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 many of you have more than one computer at home?

How do you connect to the Internet (DSL, cable, or dial-up)?

Do you have children at home and if so, what ages?

Have you ever been hit by a virus?

What are you using to read your e-mail?

Do you back up your computer? How often?

Do you back up your data? How often?

Do you use encryption?
Types

- Social networking sites
  - Facebook
  - Twitter

- Blogging sites
  - Xanga
  - LiveJournal

- Video sharing
  - YouTube

- Photo sharing
  - Flickr

- Bookmarking sites
  - Digg
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.
Social Networking Sites

Billy Bob, Jr.
Profile Management

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

- Desk call personnel
- Janitorial
- Dumpster diving
- Eagerly talkative employees
- Contract staff
- Delivery personnel

Corporate
Demonstration

Dumpster Diving video
Discussion

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
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.


Thank you for using First Tennessee Bank
Phishing

SSL

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?

Yes  No  View 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
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 Jay

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
Exercise 3
Exercise 4

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 manage your account.

User ID

Password

I forgot my user ID
I forgot my password
Questions

Thank you for attending if you have questions

Jayson.ferron@globalknowledge.com