Introduction

• What ARSC is
  – part of the University of Alaska Fairbanks

• Why the training
  – To provide an introduction to the various security issues involved with computing and data management.

Information Assurance (IA) and Phishing Training

Version 1.3 (August, 2011)

ARSC

Importance of Information Assurance

Information Assurance Visibility

• Identity theft on the rise
  – Online data brokers collect and sell personal information
  – Thieves purchase reports with stolen credit cards and use information to obtain phony documentation
  – Internet fraud is one of the fastest growing white collar crimes

• Hijacked computers
  – Potentially millions of systems are in botnets
  – Hijacked systems can be used for spam, DDOS attacks, illegal file distribution, etc.

Information Assurance Overview

Information Assurance (IA) - Information Operations that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authenticity, and non-repudiation.

• Confidentiality - Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

• Integrity - Protection against unauthorized modification or destruction of information

• Availability - Timely, reliable access to data and information services for authorized users.

• Authenticity - Assures the recipient that the message is actually from the sender and has not been changed in transit

• Non-Repudiation - Provides the sender verification that the message was delivered and provides the recipient proof of the sender’s identity
Sources of Laws, Policies and Directives

- Federal Laws
- State of Alaska Laws
- University of Alaska Regulations.
- ARSC Policies

Importance of Information Assurance

Information Assurance Concepts

Threat - Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Vulnerability - Any weakness in an information system (IS), cryptographic system, or components (e.g. system security procedures, hardware design, internal controls) that could be exploited.

Laws, Policies, Directives (UA/ARSC)

University of Alaska Board of Regents Policies
- www.alaska.edu/bor/policy.regulations

ARSC User and Security Policies
- http://www.arsc.edu/support/policy/policy
- http://www.arsc.edu/support/policy/secpolicy

Threats

<table>
<thead>
<tr>
<th>Natural Threat</th>
<th>Human Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Events</td>
<td>System Environment</td>
</tr>
<tr>
<td>• Lightning</td>
<td>• Poor wiring</td>
</tr>
<tr>
<td>• Fires</td>
<td>• Insufficient cooling</td>
</tr>
<tr>
<td>• Hurricanes</td>
<td>• Accident</td>
</tr>
<tr>
<td>• Tornadoes</td>
<td>• Bad habit</td>
</tr>
<tr>
<td>• Floods</td>
<td>• Careless act</td>
</tr>
<tr>
<td></td>
<td>• Incorrect information</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Unintentional</td>
<td>Intentional</td>
</tr>
<tr>
<td>• Corporate Raider</td>
<td>• Disgruntled employee</td>
</tr>
<tr>
<td>• Social Engineer</td>
<td>• Hacker</td>
</tr>
<tr>
<td>• Engineering</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Threats

- Social Engineering is an intentional, human threat that is defined as:
  "a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim."


Risks When Interacting with Internet Sites and Services

- Phishing
  - This is where one web site pretends to be another so that it can gather confidential and/or private information.

- Cookies
  - Small snippets of information that are stored in your web browser and that are manipulated by web sites

- Unknown and/or downloaded code
  - Mobile code
  - Malicious code

Phishing

- "Phishing" is the process whereby malicious users employ a combination of Social Engineering and browser/internet vulnerabilities to trick a user into disclosing personal or otherwise sensitive information to a criminal enterprise.
- In addition to collecting information, many phishing emails can also install malicious software (typically spyware) onto the user’s system.
- Targeted Phishing attempts (where the phisher starts with knowledge about you) are called Spear Phishing and can frequently be very hard to detect.

Ways to spot a phishing attempt

- A business or service that you do not have an account with
- Odd looking fields in the email
- Generic greetings
- Obviously faked email addresses
- Poor spelling or grammar
- False sense of urgency
- Fake or deceptive web links
Phishing

- **Browsers**
  - New web browsers like Firefox and IE7 can help by checking the URL you are going to against a database of known phishing sites and then warn you when they suspect you are at a bogus location

- **Email**
  - Never trust the URLs in an unsolicited email sent to you
    - View the ‘raw’ or plain text version of the message
    - Type the listed URL into your browser rather than clicking on the link in the message

Phishing Email Example

Phishing Email ‘raw’ Text

Malicious Code

- **Malicious Code** - software intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity or availability of an information system

  - **Viruses**
    - Generally spread via email or portable media

  - **Trojan Horses**
    - Backdoors, phising, etc

  - **Worms**
    - Self propagating
    - Often used to spread other types of malware
**Rules for Computing on ARSC Systems**

- Use the computer only for legitimate authorized use
- Don’t interfere with other’s work
- Don’t look at other’s files unless you have permission
- Don’t use the computer to steal
- Don’t use or copy unauthorized software
- Don’t steal intellectual property
- Use your own account.

Ref: [http://www.arsc.edu/support/policy/secpolicy](http://www.arsc.edu/support/policy/secpolicy)

---

**Authentication/Authorization**

- **Account Sharing**
  - Is not allowed under ARSC’s security policies.
- **Secure Shell (ssh)**
  - Available for most platforms and operating systems
  - Uses either SecurID or SSH Public Key
- **Passwords/Passphrases**
  - “Static” passwords do not change from login to login and are not used on most ARSC systems

---

**Tips for Creating Secure Passwords and Passphrases**

- Develop a password management system
- Choose a password at least eight characters long
- Combine letters, numbers, special characters
- Use keyboard patterns, or alphanumeric patterns/associations
- Avoid words or phrases in dictionary
- Avoid using personal information
- Memorize password and/or store it in a secured location or program
- Change password regularly

Ref: [http://www.arsc.edu/support/policy/password](http://www.arsc.edu/support/policy/password)

---

**Data and Storage**

- **Backups / Purging**
  - Purging is done on temporary directories and affects files that have not been accessed in 30 days
  - [http://www.arsc.edu/support/howtos/storage](http://www.arsc.edu/support/howtos/storage)
- **File permissions**
  - Dot files
  - World-write is never a good idea
- **Data Sharing**
  - Use the Unix group to own files
Physical Security

• Access Labs
• Keys and key cards
• Screen locking
• Cable locks for laptops and other peripherals

Security Tips for Home Computer

• Scan your system regularly with updated anti-virus software
• Scan all email attachments and files downloaded from the internet
• Download software updates and patches regularly
• Install and use firewall when connected to the internet
• Backup all important files
• Use complex passwords
• Disconnect computer from Internet when not in use
• Be aware of the risks of peer to peer file sharing programs

Where to find more information

• ARSC web pages
  http://www.arsc.edu
• ARSC IA page
  http://www.arsc.edu/support/policy/ia
• ARSC Help Desk
  – 08:00 - 17:00 (AK) Monday - Friday
  – consult@arsc.edu
  – <voice> 907-450-8602
  – <fax> 907-450-8603