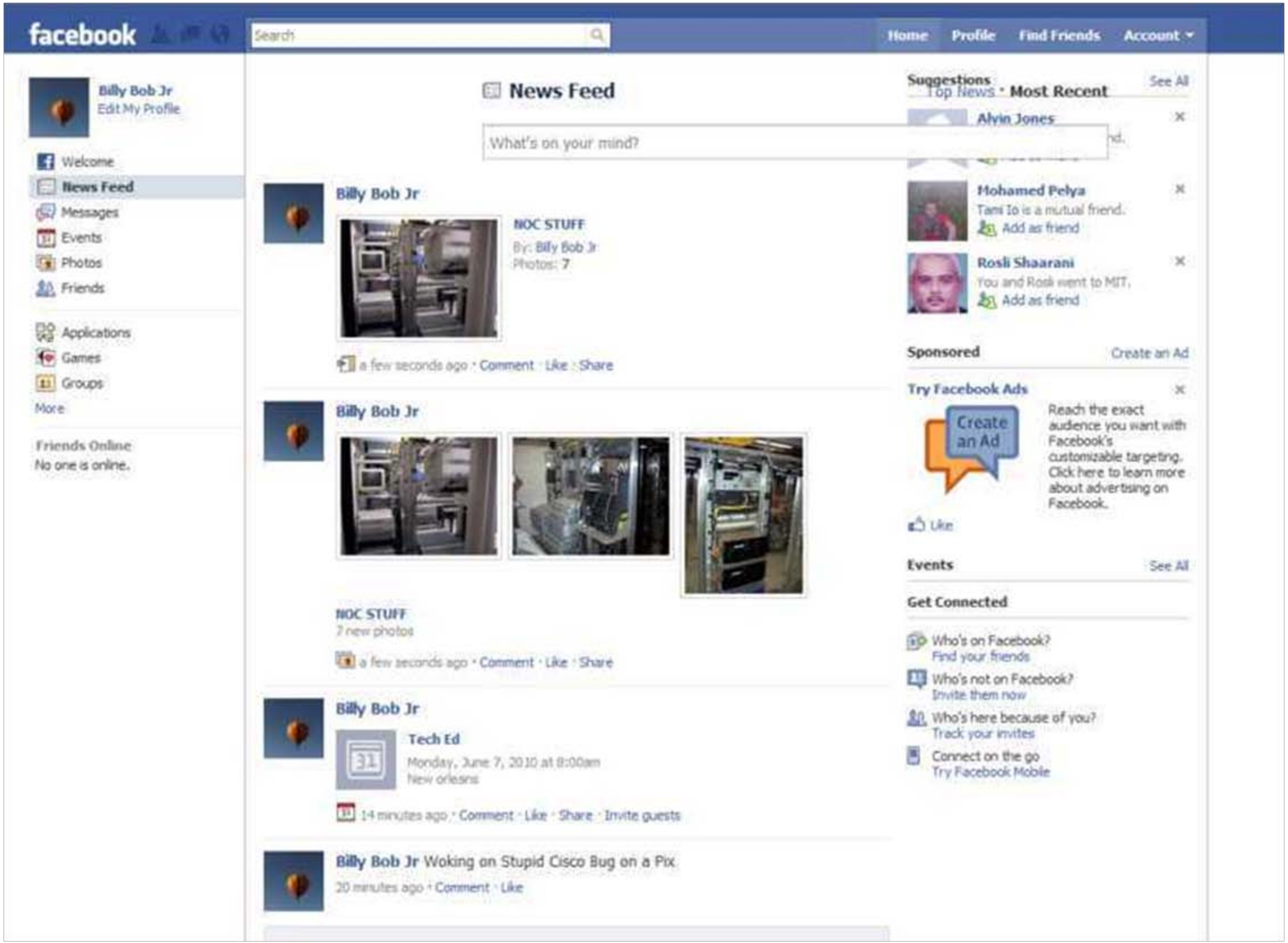
- Let Search about you
- Let create a New you

Attacker Mentality

- They look for holes
- They think creatively
- They think outside of the box



Billy Bob, Jr.



Billy Bob Jr
Edit My Profile

Friends Online
No one is online.

News Feed

Top News · Most Recent

What's on your mind?

Billy Bob Jr
NOC STUFF
By: Billy Bob Jr
Photos: 7
a few seconds ago · Comment · Like · Share

Billy Bob Jr
NOC STUFF
7 new photos
a few seconds ago · Comment · Like · Share

Billy Bob Jr
Tech Ed
Monday, June 7, 2010 at 8:00am
New orleans
14 minutes ago · Comment · Like · Share · Invite guests

Billy Bob Jr Woking on Stupid Cisco Bug on a Pix
20 minutes ago · Comment · Like

Suggestions See All

Alvin Jones
...nd.

Mohamed Pelya
Tami Io is a mutual friend.
Add as friend

Rosli Shaarani
You and Rosli went to MIT.
Add as friend

Sponsored Create an Ad

Try Facebook Ads
Create an Ad
Reach the exact audience you want with Facebook's customizable targeting. Click here to learn more about advertising on Facebook.
Like

Events See All

Get Connected

Who's on Facebook?
Find your friends

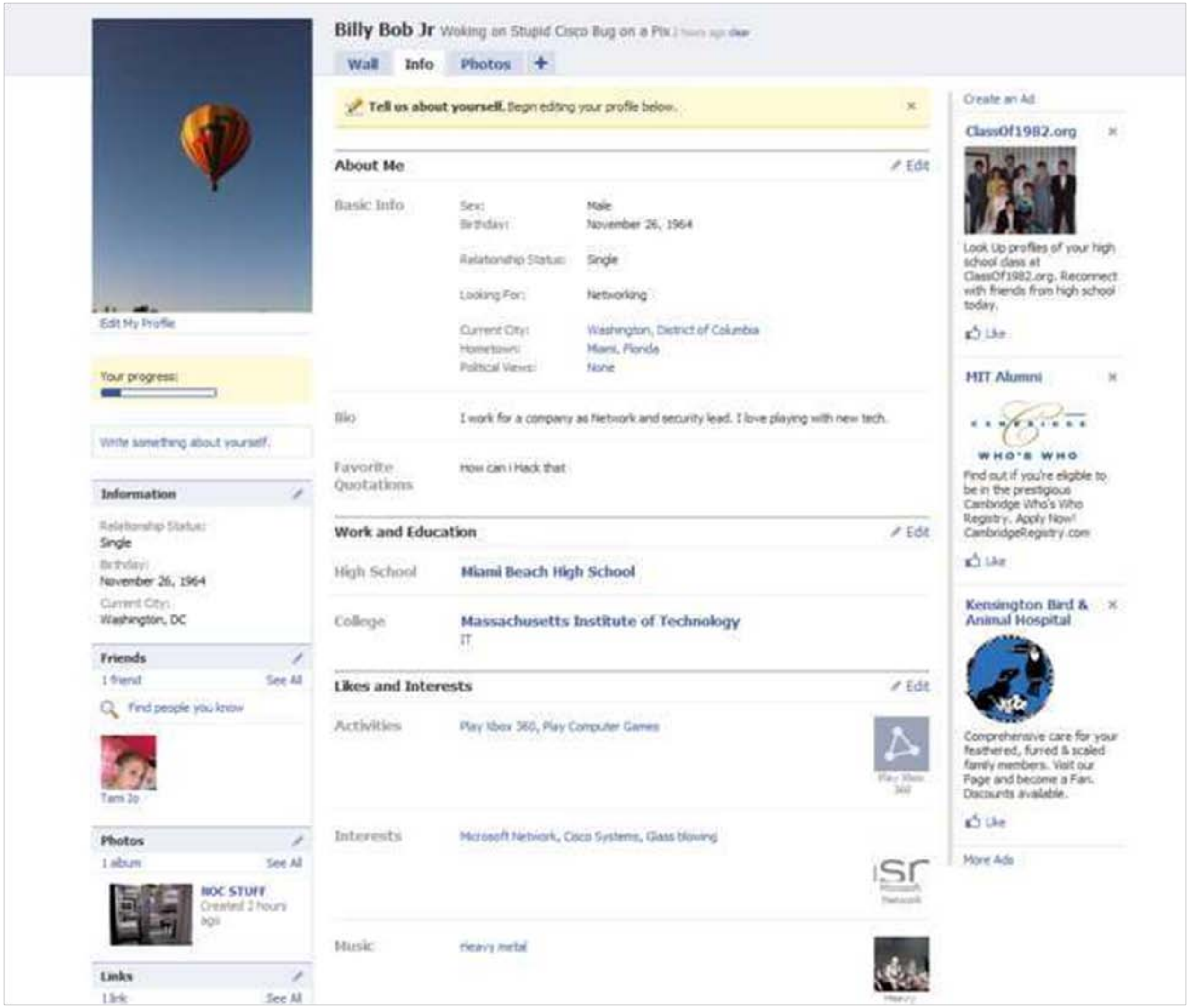
Who's not on Facebook?
Invite them now

Who's here because of you?
Track your invites

Connect on the go
Try Facebook Mobile

Not in Book

Billy Bob, Jr.



Billy Bob Jr Woking on Stupid Cisco Bug on a Pix

Tell us about yourself. Begin editing your profile below.

Edit My Profile

Your progress:

Write something about yourself.

Information

Relationship Status:
Single
Birthday:
November 26, 1964
Current City:
Washington, DC

Friends

1 friend See All

Find people you know

Tami Jo

Photos

1 album See All

NOC STUFF
Created 2 hours ago

Links

1 link See All

About Me Edit

Basic Info

Sex:	Male
Birthday:	November 26, 1964
Relationship Status:	Single
Looking For:	Networking
Current City:	Washington, District of Columbia
Hometown:	Miami, Florida
Political Views:	None

Bio: I work for a company as Network and security lead. I love playing with new tech.

Favorite Quotations: How can i Hack that

Work and Education Edit

High School: **Miami Beach High School**

College: **Massachusetts Institute of Technology**
IT

Likes and Interests Edit

Activities: Play Xbox 360, Play Computer Games

Interests: Microsoft Network, Cisco Systems, Glass blowing

Music: Heavy metal

Create an Ad

ClassOf1982.org

Look Up profiles of your high school class at ClassOf1982.org. Reconnect with friends from high school today.

Like

MIT Alumni

Find out if you're eligible to be in the prestigious Cambridge Who's Who Registry. Apply Now! CambridgeRegistry.com

Like

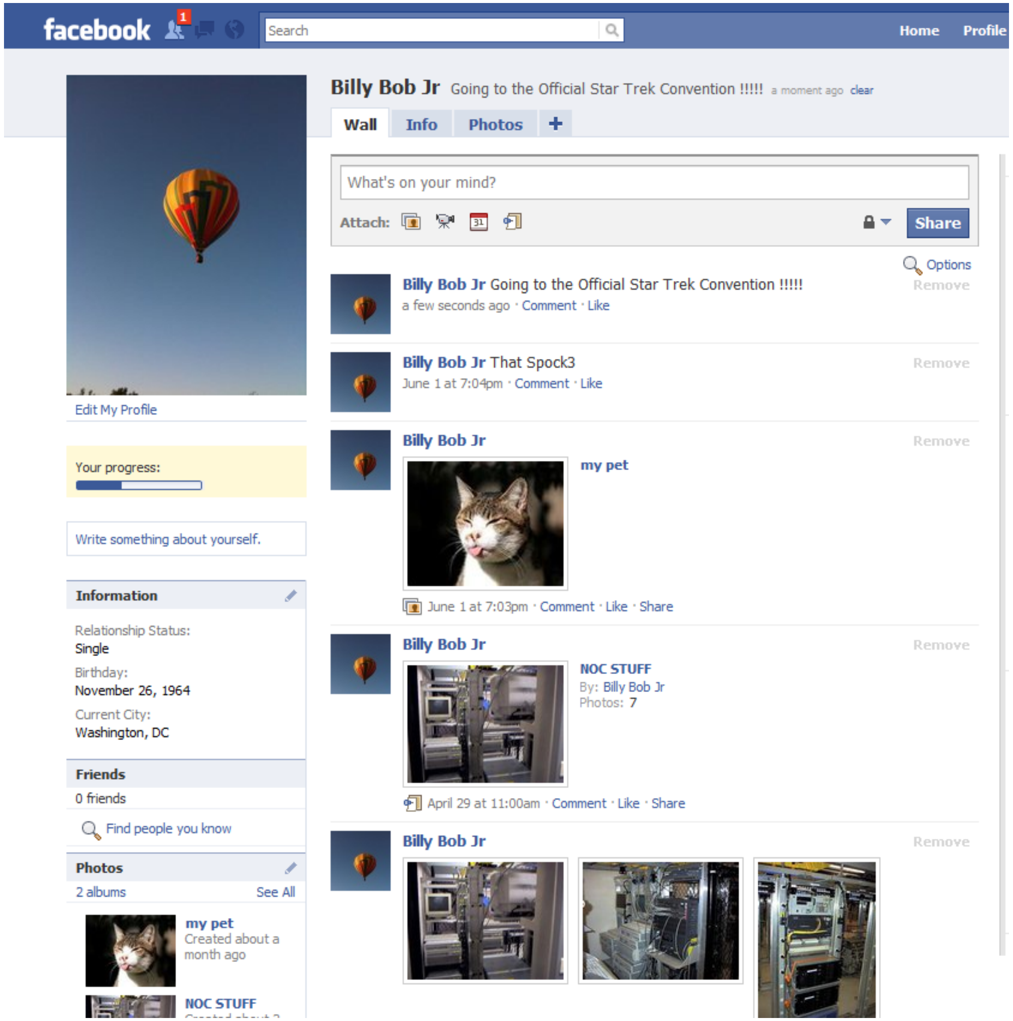
Kensington Bird & Animal Hospital

Comprehensive care for your feathered, furred & scaled family members. Visit our Page and become a Fan. Discounts available.

Like

More Ads

Billy Bob, Jr.



Billy Bob Jr Going to the Official Star Trek Convention !!!!! a moment ago clear

What's on your mind?

Edit My Profile

Your progress:

Write something about yourself.

Information

Relationship Status:
Single

Birthday:
November 26, 1964

Current City:
Washington, DC

Friends

0 friends

Find people you know

Photos

2 albums See All

my pet
Created about a month ago

NOC STUFF

Billy Bob Jr Going to the Official Star Trek Convention !!!!!
a few seconds ago · Comment · Like
Remove

Billy Bob Jr That Spock3
June 1 at 7:04pm · Comment · Like
Remove

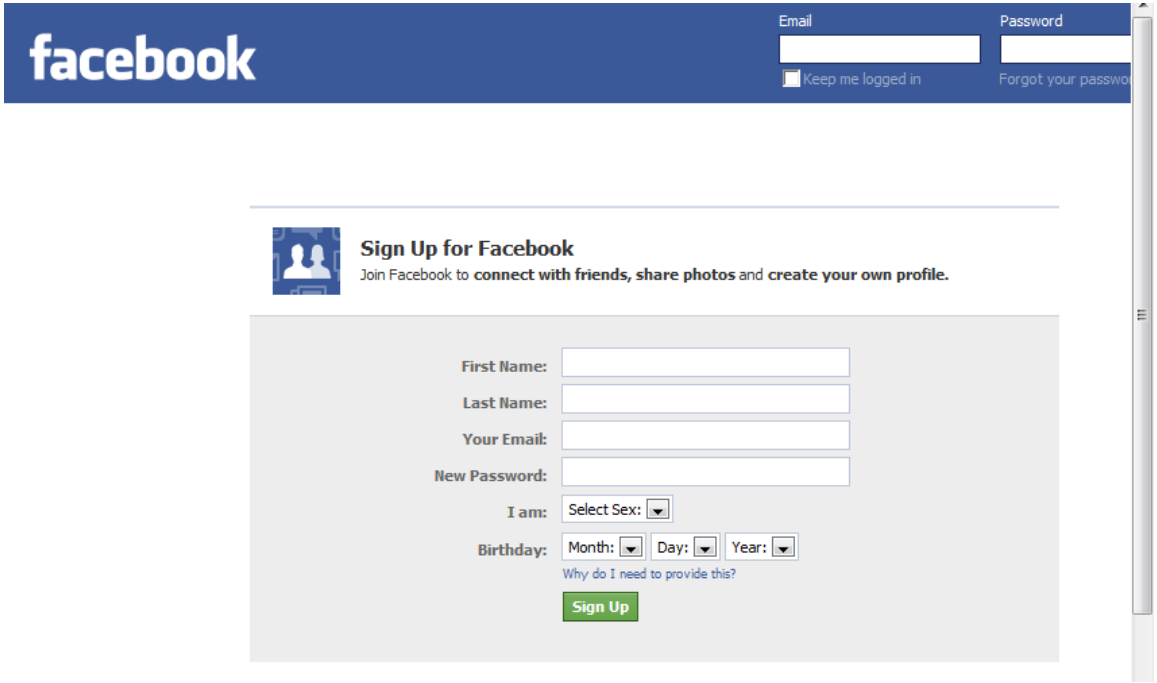
Billy Bob Jr
my pet
June 1 at 7:03pm · Comment · Like · Share
Remove

Billy Bob Jr
NOC STUFF
By: Billy Bob Jr
Photos: 7
April 29 at 11:00am · Comment · Like · Share
Remove

Billy Bob Jr
Remove

Profile Management

- Social networking profiles
  - Koobface outbreak
  - Hoax applications
  - Profile information compromised



facebook

Email

Password

☐ Keep me logged in

Forgot your passwo

Sign Up for Facebook

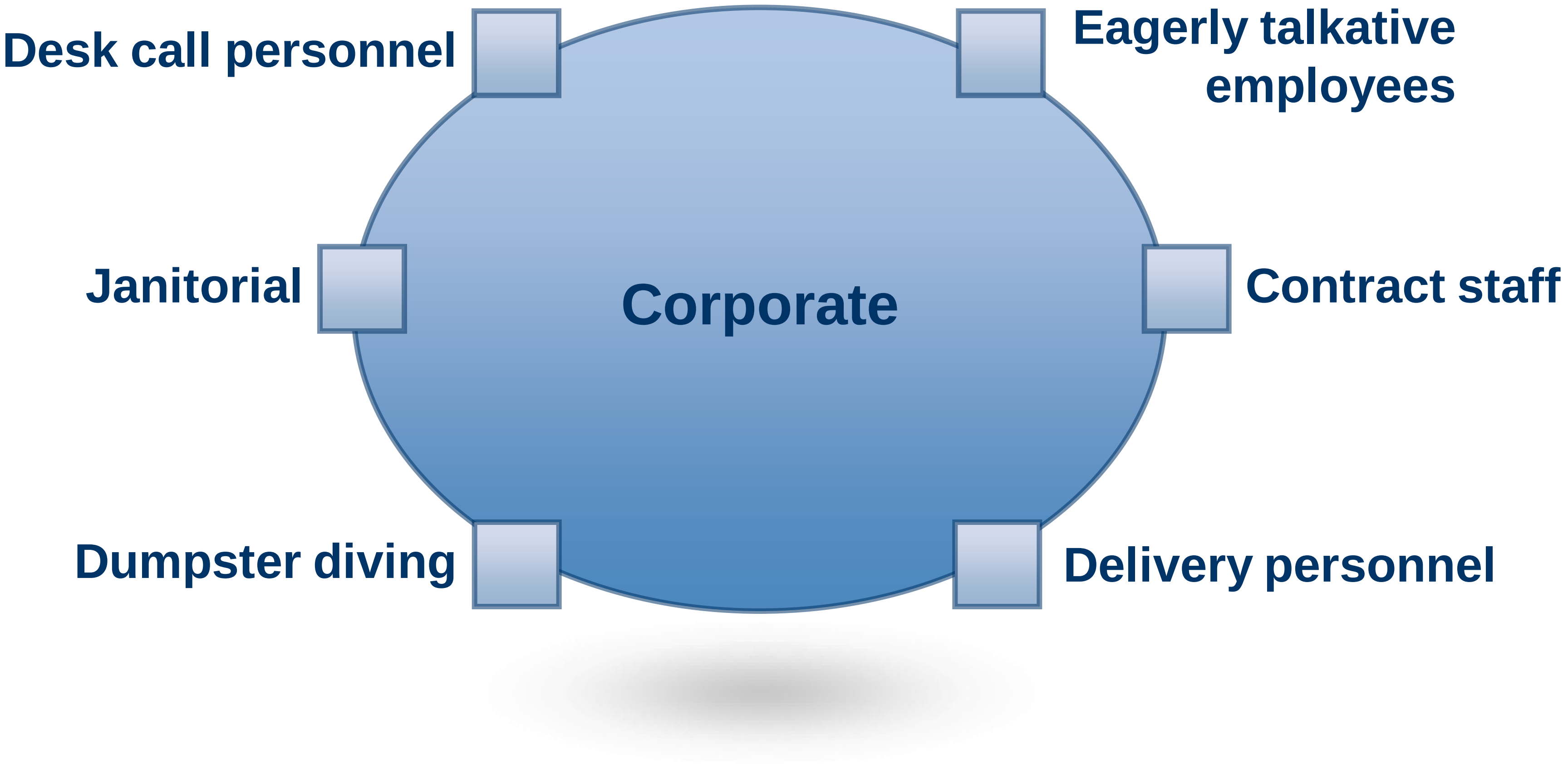
Join Facebook to **connect with friends, share photos** and **create your own profile.**

First Name:	
Last Name:	
Your Email:	
New Password:	
I am:	Select Sex: ▾
Birthday:	Month: ▾ Day: ▾ Year: ▾

Why do I need to provide this?

Sign Up

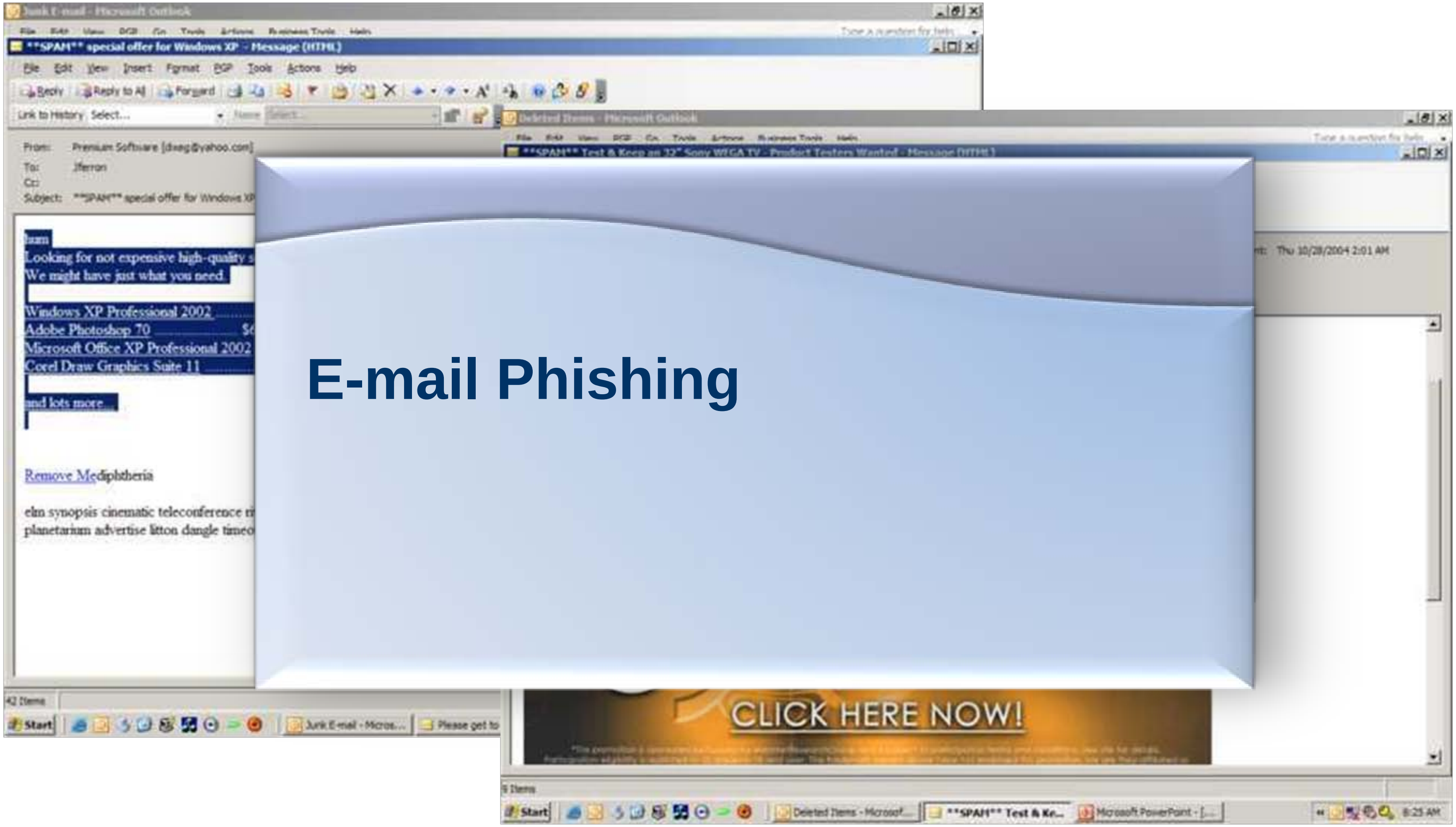
Social Engineering



Demonstration

Dumpster Diving video

Discussion


Junk E-mail - Microsoft Outlook
File Edit View PGP Go Tools Actions Business Tools Help
SPAM special offer for Windows XP - Message (HTML)
File Edit View Insert Format PGP Tools Actions Help
Reply Reply to All Forward
Link to History Select...
Deleted Items - Microsoft Outlook
SPAM Test & Keep an 32" Sony WEGA TV - Product Testers Wanted - Message (HTML)
CLICK HERE NOW!
42 Items
5 Items
Start
Junk E-mail - Micros...
Deleted Items - Microsof...
SPAM Test & Ke...
Microsoft PowerPoint - [...
8:25 AM

From: Premium Software [dxeg@yahoo.com]
To: Jferron
Cc:
Subject: **SPAM** special offer for Windows XP

Sent: Thu 10/28/2004 2:01 AM

Isam
Looking for not expensive high-quality s
We might have just what you need.

Windows XP Professional 2002
Adobe Photoshop 70 $6
Microsoft Office XP Professional 2002
Corel Draw Graphics Suite 11

and lots more...

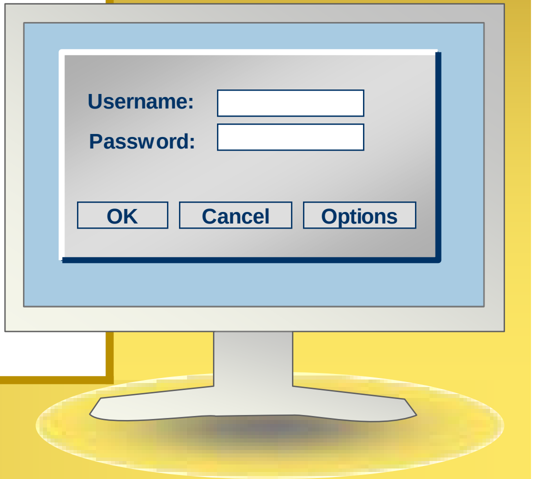
Remove Mediphtheria

eln synopsis cinematic teleconference ri
planetarium advertise litton dangle timeo

E-mail Phishing

Phishing

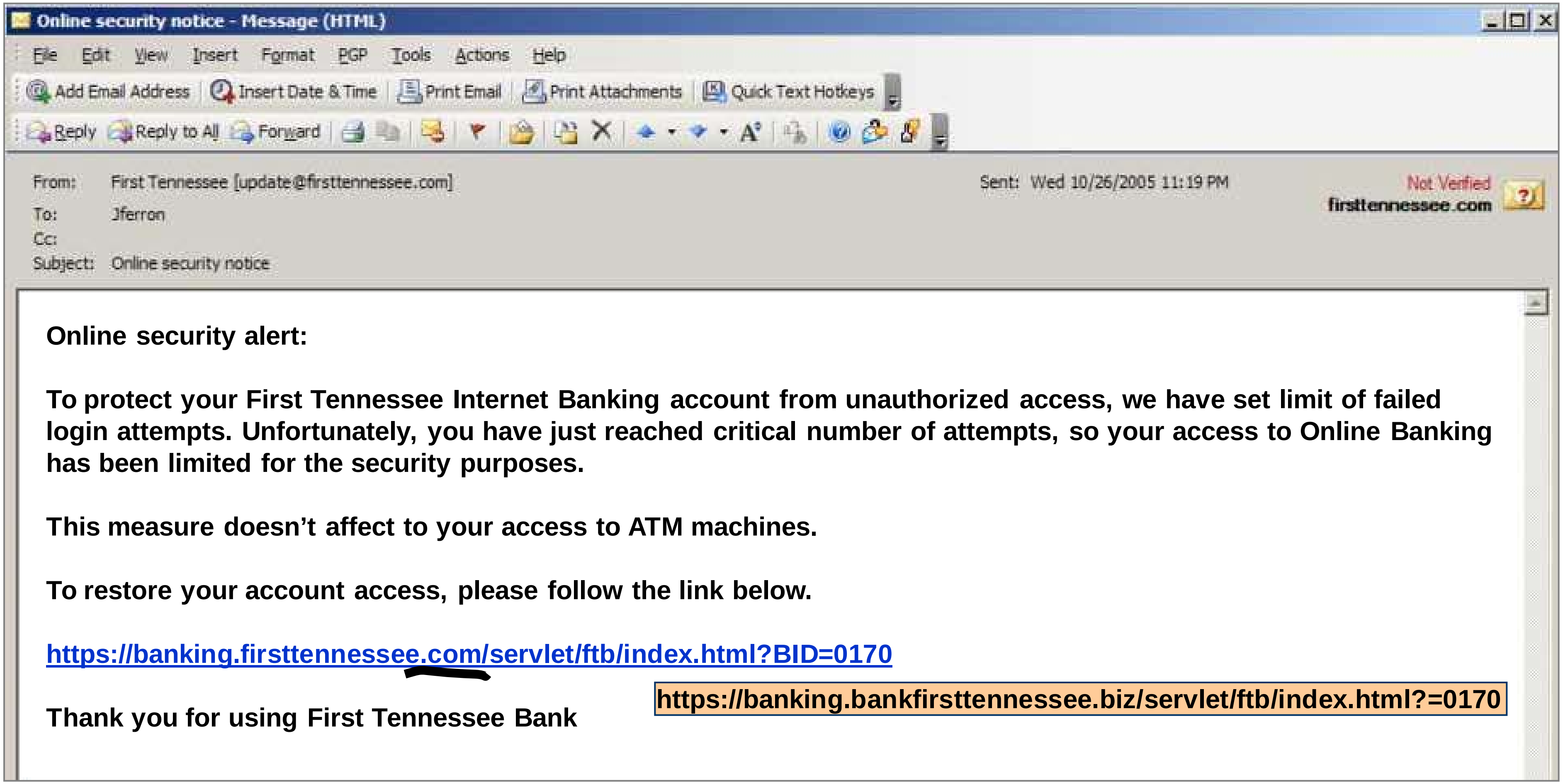
- Fraudulent process to acquire:
  - User names
  - Passwords
  - Credit card details
- Appears to be a trustworthy source
  - Banks
  - Social Web sites
  - Auction sites
  - Online payment processors
  - IT administrators



Demonstration

Internet Phishing

Phishing via E-mail



From: First Tennessee [update@firsttennessee.com]

To: Jferron

Cc:

Subject: Online security notice

Sent: Wed 10/26/2005 11:19 PM

Online security alert:

To protect your First Tennessee Internet Banking account from unauthorized access, we have set limit of failed login attempts. Unfortunately, you have just reached critical number of attempts, so your access to Online Banking has been limited for the security purposes.

This measure doesn't affect to your access to ATM machines.

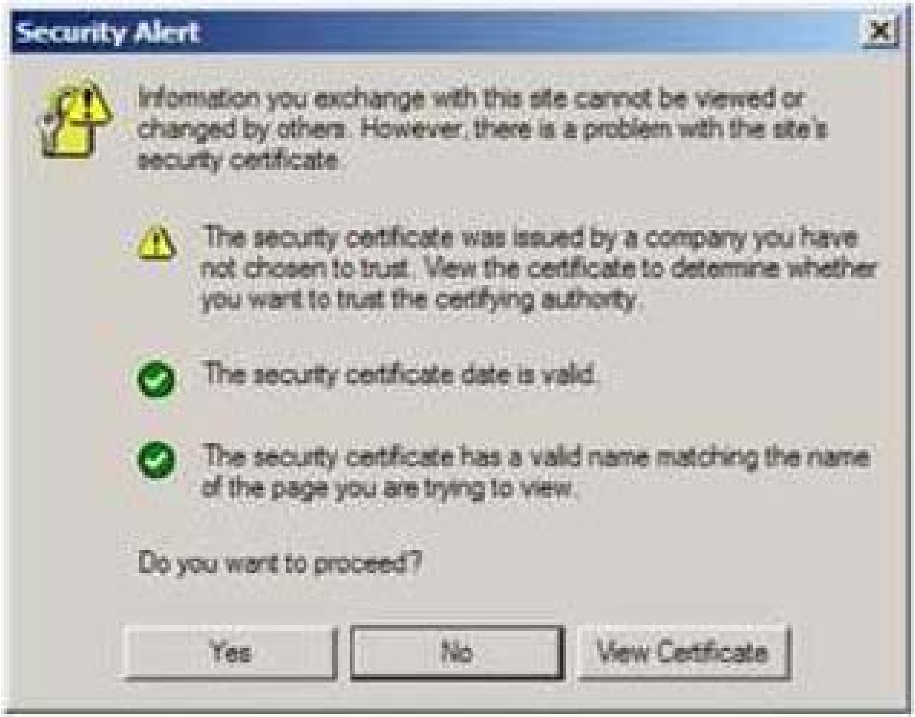
To restore your account access, please follow the link below.

https://banking.firsttennessee.com/servlet/ftb/index.html?BID=0170

https://banking.bankfirsttennessee.biz/servlet/ftb/index.html?=0170

Thank you for using First Tennessee Bank

SSL



Security Alert

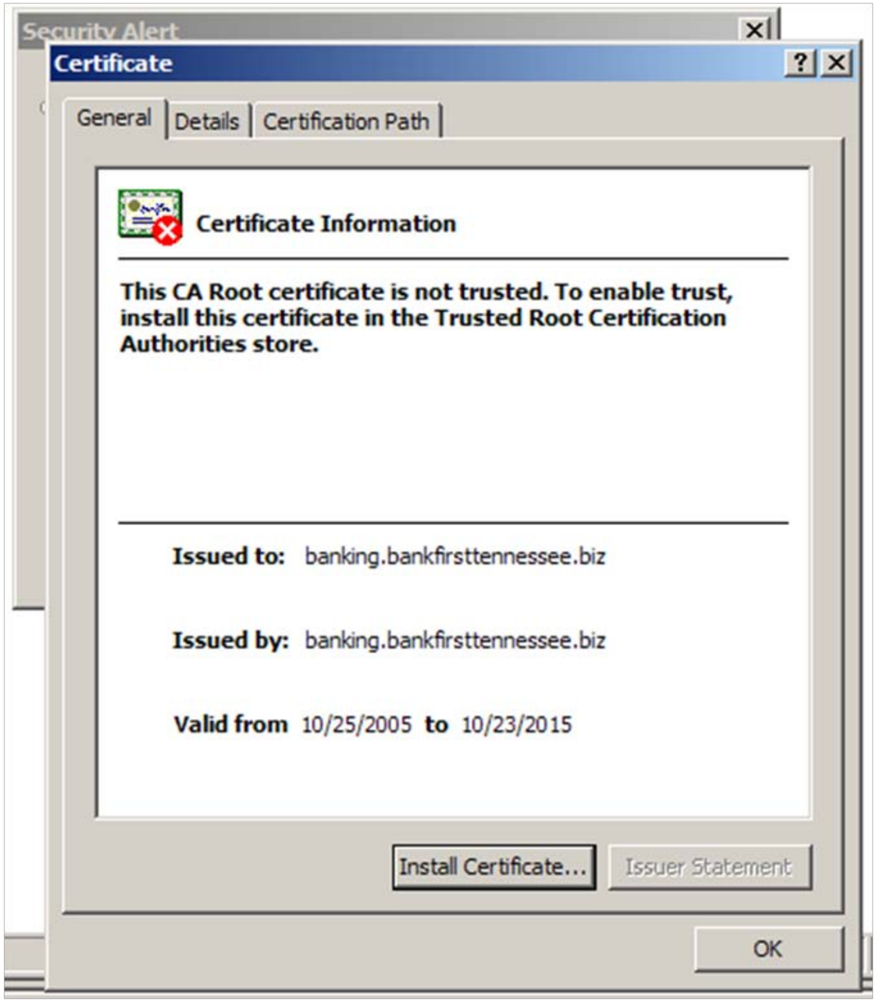
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?



Certificate

Certificate Information

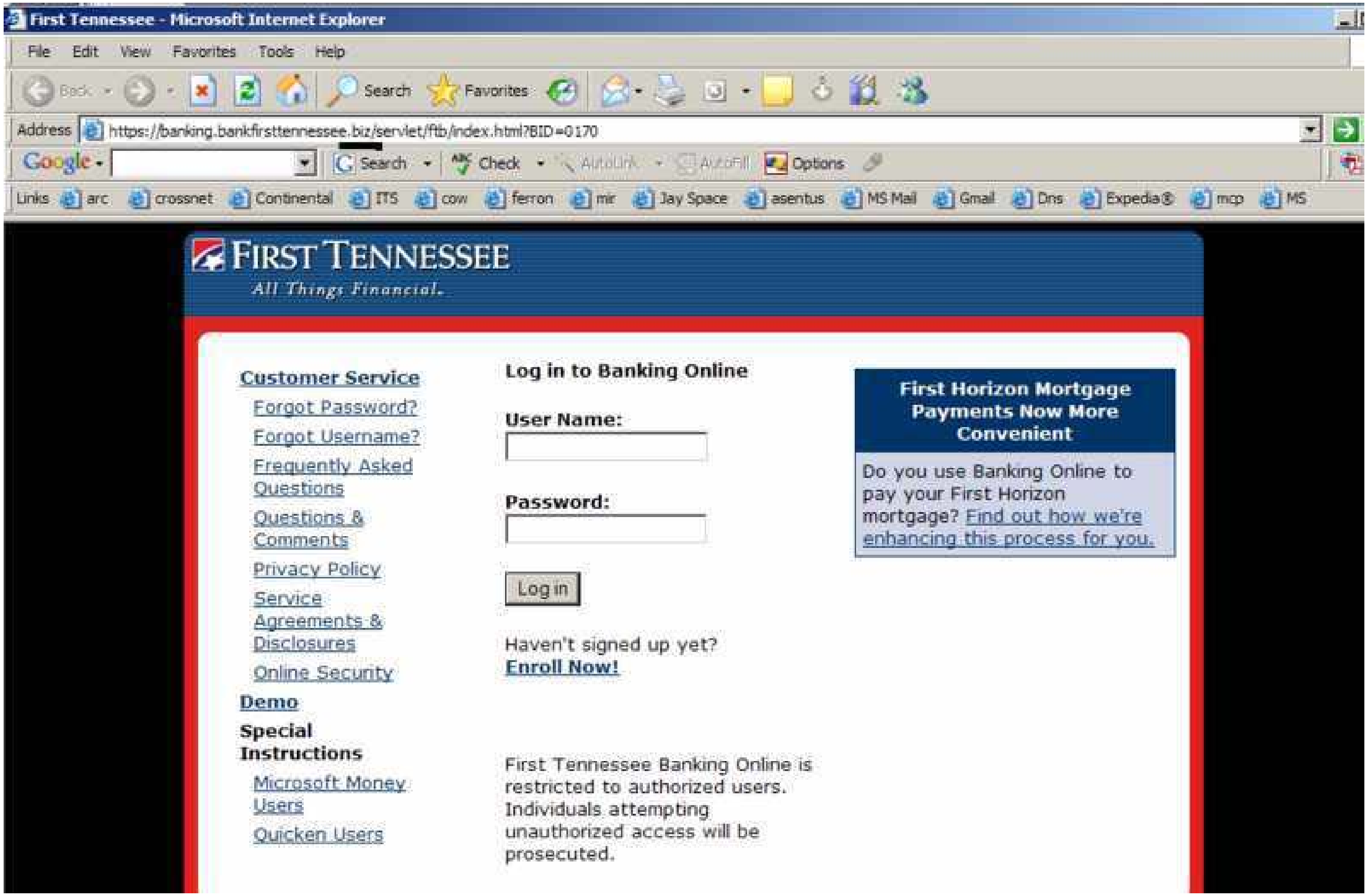
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: banking.bankfirsttennessee.biz

Issued by: banking.bankfirsttennessee.biz

Valid from 10/25/2005 **to** 10/23/2015

Phishing Result


First Tennessee - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Google Search Check AutoLink AutoFill Options
Links arc crossnet Continental ITS cow ferron mir Jay Space asentus MS Mail Gmail Dns Expedia® mcp MS
FIRST TENNESSEE
All Things Financial.
Log in

Address https://banking.bankfirsttennessee.biz/servlet/ftb/index.html?BID=0170

Customer Service
- Forgot Password?
- Forgot Username?
- Frequently Asked Questions
- Questions & Comments
- Privacy Policy
- Service Agreements & Disclosures
- Online Security

Demo

Special Instructions
- Microsoft Money Users
- Quicken Users

Log in to Banking Online

User Name:

Password:

Haven't signed up yet?
Enroll Now!

First Tennessee Banking Online is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted.

First Horizon Mortgage Payments Now More Convenient

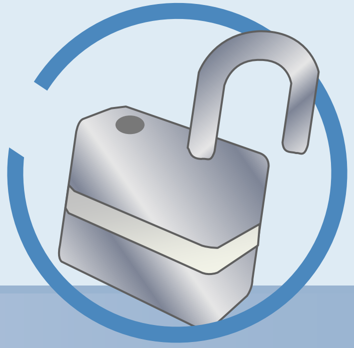
Do you use Banking Online to pay your First Horizon mortgage? Find out how we're enhancing this process for you.

Statistical Data

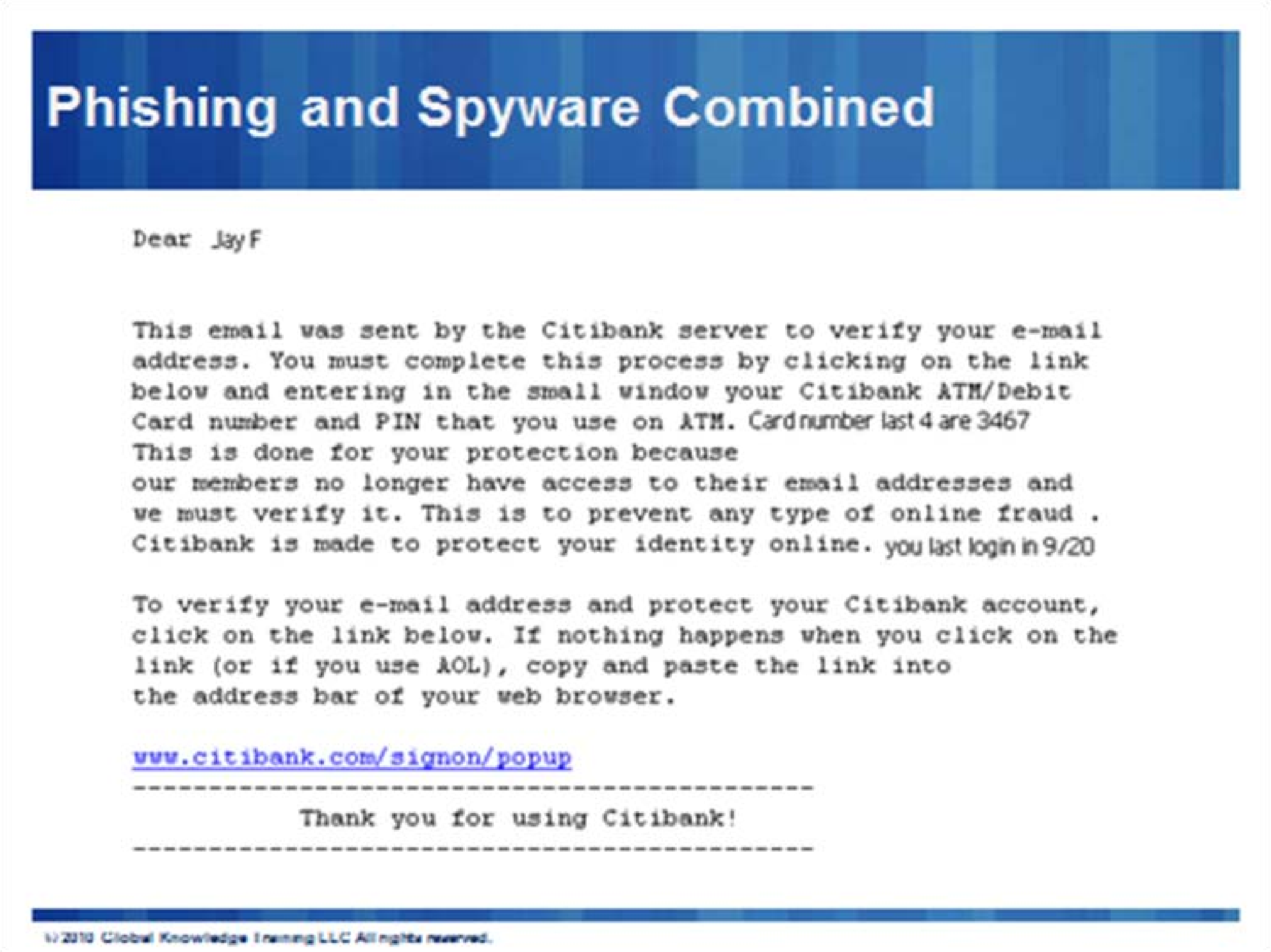
- 491,815,456 records containing personal information compromised since January 2005
- Example: TJ retail stores (TJX)
  - 45,700,000 credit and debit card account numbers compromised
  - TJMaxx
  - Marshalls
  - HomeSense
  - AJWright
  - TKMaxx
  - Winners and HomeGoods stores in Canada
  - 48 million more people affected, according to latest records

Security Breach Sources

- Lack of commitment from management
- No social motivation
- Incorrect assumptions
  - Not part of job description
  - Not part of performance appraisal
  - No economic motivation



Exercise 1



Phishing and Spyware Combined

Dear JayF

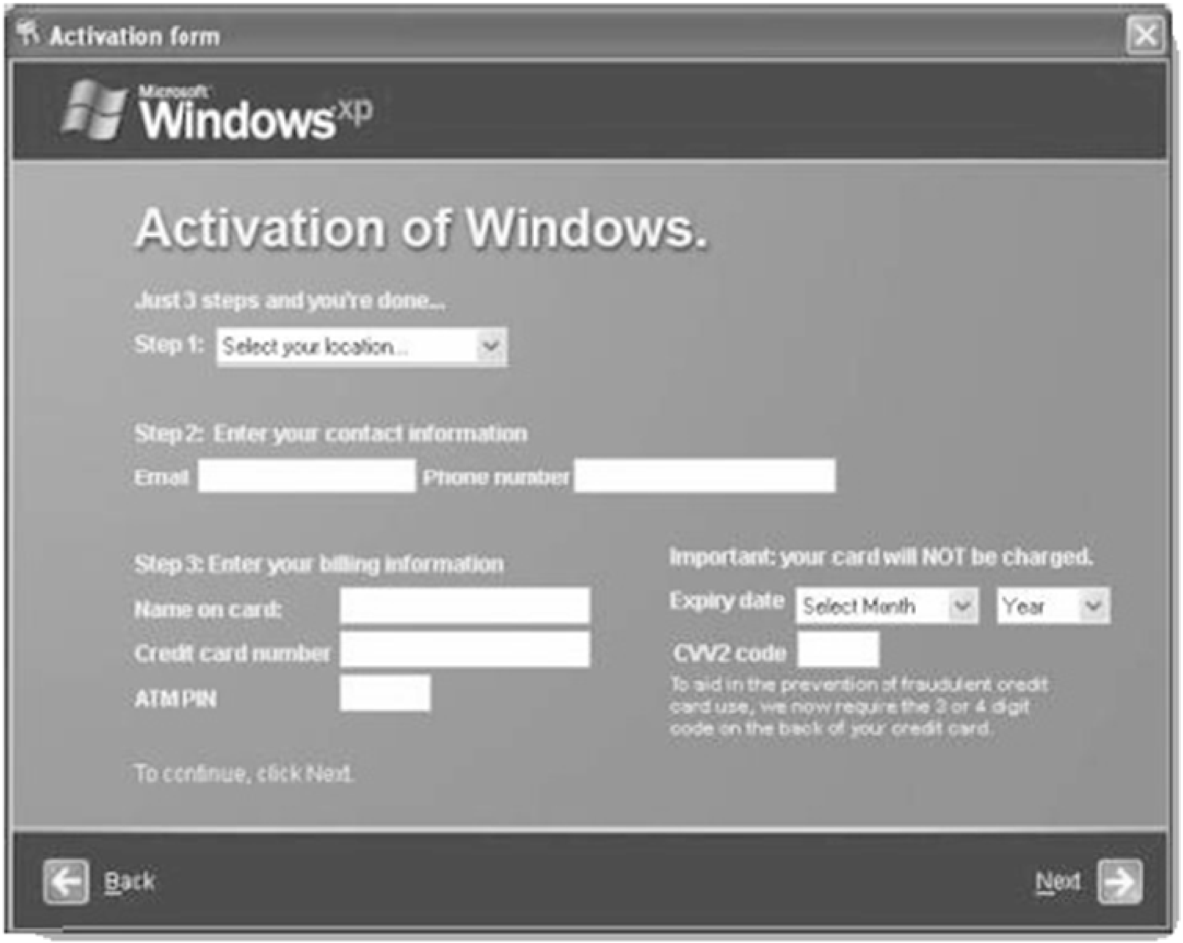
This email was sent by the Citibank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM. Card number last 4 are 3467
This is done for your protection because
our members no longer have access to their email addresses and we must verify it. This is to prevent any type of online fraud . Citibank is made to protect your identity online. you last login in 9/20

To verify your e-mail address and protect your Citibank account, click on the link below. If nothing happens when you click on the link (or if you use AOL), copy and paste the link into the address bar of your web browser.

www.citibank.com/signon/popup

```
---------------------------------------------
           Thank you for using Citibank!
---------------------------------------------
```

Exercise 2



Activation of Windows.

Just 3 steps and you're done...

Step 1: Select your location...

Step 2: Enter your contact information

Email Phone number

Step 3: Enter your billing information

Name on card:

Credit card number

ATM PIN

Important: your card will NOT be charged.

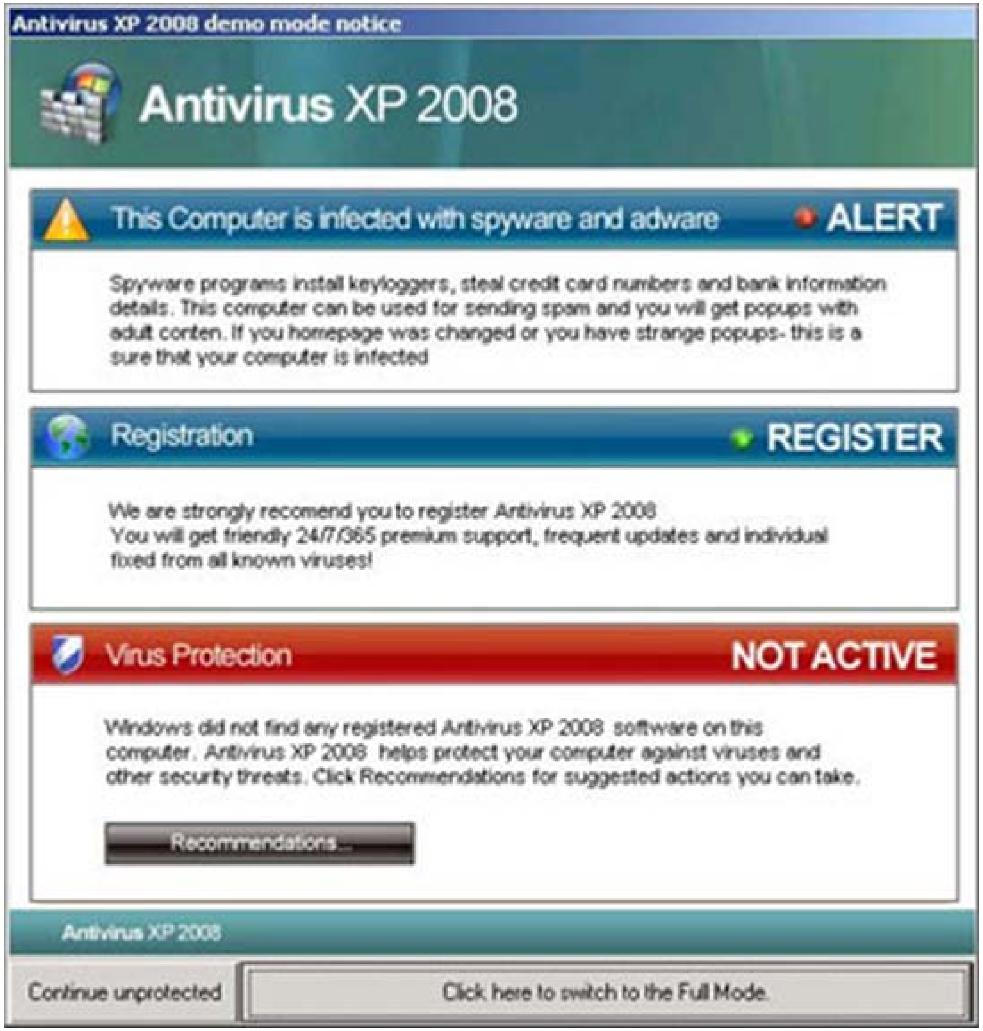
Expiry date Select Month Year

CVV2 code

To aid in the prevention of fraudulent credit card use, we now require the 3 or 4 digit code on the back of your credit card.

To continue, click Next.

Exercise 3



Antivirus XP 2008 demo mode notice

Antivirus XP 2008

This Computer is infected with spyware and adware — ALERT

Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult conten. If you homepage was changed or you have strange popups- this is a sure that your computer is infected

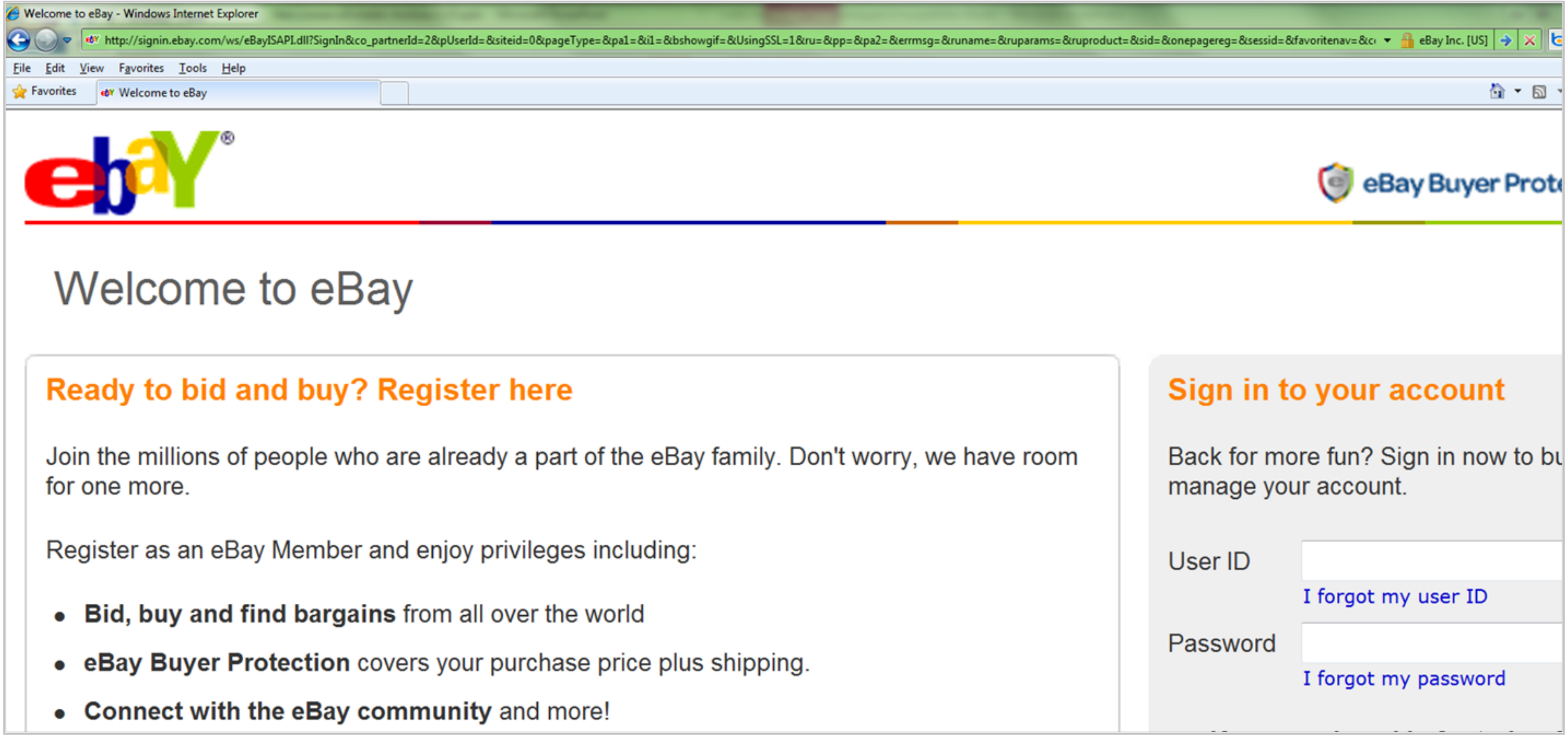
Registration — REGISTER

We are strongly recomend you to register Antivirus XP 2008
You will get friendly 24/7/365 premium support, frequent updates and individual fixed from all known viruses!

Virus Protection — NOT ACTIVE

Windows did not find any registered Antivirus XP 2008 software on this computer. Antivirus XP 2008 helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.

Exercise 4



Welcome to eBay - Windows Internet Explorer
http://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=1&ru=&pp=&pa2=&errmsg=&runame=&ruparams=&ruproduct=&sid=&onepagereg=&sessid=&favoritenav=&c
eBay Inc. [US]
File
Edit
View
Favorites
Tools
Help
Favorites
Welcome to eBay
eBay Buyer Prot

Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- **Bid, buy and find bargains** from all over the world
- **eBay Buyer Protection** covers your purchase price plus shipping.
- **Connect with the eBay community** and more!

Sign in to your account

Back for more fun? Sign in now to bu manage your account.

User ID

I forgot my user ID

Password

I forgot my password

Questions

Thank you for attending if you have questions

Jayson.ferron@globalknowledge.com