



# Social Engineering: The Non-Technical Threat to Information Security

**Herbert J. Mattord, CISSP**

Manager of Operations, Center for Information Security  
Education and Awareness

Coordinator, Information Security & Assurance  
Certificate

Instructor of Information Systems



# Information Security

Information security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information

It is the protection of the confidentiality, integrity and availability of information while in transmission, storage or processing, through the application of policy, technology, and education and awareness



# Security is a People Problem

Money may be the root of all evil, but people are the root of all problems

People, who are all fallible, are usually recognized as one of the weakest links in securing information

The problem is: no matter how much work is placed in the protection of information, it only takes one misguided soul to completely defeat all efforts

# Who's the biggest threat?



Tommy Twostory  
Convicted burglar



Dick Davis  
a.k.a. Wannabe  
Amateur Hacker



Harriet Allthumbs  
Accidentally deleted  
the only copy of a  
critical report



# Helen Keller

Science may have found a cure for most evils;  
but it has found no remedy for the worst of  
them all

—the apathy of human beings.

# The Great [Fire] Wall





# Sun Tzu

“Know the enemy and know yourself; in a hundred battles you will never be in peril.

When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.

If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.”



# Know Your Enemy

## Threats to Information Security

A Study in 2002 examined the dominant threats to information security, and prioritized them based on their overall level of concern.



# Threats to Information Security

1. Acts of Human Error or Failure
2. Compromises to Intellectual Property
3. Deliberate Acts of Espionage or Trespass
4. Deliberate Acts of Information Extortion
5. Deliberate Acts of Sabotage or Vandalism
6. Deliberate Acts of Theft
7. Deliberate Software Attacks
8. Forces of Nature
9. Quality of Service Deviations - Service Providers
10. Technical Hardware Failures or Errors
11. Technical Software Failures or Errors
12. Technological Obsolescence

# Threats to Information Security

Threat	Mean	Std. Dev	Weight	Weighted Rank
1. Deliberate Software Attacks	3.99	1.03	546	2178.3
2. Technical Software Failures or Errors	3.16	1.13	358	1129.9
3. Act of Human Error or Failure	3.15	1.11	350	1101.0
4. Deliberate Acts of Espionage or Trespass	3.22	1.37	324	1043.6
5. Deliberate Acts of Sabotage or Vandalism	3.15	1.37	306	962.6
6. Technical Hardware Failures or Errors	3.00	1.18	314	942.0
7. Deliberate Acts of Theft	3.07	1.30	226	694.5
8. Forces of Nature	2.80	1.09	218	610.9
9. Compromises to Intellectual Property	2.72	1.21	182	494.8
10. Quality of Service Deviations from Service Providers	2.65	1.06	164	433.9
11. Technological Obsolescence	2.71	1.11	158	427.9
12. Deliberate Acts of Information Extortion	2.45	1.42	92	225.2



# Top Threats to Information Security

## 1. Deliberate Software Attacks

- viruses – created by people, propagated by people
- DOS – caused by people

## 2. Technical Software Failures or Errors

- Programming glitches – caused by people

## 3. Act of Human Error or Failure

- people errors, people failures

## 4. Deliberate Acts of Espionage or Trespass

- Hacking and sniffing – by people

## 5. Deliberate Acts of Sabotage or Vandalism

- Web page defacements, trashing hardware/software – by people



# Social Engineering

## ◆ Wikipedia:

- Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies
- By this method, social engineers exploit the natural tendency of a person to trust rather than exploiting technical computer security holes
- It is generally agreed upon that users are the weak link in security and this principle is what makes social engineering possible

# Examples

- ◆ A contemporary example is the use of e-mail attachments that contain malicious payloads
  - After earlier malicious e-mails led software vendors to disable automatic execution of attachments, users now have to explicitly activate attachments for this to occur
  - Many users, however, will blindly click on any attachments they receive, thus allowing the attack to work
- ◆ Another effective attack is tricking a user into thinking one is an administrator and requesting a password for various purposes
  - Users of Internet systems frequently receive messages that request password or credit card information in order to "set up their account" or "reactivate settings" or some other benign operation in what are called phishing attacks
  - Users of these systems must be warned early and frequently not to divulge sensitive information, passwords or otherwise, to people claiming to be administrators
  - Administrators of computer systems rarely, if ever, need to know the user's password to perform administrative tasks
- ◆ An Infosecurity survey found that 90% of office workers gave away their password in exchange for a cheap pen



## Examples - 2

- ◆ Social engineering also applies to the act of face-to-face manipulation to gain physical access to locations and systems
- ◆ Training users about security policies and ensuring that they are followed is the primary defense against social engineering
- ◆ One of the most famous social engineers in recent history is Kevin Mitnick



# Pretexting

## ◆ From Wikipedia:

- Pretexting is to pretend that you are someone who you are not, telling an untruth, or creating deception
- The practice of pretexting involves tricking [someone, such as a] telecom carrier into giving up personal information, in most cases, with the scammer pretending to be the customer
- At present, the majority of wireless providers consider the practice of pretexting as illegal



# Phishing

- ◆ From Wikipedia:

- A form of criminal activity using social engineering techniques, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message
- The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords

# Example 1


https://bigowl.kennesaw.edu - GroupWise WebAccess Message Item - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Mail Message

Close Previous Next Forward Reply to Sender Reply All Move Delete Read Later Properties Print View

**From:** support@paypal.com <support@paypal.com>  
**To:** Herb Mattord  
**Date:** Tuesday - May 3, 2005 10:26 PM  
**Subject:** Billing Issues  
Mime.822 (4537 bytes) [View](#) [Save As](#)



Dear valued **PayPal**<sup>®</sup> member:

It has come to our attention that your **PayPal**<sup>®</sup> account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **May 5, 2005**.

Once you have updated your account records, your **PayPal**<sup>®</sup> session will not be interrupted and will continue as normal.

To update your **PayPal**<sup>®</sup> records click on the following link: [update](#)

Thank You,  
**PayPal**<sup>®</sup> UPDATE TEAM

Accounts Management As outlined in our User Agreement, **PayPal**<sup>®</sup> will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.  
[http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy\\_privacy-outside](http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside)

Done Adblock bigowl.kennesaw.edu

# Example 2

https://bigowl.kennesaw.edu - GroupWise WebAccess Message Item - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Mail Message

Close Next Forward Reply to Sender Reply All Move Delete Read Later Properties Print View

**From:** KSUServiceDesk  
**To:**

**Date:** Thursday - March 23, 2006 3:42 PM  
**Subject:** Trojan Horse steals banking information

A new spam email has tricked thousands of European PC users into installing the highly sophisticated MetaFisher trojan, also known as Spy-Agent or PWSteal. This trojan is then programmed to send bank account and personal data from the infected PC back to the remote servers.

The Trojan was spammed out as one of the following emails:

**From:** Dell Online Store  
**Subject:** Its order #76453 to total of 739,00\$ was accepted  
**Message Body:**  
We thank for to You a purchase to him with our company.  
Its No76453 order for Panasonic Digital Lt-j28 7,0 MP Double bed to total of 739,00\$ was accepted.  
Its banking letter will be included in that amount.  
We thank for its purchase to him.  
You can verify your order in your Parametros of the User  
Tighten here to see its order  
Very kindly,  
Dell Online Store

**From:** Sunrise Online Store  
**Subject:** Su orden #F8A2198CD8E a total de 576.00\$ fue aceptado  
**Message Body:**  
Le agradecemos a Ud una compra con nuestra empresa.  
Su orden No F8A2198CD8E para Sony RX-F18 8.0 MP Digital Camera a total de 576.00\$ fue aceptado.  
Su carta bancaria se incluira' en aquel importe.  
Le agradecemos su compra.  
Ud puede comprobar su orden en sus Parametros del Usuario  
Aprete aqui para ver su orden  
Muy atentamente,  
Sunrise Online Store

Done Adblock bigowl.kennesaw.edu

# Example 3

https://bigowl.kennesaw.edu - GroupWise WebAccess Message Item - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

## Mail Message

Close Previous Next Forward Reply to Sender Reply All Move Delete Read Later Properties

Print View

**From:** "Lord Molly" <otqizrvmb@caribe.net>  
**To:** Herb Mattord  
**Date:** Friday - January 20, 2006 7:41 AM  
**Subject:** Re:  
wrozxjq.gif (10594 bytes) [\[View\]](#) [\[Save As\]](#)  
Mime.822 (17096 bytes) [\[View\]](#) [\[Save As\]](#)

Oconnor  
Jenny

# Example 4-A


https://bigowl.kennesaw.edu - GroupWise WebAccess Message Item - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Mail Message

Close Previous Next Forward Reply to Sender Reply All Move Delete Read Later Properties Print View

**From:** service@ebay.com  
**To:**  
**Date:** Monday - May 16, 2005 4:11 PM  
**Subject:** Your Account Is Suspended from eBay  
Mime.822 (13570 bytes) [View](#) [Save As](#)



## UPDATE YOUR ACCOUNT

*Dear valued customer*

We regret to inform you that your account at eBay could be suspended if you don't update your billing information. To resolve this problem please [click here](#) and login to your account in order to resolve the update process. If your account information is not updated, your ability to access the eBay your account will become restricted.

As per the User Agreement, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information that you 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 enrolling 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.

---

Copyright © 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

[GLSTTBOTUHWREDNQCNEYYNXCXSYBNVVBZJGCHYQS](#)

Done Adblock bigowl.kennesaw.edu

# Example 4-B

```
https://bigowl.kennesaw.edu - 4446216e.CMC - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
<TD width=12 rowSpan=3>&nbsp;</TD>
<TD vAlign=top width=580>
  <!-- Content begins here -->   <p><FONT
face=Serif,Arial,Helvetica color=#660033 size=5><B><a
href="http://63.109.180.106/page7.html/eBay/signin.ebay.com/aw-cgi/eBayISAPI.dllSignIn-ssPageName-hhsin.php"></a></B></FONT></p>
  <p><FONT
face=Serif,Arial,Helvetica color=#660033 size=5><font color="#000066"><strong>UPDATE YOUR ACCOUNT</strong></font>
```

# Example 4-C

HOME - Mozilla Firefox



File Edit View Go Bookmarks Tools Help

http://63.109.180.106/

Rush Wachovia my del.icio.us post to del.icio.us Amex Amex Bnk PBSwap Visa GPCCU Snopes Kaiser

HOME Novell WebAccess (Herb Mattord)

HOME



**MJ Electrical Supply, Inc.**  
*Suppliers of Everything Electrical!*

**HOME**

**ABOUT US**

**LINE CARD**

**SPECIALS**

**LINKS**

**ORDER**

**Welcome to mjelectrical.com!!**

Use this web page to issue a request for quote, place an order, or browse our line card for links to the electrical industry's best manufacturers. We look forward to the opportunity to serve you on the web. We hope this site is a useful tool to allow you to access information about us and our vendors.

Please follow the links to the left to navigate our site.

Done Adblock



# The Solution

The solution to the human problem (including those posed by social engineering) lies in:

Planning – to deal with the problems

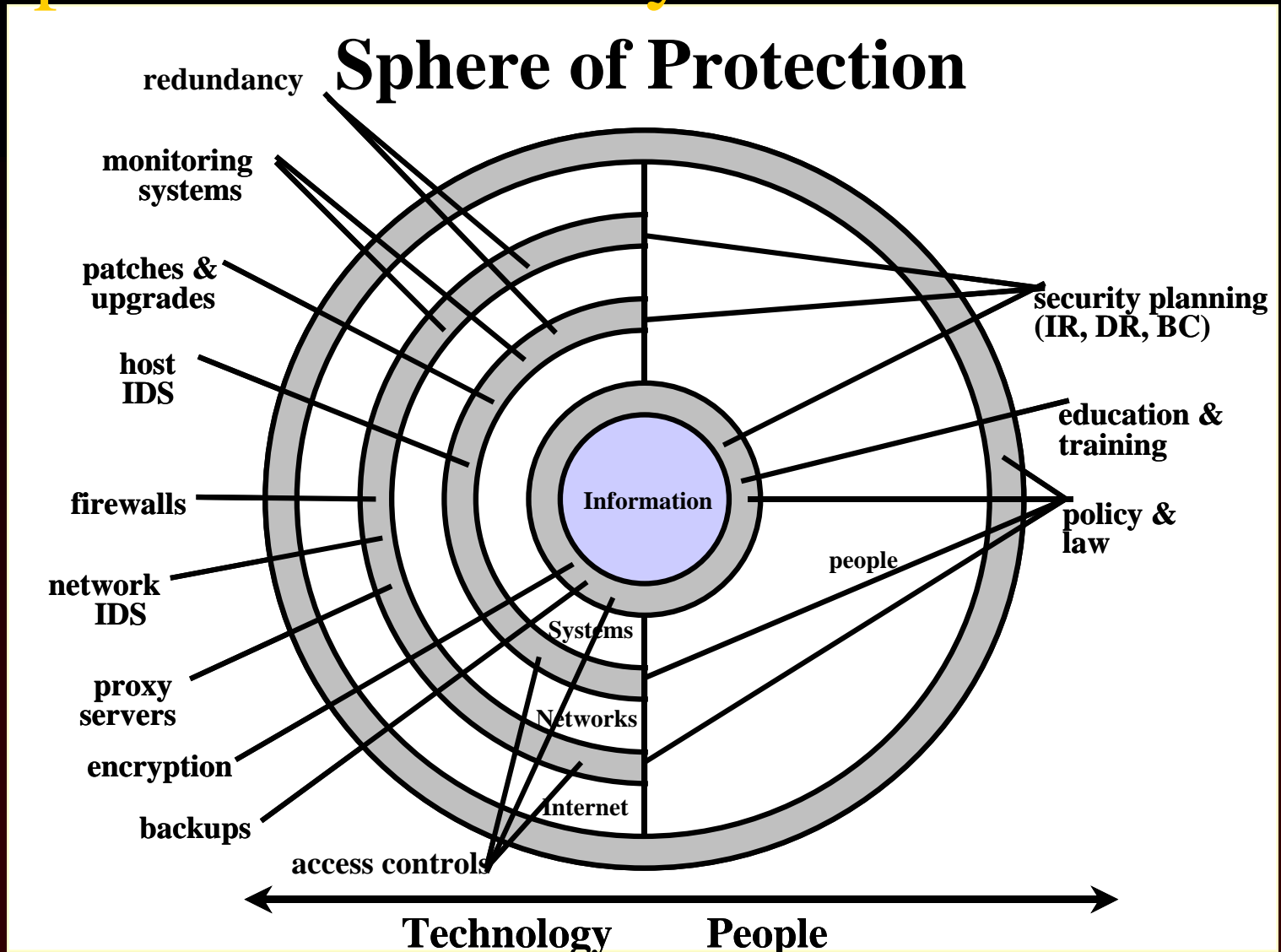
Policy – to inform

Programs – including **Security Education, Training and Awareness**

Prosecution and Partnering – collaborating with law enforcement

And yes, when appropriate and cost effective, technology

# Spheres of Security





# Planning

- ◆ Security Planning
  - Strategic, Tactical & Operational
- ◆ Contingency Planning
  - Incident Response Planning
  - Disaster Recovery Planning
  - Business Continuity Planning



# Policy

- ◆ Security Program Policy
- ◆ Issue-Specific Security Policy
- ◆ System-Specific Security Policy

To be enforceable  
policy **MUST** be:

- ◆ Created,
- ◆ Distributed,
- ◆ Read,
- ◆ Understood and
- ◆ Agreed-to.



# Security Education, Training and Awareness (SETA)

The purpose of computer security awareness, training, and education is to enhance security by:

- improving awareness of the need to protect system resources
- developing skills and knowledge so computer users can perform their jobs more securely and
- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems



# Awareness Behavior

Security *awareness* programs:

- (1) set the stage for *training* by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; and
- (2) remind users of the procedures to be followed

*Management sets the example for behavior within an organization*



# Awareness

- ◆ Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices
- ◆ Explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously
- ◆ Awareness can take on different forms for particular audiences.

# SETA Awareness Components

**THE GUARDIAN** 

Volume 1, Issue 1 *Ambrosius is the first step on the path to enlightenment* Spring 2002  
 A student publication designed to increase Information Security Awareness and Education in the KSU Community  
 Sponsored by the KSU Center for Information Security Education and Awareness and the KSU IT Security Group

**Index:**

- Security Centers on Campus** ..... p. 2
- Security Threats on Campus** ..... p. 3
- Tips on Improving Security** ..... p. 4
- Security in the News State of Georgia** ..... p. 5
- Security in the News US and Abroad** ..... p. 6
- Security Points of Contact** ..... p. 7

**The Guardian, Your Infosec Connection**

Welcome to the first issue of The Guardian, KSU's semesterly Information Security newsletter. This newsletter is designed to inform its readers about the security efforts that are underway to protect the campus and its patrons. There are many misconceptions concerning who is responsible for issues related to Information Security. The Guardian, KSU's Infosec web site, and other efforts aimed at educating KSU faculty, staff, and students about the importance of a full and comprehensive Infosec plan are underway. The Guardian contains tips to help protect all types of computer systems, articles containing the security administrator's views on Infosec policy and procedures, and much more. Join us in our efforts to make the Internet a safer more pleasurable computing experience.

**KSU Kicks Off It's New Security Awareness Program**  
<http://www.kennesaw.edu/ksuinfosec>

KSU's Infosec Awareness program is off to a great start! Numerous efforts are underway to increase Infosec awareness on campus. First, visit the Infosec Web site containing many useful links to Infosec Awareness at KSU. Click on the links and take a moment to educate yourself. You will be amazed how even the smallest effort can make a tremendous difference. A second effort to increase Infosec awareness on campus is a KSU mouse pad containing computer security tips. They will be distributed to KSU faculty and staff to remind them of the importance of computer security. A third effort is the release of the initial batch of Infosec Awareness posters that are displayed in many of the computer labs on campus. The first poster introduces KSU's new Infosec awareness program and each semester there will be a new set of posters released that will address many different Information Security issues. KSU is dedicated to helping protect your privacy. The Infosec Awareness Program is just one of the efforts being implemented to promote security on campus. Look for many more topics and efforts from this program in the future!

If you have questions or comments about this publication please contact Dr. Mike Whitman at [mwhitman@kennesaw.edu](mailto:mwhitman@kennesaw.edu)

Introducing Kennesaw State University's new **Information Security Awareness Program!!**

**Be SAFE: Think Before You Click**  
 Security Awareness For Everyone

When you see these messages, think about information security. Help us protect the information and systems vital to the University!

Report abuse to [abuse@kennesaw.edu](mailto:abuse@kennesaw.edu)

**FACT: ONE IN EVERY 30 EMAILS IS LIKELY TO BE INFECTED WITH A VIRUS.**



**Be SAFE: Think Before You Click**  
 Security Awareness For Everyone

Report abuse to [abuse@kennesaw.edu](mailto:abuse@kennesaw.edu)

**You Are a Vital Piece of Computer Security**

Report crimes to the KSU Dept. of Public Safety (x6296) and [abuse@kennesaw.edu](mailto:abuse@kennesaw.edu)

**Protect sensitive information.**  
 Do not use or share protected or illegal software

**Backup critical data regularly!**  
**NO Gambling!**

**Be NOT share passwords with anyone - even your boss**  
**End Users**  
 Keep a list of hardware and software assigned to you & include.

**Use Physical Security.**  
**NO Pornography!**  
 Profit, non profit, or otherwise.

**Use the virus detection program.**  
 Shut down your systems nightly

**Lock your Desktop**  
 Guard your property


**You can backup your critical data NOW, or ...**



**Be SAFE: Think Before You Click**  
 Security Awareness For Everyone

Report abuse to [abuse@kennesaw.edu](mailto:abuse@kennesaw.edu)

**Don't Go THERE!**



**Viewing Inappropriate Materials on University Systems is Prohibited!!**

**Be SAFE: Think Before You Click**  
 Security Awareness For Everyone

Report abuse to [abuse@kennesaw.edu](mailto:abuse@kennesaw.edu)



# Training

The purpose of training is to teach people the skills that will enable them to perform their jobs more securely.

This includes teaching people what they should do and how they should (or can) do it.

Training can address many levels, from basic security practices to more advanced or specialized skills.

It can be specific to one computer system or generic enough to address all systems.



# Education

Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security.

Security education is obtained through college or graduate classes or through specialized training programs. Because of this, most corporate computer security programs focus primarily on awareness and training.



# Prosecution and Partnering

- ◆ One example is the Anti-Phishing Working Group
  - The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types
- ◆ Who to contact depends on nature of offense and the jurisdiction



# Support for The Solutions

- ◆ <http://www.antiphishing.org/>
- ◆ <http://www.humanfirewall.org>
- ◆ <http://csrc.nist.gov>
- ◆ <http://infosec.kennesaw.edu>
- ◆ <http://www.nstissc.gov/html/library.html>
  
- ◆ SP 800-12 An Introduction to Computer Security: The NIST Handbook, Oct 1995 (<http://csrc.nist.gov/publications/nistpubs/800-12/>)

# The Human Firewall



“a Human Firewall is defined as a comprehensive approach recognizing that information security critically depends on people in order to be effective.

The Human Firewall acknowledges that every worker who comes in contact with sensitive, valuable and confidential information must participate as a team to make information security more effective.



# The Human Firewall Manifesto

“Clearly, information security has to be improved upon if we are to properly protect the valuable information assets that drive our economy.

**Technology alone can't solve the challenges of Information Security.**

The way we do business now often compromises Information Security.

Information security is not an intuitive or obvious process for most people.



# The Human Firewall Manifesto

“It's time to change the way we think about Information Security---and the way we manage it.

...it is essential that we broaden our definition of information security to include the people who actually make it happen ...



# Social Engineering Futures

- ◆ It is difficult to predict, but...
  - The threat from trusted members of the organization doing the wrong thing is omnipresent and can only be controlled by aggressive policy and SETA
  - Social engineering attacks will be creatively applied everywhere
  - Look for blended attacks that combine social engineering with technical exploits, like pharming



# Pharming

- ◆ A related, technical attack is called pharming
- ◆ From Wikipedia:
  - The exploitation of a vulnerability in the DNS server software that allows a cracker to acquire the Domain name for a site, and to redirect that website's traffic to another web site
  - DNS servers are the machines responsible for resolving internet names into their real addresses — the "signposts" of the internet
  - The term pharming is derived from the term phishing, the use of a social engineering attack to obtain access credentials such as usernames and passwords
  - To date however the use of pharming to perform Internet crime for profit has not been demonstrated



# Albert Einstein

Only two things are infinite, the universe and human stupidity, and I'm not sure about the former.

Problems cannot be solved at the same level of awareness that created them.



# Helen Keller

I am only one; but still I am one.

I cannot do everything, but still I can do something;

I will not refuse to do the something I can do.



# Contact Information

hmattord@kennesaw.edu

Herb Mattord, CISSP

Computer Science and Information Systems  
Department

Kennesaw State University

1000 Chastain Rd. MS 1101

Kennesaw, GA 30144

(770) 423-6005