Information Security

2010

Information Security

Awareness Program

Agenda

Program Objectives

Emerging Threats of Cybercrime

Information Security Policy

User Responsibilities

Question & Answers

Agenda

- Program Objectives
- Emerging Threats of Cybercrime
- Information Security Policy
- User Responsibilities
- Question & Answers

Program Objectives

Saveology.com
We Compare, You Save

A Word From Upper Management

Security Awareness Program

The company believes that understanding the role that each of us plays in the implementation of the security awareness program is essential to our enterprise's operations, work philosophy and reputation.

Its Everyone's Responsibility

It is through this program that each of us will gain and understanding of the responsibility we all have to protect the **Availability, Integrity** & **Confidentiality** of the Company's information assets by applying guidelines, and practices learned from this program to everyday activities.

Program Objectives

Information Security Areas of Responsibility

Availability

Assurance that the systems responsible for delivering, storing, and processing information are accessible when needed by those who need them.

Integrity

Assurance that the information is authentic and complete, and that information can be relied upon to be sufficiently accurate for its purpose. Integrity addresses whether or not data is trustworthy and reliable.

Confidentiality

Assurance that information is shared only among authorized persons or organizations.

Agenda

Program Objectives

Emerging Threats of Cybercrime

Information Security Policy

User Responsibilities

Question & Answers

Emerging Threats of Cybercrime

To guarantee security an enterprise has to make sure that 100% of its systems are invulnerable – **100% of the time!**

To bypass security, an attacker only has to find **one** vulnerable system.

Risk – It's Everywhere!

- Exposure to personal identification information (CC#, SS# etc...)
- Malware: viruses, worms, key-loggers, root-kits, spy-ware etc..
- Vulnerable networks & systems
- Access to a unprotected wireless network
- Increasingly powerful hacker tools
- Skilled technical professionals, hackers, organized crime / web mobs, script kiddies etc...

Emerging Threats of Cybercrime

What really matters:

- Do we understand?
- Can we educate?
- Are we prepared?
- Do we share?

Emerging Threats of Cybercrime

Understand:

- That there are constantly changing threats
- That you can be a target
- The bad guys are smart and have time to spend on attacks

Educate:

- Starts at the top and works its way down
- Understand that it is not your computer**. It's the company's**
- Understand company Information Security Policies

Prepare:

- Plan for the best – prepare for the worst
- Have a plan
- When it happens, don't be caught saying "what do we do now?"

Share:

- Collaborate with other security experts and organizations for trends etc…
- The bad guys do….(DEFCON, user groups etc..)

Emerging Threats of Cybercrime

Saveology.com
We Compare, You Save

Summary:

The Internet is a very powerful tool. Unfortunately, some people do not use it appropriately.

Therefore, please be very careful when clicking on links, installing applications and opening emails unless its from a trusted source.

You can't predict …but you can prepare!

Hope is not a strategy!

Agenda

- Program Objectives
- Emerging Threats of Cybercrime
- Information Security Policy
- User Responsibilities
- Question & Answers

Information Security Policy

Why is Information Security important?

Everyone has a role to play in protecting the Company.

Having a workforce that is well educated in proper Information Security practices helps the company deal more effectively with:

- Responding to emergency situations:
  - - Computer attacks
  - - Virus & worm outbreaks
  - - Threats to Identity information and safety of personnel
- Protection to our company and customers data
- Maintaining customer satisfaction!

We maintain our competitive advantage.

We have increased accountability and responsibility.

Information Security Policy

What are we protecting?

Company information in <u>any form</u> is a company asset:

- Customer confidentiality – Personal Identity Information (PII)
- Credit Card numbers
- Social Security numbers
- Banking information
- Networks
- Servers, laptops & desktops
- Documents (electronic & paper)
- Data files
- Fax machines
- External storage devices
- PDA's, cell phones and other mobile devices

Information Security Policy

Reporting a Violation

Employees discovering a violation of the Company's

security policies should notify:

- Their immediate supervisor
- Human Resources
- IT Helpdesk or Network Operations Center (NOC)

Information Security Policy

Saveology.com
We Compare, You Save

Summary:

Company information in any form is a company asset

The Company's security policies protect our information assets from:

- Internal & external threats
- Deliberate & accidental threats
- Use non-disclosure agreements whenever applicable

The goals of the information security policy are to:

- Limit risk to information assets
- Protect the privacy of employees and customers
- Enhance the operation of information assets to support our mission

Report policy violations to:

- Your immediate supervisor
- Human Resources
- IT Helpdesk or Network Operations Center (NOC)

Agenda

- Program Objectives
- Emerging Threats of Cybercrime
- Information Security Policy
- User Responsibilities
- Question & Answers

User Responsibilities

Objectives:

- Acceptable use policy
- Maintain Customer Confidentially
- Guidelines for protecting your password
- Guidelines for the appropriate use of email and the internet
- Guidelines for virus protection
- Information that is subject to monitoring when using company information assets

User Responsibilities

Objectives continued:

- Guidelines for data backups
- Guidelines for physical security
- Guidelines for copyrights & software licensing
- Management responsibilities
- Where to find company's:

- Information Security Policy
- Guidelines

User Responsibilities

Acceptable Use of Company Systems

You should use company information assets only for approved business purposes.

If you are unclear about what is considered appropriate or acceptable use for Saveology systems:

- Ask your manager or supervisor
- Review the Information Security Policy
- If a manager is not available, contact Human Resources or IT Operations

User Responsibilities

Maintain Customer Confidentially:

- Protect customer personal identification information:
- Keep credit card information secure & confidential:
  - No phones or cameras allowed at agent's desk
  - Leave personal belongings in your vehicle
  - Or securely in a Saveology approved locker
  - Do not write numbers down on any paper
  - No printing capabilities in our Contact Centers

User Responsibilities

User ID's and passwords should <u>not</u> be shared with anyone under any circumstances.

- Employees should never respond to unsolicited requests for their User ID or Passwords
(including requests from the helpdesk, NOC or system administrators)

- Employee passwords are not required to correct password problems, since support staff can reset passwords

- Do not share you password with anyone

- Employees are required to change passwords after 90 days

- Password protecting screensavers should be used

Q: How many passwords does it take to get into a Network?

A: Only one. **Protect it!**

User Responsibilities

Saveology.com
We Compare, You Save

Summary for protecting you password

Follow these password guidelines:

- Don’t tell anyone your password
- Don’t write your password down anywhere
- Don’t make a password easily guessed
- Change it every 90 days
- Think someone may have your password?

- Change it immediately!

User Responsibilities

Guidelines for use of Email and the Internet

Employees are expected to use Company Internet, Intranet and email communications systems in a manner that is:

- Professional
- Ethical
- Lawful
- In compliance with Company policies

User Responsibilities

Anti-virus Application

The following represent common mistakes that employees make in the work environment that directly impact security measures in place.

- Disabling the Anti-virus application
- Bringing software applications or electronic devices from home and installing them in the work environment
- Trusting every email that is received

User Responsibilities

Saveology.com
We Compare, You Save

Anti-virus Summary:

- Never disable an antivirus application
- Never load unauthorized software without approval and scanning
- Use caution when opening email attachments or when clicking on hyperlinks to the Internet
- Do not open email attachments unless you know the source, and are expecting the attachment
- Do not click on un-trusted hyperlinks to the Internet
  - ***Not all sites should be trusted***
- Do not accept automated downloads from websites

User Responsibilities

Privacy and Monitoring

Each employee is responsible for understanding that there is no expectation of privacy when using a company Information asset to create, store, send or receive information.

What does this really mean?

- Information stored on company computers is corporate intellectual property
- No user should expect that information is private and not subject to internal disclosure
- Any data traversing the network is subject to monitoring

- This includes, but is not limited to, Internet, email & voice traffic.

User Responsibilities

Data Backup

Every computer user is responsible for:

- Ensuring that frequent backups of critical data files are performed
- That important data files are not irreplaceable
- Do not cause a high replacement cost or are considered critical to the system

Any production data or applications on any user computer should be:

- Replicated to IT approved systems
- Copied to backup (spare) disk, USB device or tape
- Tested regularly to ensure proper and reliable backups

User Responsibilities

Physical Security

Saveology information assets must be protected from physical theft.

Good physical protection methods include:

- Lock laptops and devices when traveling
- Do not leave Saveology laptops or any information assets in your car
- Lock all PDA's Blackberry devices and cellular phones and do not leave them in the open unattended
- Confidential information resides on your computer. **Protect it!**
  If you leave your desk, remove all confidential information and lock computer with a locking (password) screensaver
- Keep printed material out of sight and locked within a desk drawer or filing cabinet

User Responsibilities

Physical Security continued:

- Protect information by assigning data classifications:
  - Confidential (shred when disposing)
  - Internal Use (shred when disposing)
  - Public
  - Unmarked
- Information Disposal Guidelines:
  - Never discard confidential Saveology information in regular trash or recycling bins
  - Always shred confidential and personal information prior to disposal
  - Destroy electronic storage media such as CD's, USB sticks or backup tapes prior to disposal
- If you lose or misplace your badge, report it to facilities **Immediately!**

User Responsibilities

Why copyright?

- A copyright notice must be used to protect software or other copyrighted materials developed by or for the Company.
- All copyrights of others must be honored and used in accordance with the copyright notice.
- Information you download from the Internet may be protected by copyright law.

What needs a Copyright?

- You must use a copyright notice to protect software or other copyrighted materials developed by or for the company.
- Any approved material that you post on public systems, bulletin boards or newsgroups must contain all proper copyright, trademark and disclaimer notices.

Software Licensing Guidelines:

- Employees may not agree to a license and may not download any material for which a registration fee is charged unless given prior written permission by their manager.
- All desktop and laptop software should be licensed appropriately by the IT department.
- You may not agree to a license or download any material for which a registration fee is charged, unless given prior written permission by your manager.

User Responsibilities

Saveology.com
We Compare, You Save

Management Responsibilities

- Enforcing the company information security policies
- Adhering to the company information security policies and procedures
- Maintaining the Availability, Integrity and Confidentiality of company information assets
- Protecting the reputation of Saveology to ensure our continued success

User Responsibilities

Saveology™ We Compare, You Save .com

Where can I find the Information Security Policy?

- Corporate Intranet*: http://www.saveologycentral.com*
- Human Resources
- Corporate Policies
  - **Information Security Policy**

Other important guidelines to be aware of:

- Employee handbook guidelines
- Code of business conduct / ethic guidelines
- Phone / e-mail policy guidelines
- Branding copyright policy

User Responsibilities

Summary:

- Understand the Information Security Policies “Acceptable use Policy”
- Maintain Customer Confidentially
- Protect your passwords. Use password protecting screensavers
- Use email and the Internet appropriately
- Make sure your anti-virus application is always up to date
- Information is subject to monitoring when using company assets
- Backup your data
- Follow guidelines for physical security
- Follow guidelines to copyright & software licensing
- Management & employee responsibilities are to protect company information assets
- Visit ***saveologycentral.com*** for company policy guidelines

Agenda

Saveology.com
We Compare, You Save

- Program Objectives
- Emerging Threats of Cybercrime
- Information Security Policy
- User Responsibilities
- Question & Answers

Information Security Awareness

Questions
&
Answers