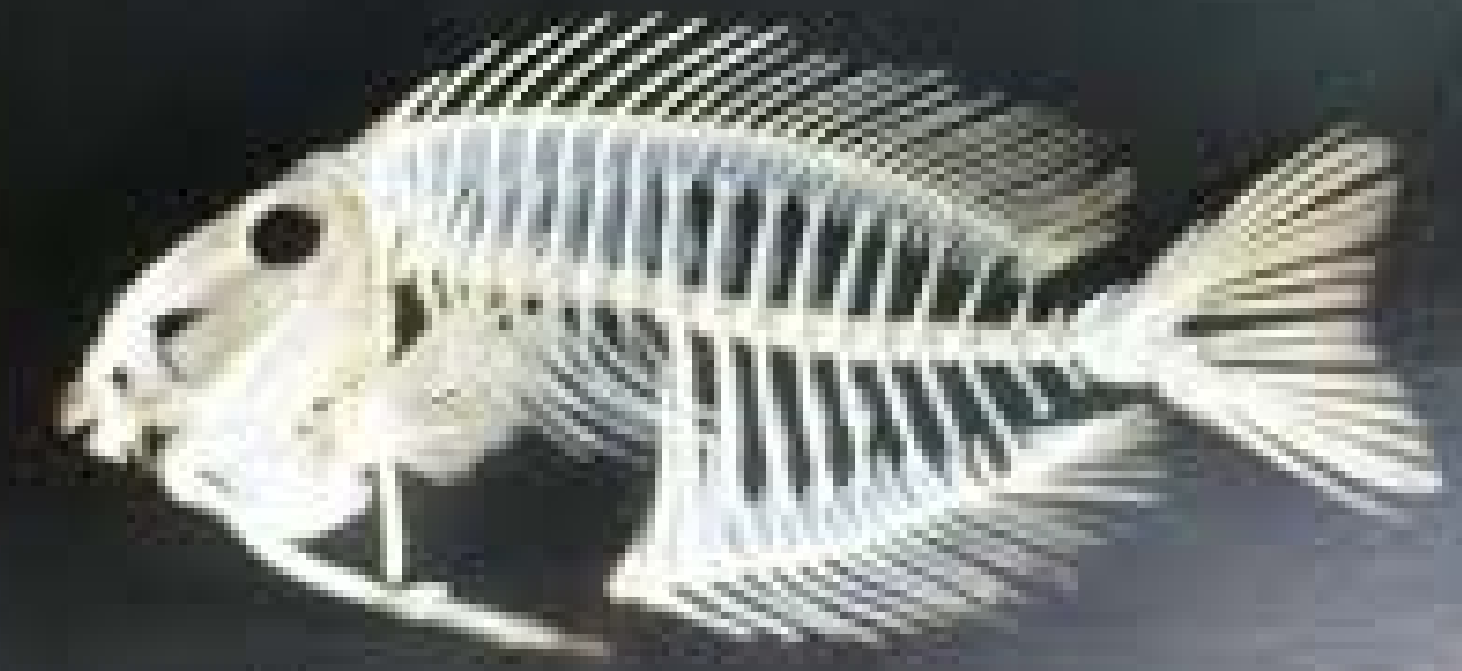
Phish Anatomy



Welcome.

- Pamela King
- Professor, Digital Forensics
- Chestnut Hill College, Philadelphia, PA
- 17 years law enforcement digital forensics
- 10 years private industry digital forensics and e-discovery.
- Academics since 2006 (part time) and full-time for the last 3 years at Chestnut Hill College where we have a B.S. Degree in Digital Forensics.

Today's Presentation…

- Define phishing
- Explain phishing techniques
- Examples of phishing
- Statistics about phishing
- Defense against Dark Arts
- Resources

Define Phishing

What is phishing?

- By deception, convince a person to provide you with personal information by emulating a legitimate site.
  - Credentials
  - Personally Identifiable Information
  - Banking & Finance Information

Crimes involving Phishing

- Phishing is a method commit crimes such as
  - Theft
  - Fraud
  - Identity Theft
  - Trafficking in Identity Information

Types of Phishing

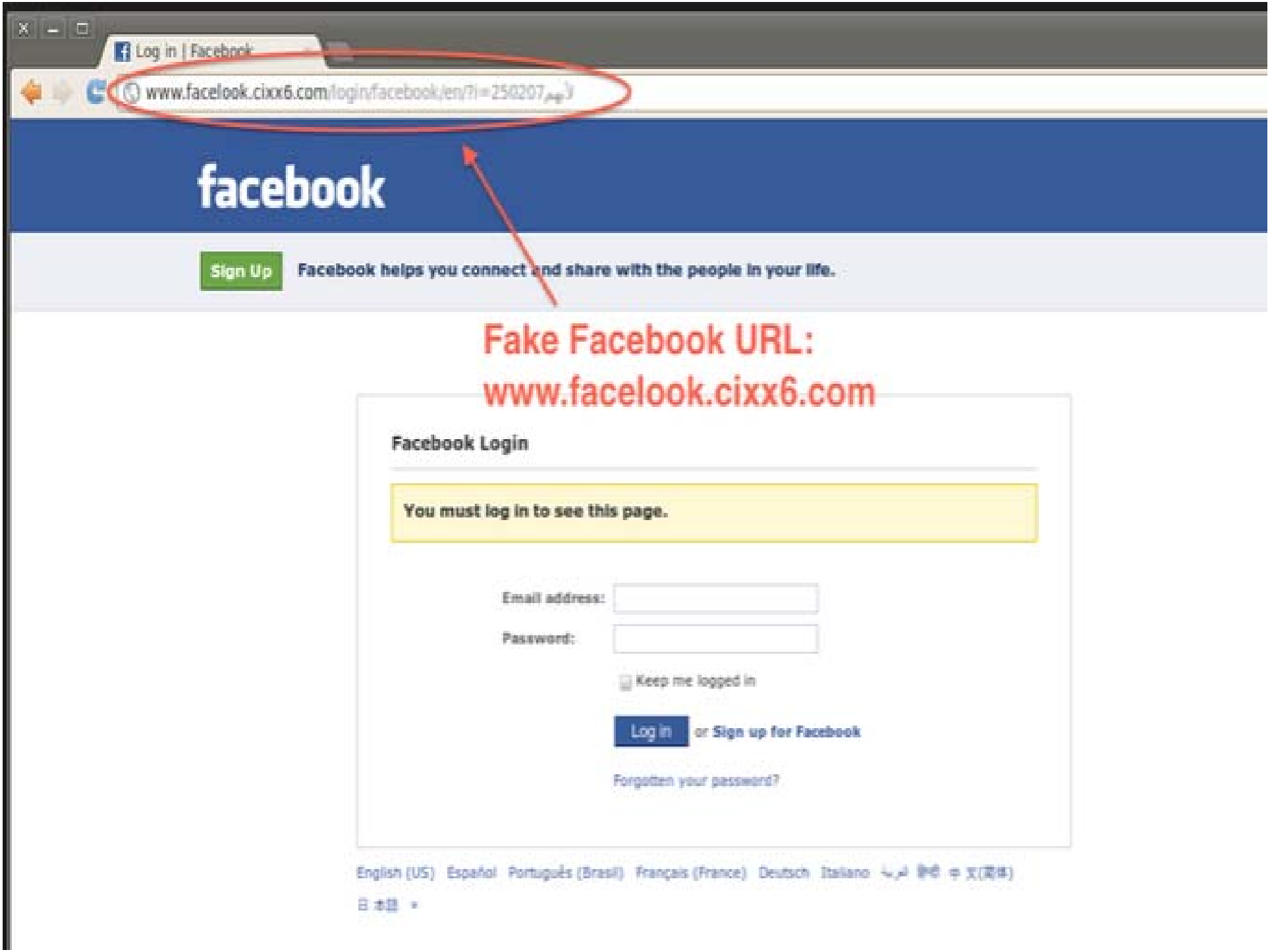
- Phishing
  - Generic term
- Spear Phishing
  - Targeted approach based on reconnaissance
- Vishing
  - Phishing using voice mail
- Whaling
  - Phishing targeting CEO and other Executives

Phishing Techniques

Typical Attack Process

- Email
  - Needs a list of potential victim email addresses.
  - Email requests information and provides a link to a web site.
  - Includes content copied from legitimate sites.
- Web page
  - Remote hosting site
  - Content copied from legitimate site

Examples


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Fake Facebook URL:
www.facelook.cixx6.com
Facebook Login
You must log in to see this page.
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano

Subject: Account Update ALERT!!!!!!!!!!!!!!

WACHOVIA

WACHOVIA SPECIAL ACCOUNT UPGRADE

Dear Customer,

Due to concerns for safety, Your account has been randomly flagged in our system as a part of our latest security measures against Fraud and ID Theft. This happens to ensure that only you have access to your Wachovia account and to ensure a safe Banking experience against online fraud. We require all flagged accounts as yours, to verify their information on file with us. To Speed up the Verification Process, We urge you verify your account now to avoid your online access disabled.

To Begin the verification process of your Wachovia records, Please click on the reference link below:

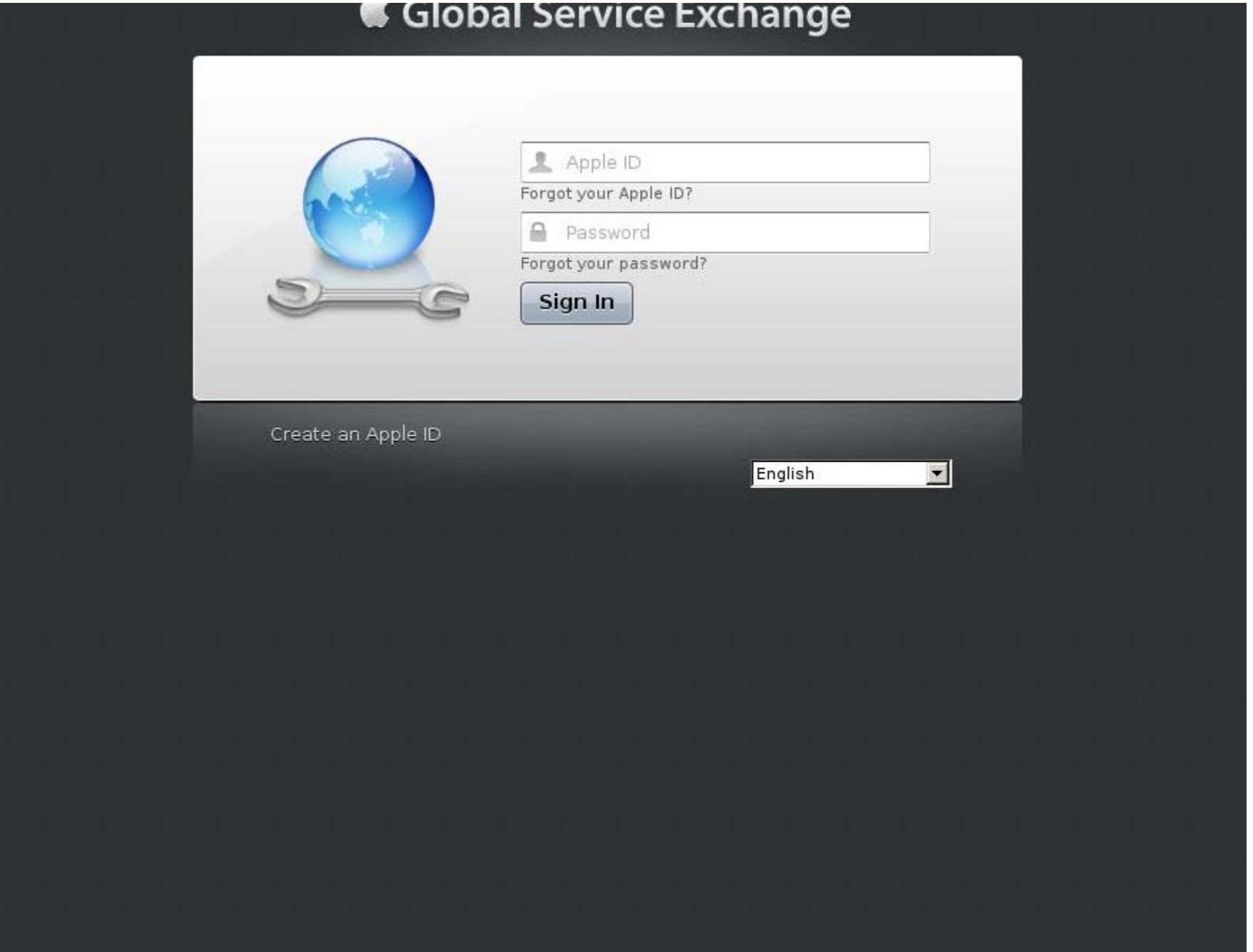
Reference*

http://www.wachovia.com/secureUpdate/ssl.cfm

If you have any questions, please call us at (800) 950-2296 or email online1.services@wachovia.com. We're available to assist you 24 hours a day, seven days a week.

We hope you enjoy banking online with Wachovia.

Contact Us
Online Services
(800) 950-2296
24 hours a day
seven days a week
online1.services@wachovia.com


Global Service Exchange
Apple ID
Forgot your Apple ID?
Password
Forgot your password?
Sign In
Create an Apple ID
English


Internal Revenue Service IRS.gov

DEPARTMENT OF THE TREASURY

Home | Get Tax Refund on your Visa or MasterCard | Refund Help

Tax Refund Online Form

Get Tax Refund on your VISA or MasterCard Now!

Please enter your Social Security Number and your **DEBIT** card information where refunds will be made.
*See our Privacy Notice regarding our request for your personal information.

Social Security Number
or IRS Individual Taxpayer Identification Number.

Debit Card

Full Name:

Card Number:

Expiration Date: Month Year

CVV Code:

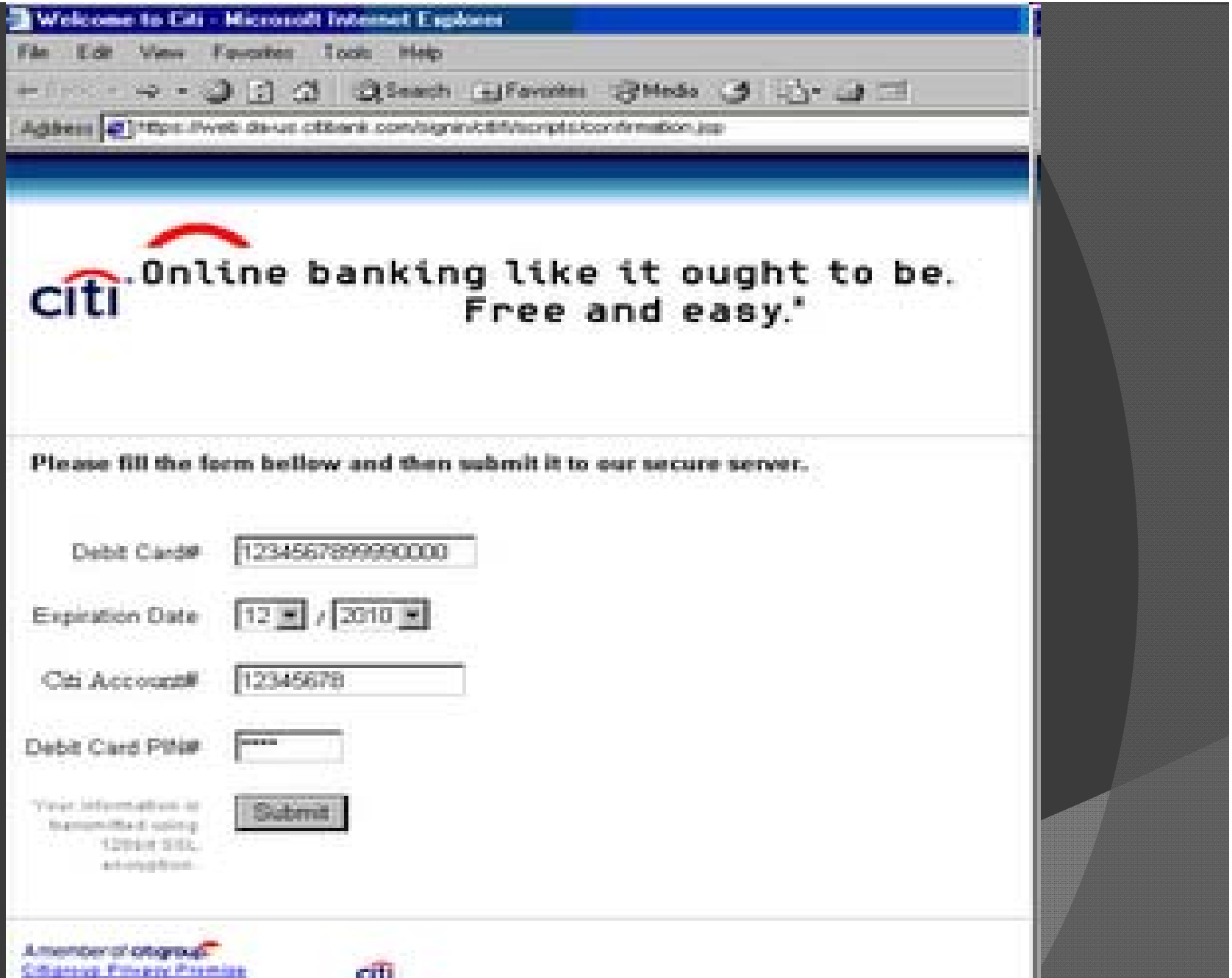
Electronic Signature: (atm pin)

Refund Amount

$ 109.30

Submit

Note: For security reasons, we recommend that you close your browser after you have finished the refund process.


Welcome to Citi - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites Media
Address
citi
Online banking like it ought to be.
Free and easy.*
Please fill the form bellow and then submit it to our secure server.
Debit Card#
1234567899990000
Expiration Date
12
2010
Citi Account#
12345678
Debit Card PIN#
****
Submit

Statistics

rime pays.

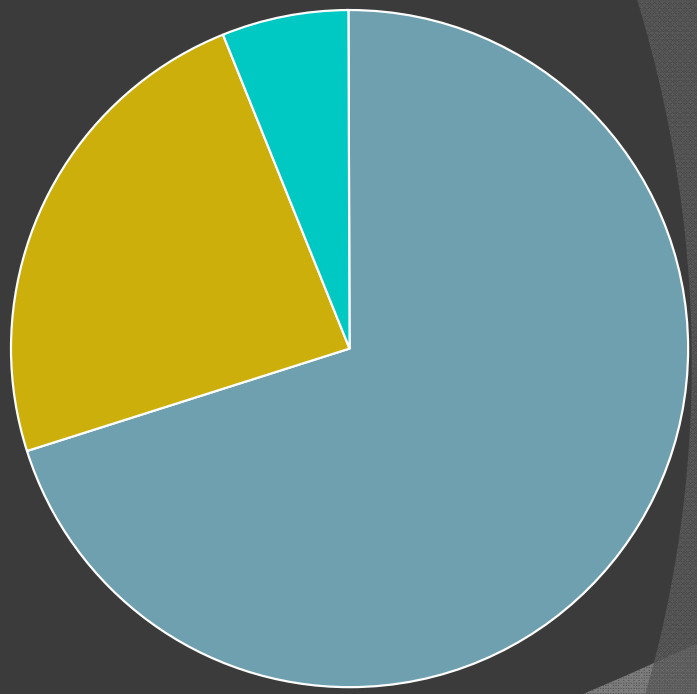
Hypothetical:
100,000 emails sent out.

70% are bad addresses or get filtered by security application.

Of those left, 80% of the people who receive the email are smart enough not to respond.

That is still 6,000 responses!

If the phishers make only $100 per person, that is $600,000!



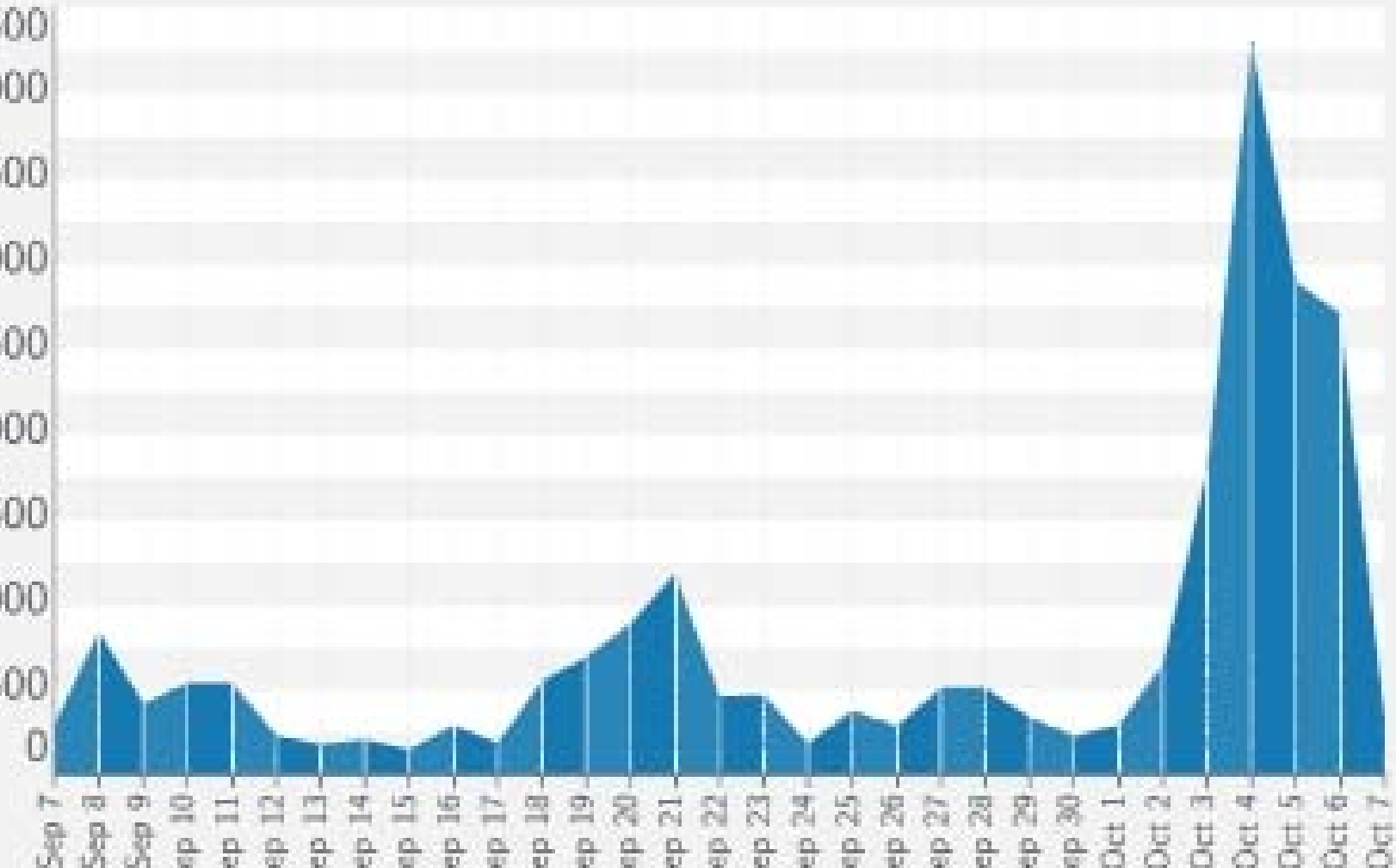
rime pays.

- In the United States during 2008, over 5 million people lost money from phishing scams. (2008)
- The average loss was approximately $351 per person.
- Therefore, in 2008 there was approximately $1.8 billion stolen by phishing.
- One Brazil phisher netted between US$18-37 million before he was caught.
- Eight Japanese phishers netted ¥100 million (US$870,000) before they were caught.

aily Phishes Verified

art created Oct 7 2016 03:40 UTC

PhishTank



uly 2016 – Top Ten Targets

1	PayPal
2	United Services Automobile Association
3	Facebook
4	AOL
5	Yahoo
6	Apple
7	Google
8	Microsoft
9	ABN AMRO Bank
10	Wells Fargo

Defense against Dark Arts

potting the Hook

Verify your account.

Update your financial information.

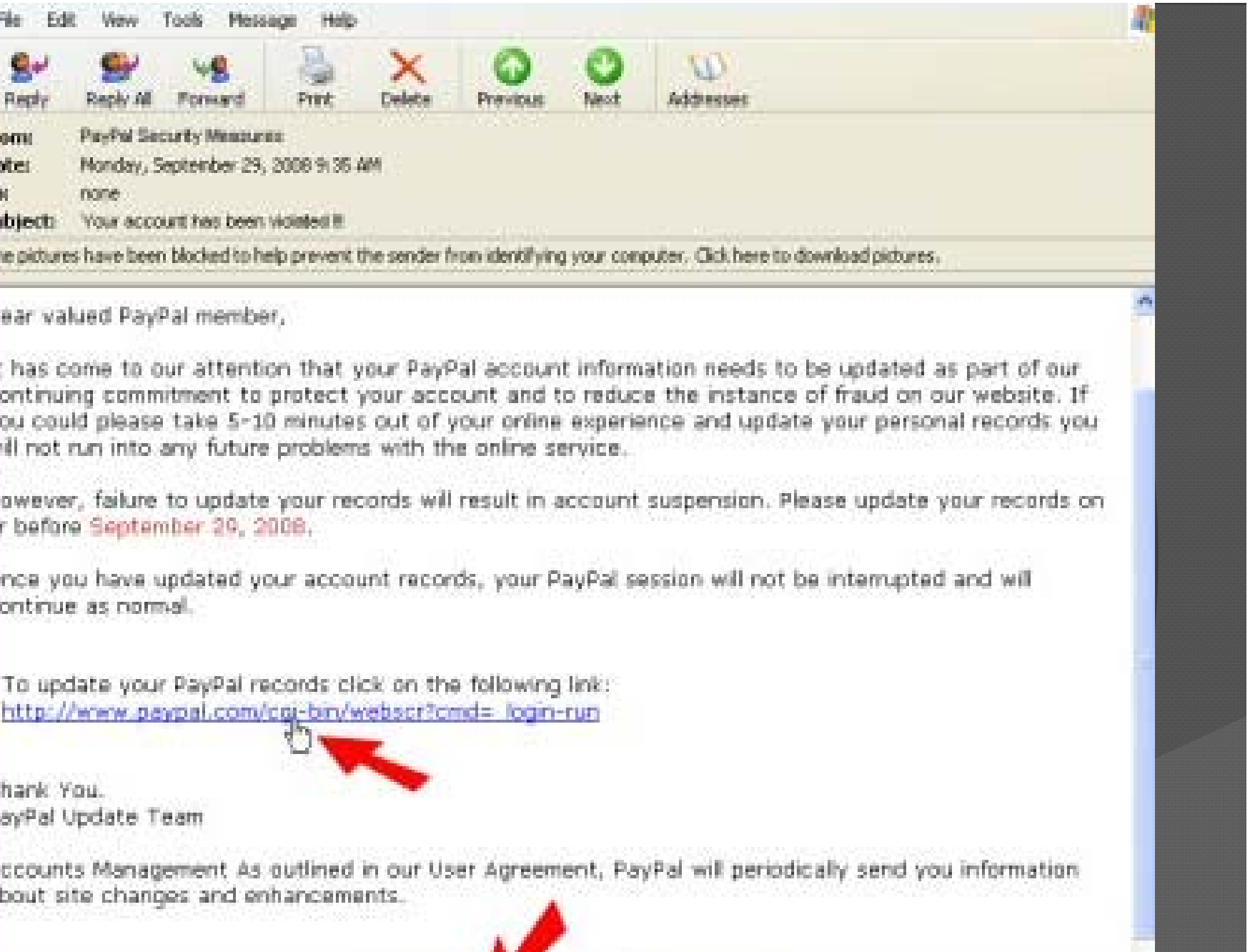
Your account will be closed.

The IT Department…

Verify your security details.

You owe us money.

- Our system has been breached, please check your account status.
- You've won money (or anything else).
- Generic greetings
  - "Hello bank customer"
- Misspelled words, poor grammar


File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
PayPal Security Measures
Monday, September 29, 2008 9:35 AM
none
Your account has been violated !!!
e pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.
ear valued PayPal member,
has come to our attention that your PayPal account information needs to be updated as part of our
ontinuing commitment to protect your account and to reduce the instance of fraud on our website. If
ou could please take 5-10 minutes out of your online experience and update your personal records you
ill not run into any future problems with the online service.
owever, failure to update your records will result in account suspension. Please update your records on
before September 29, 2008.
nce you have updated your account records, your PayPal session will not be interrupted and will
ontinue as normal.
To update your PayPal records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run
hank You.
ayPal Update Team
ccounts Management As outlined in our User Agreement, PayPal will periodically send you information
bout site changes and enhancements.

potting the Hook

- Provide Social Security Number, Password, Date of Birth, and similar information.
- Legitimate companies will not do this over email!
- Look carefully at the links! Type the site in your browser in stead. Never click on email links.
- Are there typos, generic reference (e.g. Dear Customer), or scare tactics (e.g. “Your account will be shutdown immediately!”)

potting the Hook

Never click on links in email.

- Go to the website directly in a browser.

Look carefully at the sending (from) address.

Call the company on the phone using a published number.

If a known sender, verify they sent the email.

If you are being offered something too good to be true, it is.

Resources

eporting

- ictims can report to
  ocal Law Enforcement
- nternet Crimes Complaint Center
  ttps://www.ic3.gov/
- ederal Trade Commission (FTC)
  ttps://www.ftc.gov

nvestigation

- The investigation of these cases involve:
  - Tracing network events and assigned Internet addresses.
  - Finding the registered owners of the servers/services.
  - Performing computer forensic examinations of victim's computers.
  - Following the money through various financial institutions to the pay-off point.

utcomes

- Establishing ownership of servers and sourcing emails problematic.
- Often servers are shutdown shortly after the scam starts.
- Often the servers are operated in a foreign country.
- Potentially, follow money trail.
- Outcomes are usually poor.

esources

icrosoft Fraud Protection Site
tp://www.microsoft.com/protect/

nti-Phishing Working Group
ww.antiphishing.org

hishTank
ww.phishtank.com

EPORTS:
tp://www.justice.gov/opa/report_on_phishing.pdf
tp://www.antiphishing.org/Phishing-dhs-report.pdf

ontact Information:

Pamela King
Chestnut Hill College
kingp@chc.edu
www.chc.edu
215-745-7148