Cyber Security Awareness Training

FY 2007

Welcome & Introduction

The Federal Information Security Management Act (FISMA) 44 USC 3544(b)(4) mandates that each federal agency provide annual training in computer security awareness and accepted computer practices.

This course will help you understand the responsibilities you have to protect VA's information assets, especially information about our veterans and it shows you ways to meet these responsibilities.

This course is mandatory for all VA employees, contractors and volunteers and any persons that use VA computers, networks, and electronic information systems. All new employees, contractors and volunteers are required to take this training within 30 days of joining VA.

Outcome Objectives:

1. identify the ISO and situations in which it is important to make contact;
2. create passwords in a manner that maintain their security effectiveness;
3. recognize confidential information and handle in a manner consistent with VA Policy;
4. comply with cyber security requirements that protect an individual's privacy;
5. recognize dangerous activities when using e-mail;
6. report suspected cyber security incidents to the ISO;

Continued next slide

Outcome Objectives:

7. recognize that VA's information is an important part of the nation's critical infrastructure;

8. know when an attempt is made to extract information without authorization;

9. identify instances where the use of VA's information resources is not authorized under the concept of "Limited Personal Use;" and

10. determine when computer gear needs to be thoroughly "scrubbed."

What is Cyber Security Awareness?

"Cyber Security Awareness" is the knowledge that VA employees, contractors, and volunteers use to protect VA computer systems and data. It refers to the personal responsibility each of us assumes for ensuring:

- the confidentiality, integrity, and appropriate availability of veterans' private data,

- timely and uninterrupted flow of information throughout the VA enterprise, and

- VA information systems are protected from the potential of fraud, waste and abuse.

Please be aware of any activity that might violate and/or compromise the security of VA information systems. Report all incidents to your information security officer, Donna Mills at extension is 6383 or pager 769.

Know Your ISO

Do you know:

- all the rules and requirements you should follow to keep VA's information secure?
- what to do if your computer is infected with an electronic virus?
- your responsibilities for maintaining confidentiality and privacy?
- your role in your facility's contingency plan?
- what to do if you witnessed someone using VA's computers for theft or fraud?

Your facility Information Security Officer has the answers!

Donna Mills is the Information Security Officer (ISO) for the WJB Dorn VAMC. She can be reached at ext. 6383 or pager 769.

Passwords

Passwords are important tools protecting VA information systems. They ensure you have access to the information you need.

Keep your password secret to protect yourself and your work. If you have several passwords, it is permissible to record and store them in a safe place, to which only you have access.

Passwords can be easily stolen or duplicated if constructed poorly. Most password thefts occur as a result of poorly constructed passwords or social engineering. We’ll discuss social engineering later in this course.

Password Requirements

Password must:

- Be constructed of at least eight characters (i.e., Gabc123&).
- Use at least three of the following four kinds of characters:
  - Upper case letters (ABC...)
  - Lower-case letters (...xyz)
  - Numbers (0123456789)
  - Special characters," such as #, &, *, or @.
- Be changed at least every 90 days.

Using these rules will provide you with a "strong" password.
VA requires strong passwords on all information systems .

Poor Password Construction

Many factors can contribute to poor passwords. Some of the most notable are:

- Passwords that are not "strong," as explained previously.
- Use of common words easily obtained from a dictionary.
- Passwords referring to your personal life (for example, names of family members or pets).
- Easily identifiable passwords are an open invitation to hackers.

Rules of Thumb for Passwords

- Don't use words found in a dictionary.
- Don't use personal references (names, birthdays, addresses, etc.)
- If you suspect that someone is trying or may have obtained your password, change it immediately, and inform your information security officer.
- Be sure nobody can watch over your shoulder while you type your password. Ask them to turn away while you type. Position your keyboard so that it is not easy to see what you type.
- If you have a number of passwords to remember, you may want to write them down. You must securely lock them away where they cannot be accessed by others.

Accounts for employees, volunteers, contractors, and students are to be terminated within 24 hours of their departure.

Risk Awareness

Username and password combinations, the primary method used by VA, provide a guarantee that you are who you say you are. Your username and password also limit you to only actions within your level of authorization.

Once the details of your username and password have been shared with others, you have lost control over how they may be used or abused.

It is worth noting that in most cases, usernames are very easy to get and tend to follow a pattern which relates directly to your own name. This is a necessary risk. Therefore, constructing strong passwords and maintaining their confidentiality is of great importance.

You are held solely accountable for your account access.
No one other than yourself should know your password(s).

Confidentiality

In VA, confidentiality is a must. Confidentiality is the condition in which VA's information is available to only those people who need it to do their jobs.

Breaches in confidentiality can occur when:

- you walk away from your computer without logging off
- paper documents are not adequately controlled
- you are accidentally given access to too much computer information.
- you have conversations about veteran's cases in public places such as elevators and hallways.

Breaches can occur when someone has access to information that they do not need to do their jobs.

Computer Disposal & Confidentiality

Need to get rid of old computer equipment? Be careful – all data must be removed prior to disposal. To ensure all data is removed from computers prior to disposal, all VA facility IT departments have a special software tool that prepares computers for proper disposal.

How you can help:

- Store your data on network drives instead of your desktop computer.
- If you notice computers being excessed without full data erasure, let your ISO know.
- Know that the "delete" command cannot remove all traces of data from your computer.

ONLY VA Dorn Information Management Service personnel are authorized to dispose of computer equipment!

Privacy

The Privacy Act requires that we as government employees take special care when we provide information to anyone about our veteran employees and other customers.

Providing personal information to anyone, including veterans themselves, must be done only by persons authorized to do so.

The same applies to requesting and receiving information about ourselves as employees and/or as veterans.

HIPAA

The Healthcare Insurance Portability and Accountability Act (HIPAA), is an additional requirement with which VA must comply. HIPAA established federal criminal penalties for wrongfully using/disclosing protected health information.

If you handle health care information in your job at VA, you need to know about HIPAA. HIPAA grants rights to individuals and imposes obligations on organizations.

For more information on Privacy and HIPAA you can go to the Privacy Awareness course or contact your local Privacy Officer.

Barbara Toole is the WJB Dorn VAMC Privacy Officer.

Her extension is 6270.

Helpful Guidance for Handling Privacy Requests

If another VA employee asks you for veteran information under your control, your response may depend on several things, including:

- The purpose of the request
- The authority of the individual making the request
- The established procedures for managing the request.

If the request does not follow the standard procedures that you are familiar with, do not hesitate to consult your supervisor for directions prior to accessing or disclosing any information.

Unauthorized access or use of veteran, employee, or enterprise information entrusted to VA is a serious offense. Disciplinary action can be brought against you as well as legal action that could result in civil and felony punishment.

Risk Awareness

Privacy laws are designed primarily to protect the people whose data you work with on a day-to-day basis.

The laws are there to ensure that veterans and their beneficiaries have recourse against intentional or unintentional misuse and abuse of protected data.

Your protection within the VA is to adhere to the procedures and check when you are unsure of how to handle information.

If you deviate from the established procedures, you and/or the VA could potentially become liable for any losses incurred in the event of legal action.

E-Mail

Proper use of VA electronic mail is essential to ensure this resource is uninterrupted and used in legal ways.

Chain letters and hoax messages rob us of valuable network capacity, computer space, and processing speed. You should not forward these messages to others. In fact, don't even request the sender stop sending you messages. Just delete them. These "please stop" messages sent by the thousands slow down our e-mail systems!

Sensitive information should not be sent using e-mail unless it can be done securely. Before you send sensitive information on e-mail, you must ensure that it can be done securely.

Some computer viruses attack e-mail systems, making them unavailable. You should learn to recognize the signs of a virus infection.

E-Mail Privacy and Security

Do not think of e-mail as being similar to a personal letter delivered to you in a sealed envelope by the post office. Instead, e-mail is more like a postcard. Most often, it gets delivered but there may be opportunities along the way for people other than the addressee to view the contents.

- E-mail is not considered private. You should have no expectation of privacy when using e-mail to transmit, store and communicate information.
- Private information about veterans and employees is not permitted to be transmitted by e-mail unless it is encrypted.
- E-mail is not considered secure. E-mail systems, including VA's, are vulnerable to virus attacks. In fact, most computer viruses are spread through e-mail messages.

E-mail Privacy and Security (cont'd)

- Virus-scanning software scans all e-mails and attachments sent to you.
- Don't open attachments from people you don't know.
- Use e-mail in an appropriate manner. Don't forward or create hoaxes or ask people to modify their computer systems. Don't spread rumors using e-mail. Be suspicious of any message that tells you to forward it to others.
- **Use "reply to all" sparingly.** Does everyone in your large mail group really need to see your response? Often, it is more appropriate to limit your response to just the sender.

For more information about E-mail etiquette, see http://vaww.vaco.va.gov/goodinfo/mailetiquette.htm

Viruses

Computer viruses can be one of the biggest causes of business loss at VA and the data we depend on to fulfill our mission can compromised by a virus.

Take an active role in virus defense:

- When anti-virus programs are loading, let them run to completion.
- Be suspicious of e-mail messages from people you do not know as well as of unexpected messages from people you do know.
- Look for suspicious activity, like a constantly active hard drive.
- Make sure data files and programs you load on your computer are authorized and free from viruses.

Viruses

Improvements in technology have permitted VA to institute an anti-virus defense program.

Often, anti-virus software is automatically installed and updated. Nonetheless, new viruses are an everyday occurrence, and anti-virus software offers no protection from newly developed, unknown viruses.

Viruses can be spread from inside as well as from outside VA. Viruses can be contracted through a variety of access points on your computer, from a software diskette, a CD-ROM, DVD, removable storage medium (zip drives, etc.) or e-mail.

Worms and Trojan Horses

Worms and Trojan Horses - software specifically designed to damage, corrupt, and disrupt a computer or network system - are collectively known as malicious software, or "malware."

A virus is a software program loaded onto your computer and executed without your knowledge.

One type of virus is called a worm. A worm is a simple virus that can make a copy of itself over and over again is relatively easy to produce. It can be dangerous because it quickly uses all the available memory of your system and bring it to a halt. Some viruses are capable of transmitting themselves across the network and bypassing VA protections to infect system after system within the VA.

Worms and Trojan Horses

Another type of virus is called a "Trojan Horse." These destructive programs masquerade as benign applications. They carry destructive viruses and introduce them into your computer or network. One of the most insidious types of Trojan Horse programs is one that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Malicious e-mail hoaxes are not viruses, but they are also potentially dangerous. In most cases, the sender asks you to forward a warning message "to everyone you know." The hoax may request the recipient to take corrective action, which instead, disables your system.

Public peer-to-peer File Sharing

Public peer-to-peer (“P2P”) file sharing refers to programs that allow anonymous sharing of files between computers. While there can be legitimate uses for P2P, more often these programs promote violations of copyright laws through exchange and distribution of music, videos, and games.

Public P2P programs may include viruses and "spyware". Spyware programs track and send information about you and your computer to thieves and hackers.

VA Memorandum "Prohibition on the Use of Public Peer-To-Peer File Sharing Programs " (http://vaww.ocis.va.gov) establishes policies that forbid loading, installing, or using public peer to peer programs.

Use of VA computing resources for public P2P file sharing violates VA Directive 6001 "Limited Personal Use of Office Equipment".

Symptoms

If your computer has any of these symptoms, there may be a problem. Please call the Help desk (x4357) immediately if you have reason to believe your computer has been infected with a virus.

- reacts slower than usual.
- stops running for no apparent reason.
- fails to boot.
- seems to be missing important files.
- prevents you from saving your work.

In VA, all computers are required to have virus protection software. New updates are usually issued every week. While many sites automatically update virus protection software on networked computers, remember that non-networked computers, particularly VA issued laptops, will not receive automatic updates to virus protection software.

Virus Protection

Protect yourself:

- Delete e-mail messages with unusual subject lines, for example, "Open this immediately."
- Never stop or disable your anti-virus program.
- Always allow an anti-virus program to perform its routines without interruption.
- Back up your files on a regular schedule.
- Have your virus protection software set to scan your e-mails and attachments.
- Be cautious and sensitive to attachments that have file extensions that execute system commands or applications. For example: .exe, .vbs, .js, .jse, .wsf, .vbe and .wsh.
- Unless you can verify, do not delete any system files based on a request made on e-mail.

Reporting Computer-Related Incidents

Take a few moments to consider how important VA's computers are in conducting our business. It is important to let your supervisor and Information Security Officer (ISO) know when you witness computer-related incidents, such as:

- Electronic viruses
- Stolen and vandalized computers.
- Use of computers to distribute sensitive information to those not authorized to receive it.

Reporting cyber security incidents helps VA to reduce the negative impact of these events and to improve VA's information processing ability.

Incident Do’s and Don’ts

When you think a computer security incident may have occurred, you should:

- Gather details of the incident so you can communicate specific information to your ISO.
- Collect the date, time, location, and involved computer systems.
- Describe what you believe happened.
- Copy any error messages displayed on your screen.
- Copy any involved web addresses, server names, or IP addresses.
- Time may be of the essence. Don't wait to call your ISO.
- E-mail may not be the best way to report the incident. You may need to contact your ISO by phone or in person.

Incident Do’s and Don’ts

When you think a computer security incident may have occurred, you should:

- Limit discussion of the incident to only those with a specific need to know.
- Do not discuss the incident with the media (radio, TV, newspapers) or anyone outside of your facility without first consulting your ISO and facility management.

Risk Awareness

The key to effective incident prevention lies in your ability to establish the context of the request and to clearly establish where you are within the task you are conducting at the time. This will ensure you know whether it is appropriate to accept the modification of a computer setting or that a file should be deleted.

VA Cyber Security: Part of Infrastructure Protection

As a VA employee, you must be aware that the Department’s information systems are part of America’s strategic infrastructure. We are expected to maintain our ability to provide veteran services even in times of national tension. VA's information systems not only enable us to provide efficient services to America's veterans, they also enable VA to work with other agencies, including the Departments of Defense (DoD), Health and Human Services (HHS), and Homeland Security. In addition to our primary mission of serving veterans, VA has a role in responding to a variety of regional and national emergencies.

VA Cyber Security: Part of Infrastructure Protection

The FBI has warned all Federal agencies that their systems and the information in those systems are potential targets for an ever-increasing number of cyber attacks. Now more than ever, the VA's systems and the information they contain must be available to serve our nation and its veterans. Please be alert to anything that might compromise VA's cyber security. Immediately report any incidents to your Information Security Officer. If your ISO is unavailable, contact VA SOC at 1-877-279-8856.

Contact your facility Information Security Officer (ISO) if you have questions about cyber security issues. For general information about VA's Cyber Security program, go to vaww.infosec.va.gov.

Risk Awareness

The nature of work at the VA and its close involvement with the Strategic Infrastructure program may increase the likelihood and diversity of attacks on its information and systems. This heightened risk makes it more important for VA staff to know their jobs better to correctly decide appropriate procedures and courses of action to take in the event of unusual activity.

Social Engineering

Social engineering is an unauthorized person's manipulation of your trust to get you to give up information or resources that you should not give out. This is an important information security issue!

Make sure when you are asked by someone to provide information or allow the use of your computer or accounts (in person, over the phone, or electronically), that you are certain of who they are and of their authorization to have/use that information or access as part of their job.

Unauthorized disclosure of information or granting of resources to dishonest social engineers are potentially bigger threats to you and VA than most computer hackers.

Risk Awareness

As a result of improvements in system security, hackers generally require more information from different sources in order to compromise modern systems.

This progress in risk mitigations systems and techniques has created a rise in the number and sophistication of the social engineering techniques employed by hackers.

Social engineers will rarely ask for secure or confidential information directly and instead will gradually gain your confidence, often asking for nothing the first call in favor of building up confidence for a later time.

This means that your diligence is critically important and, in some cases, constitutes the last line of defense.

Authorized Use

As a VA employee, you may have the privilege of some "Limited Personal Use" of certain government resources, such as computers, e-mail, Internet access, and telephone/fax service.

This benefit is available only as long as it does not interfere with official VA business, is performed on the employee's non-work time, involves minimal additional expense to the Government, and is legal and ethical.

Remember that your personal use may be limited at any time either by your management or by those responsible for the particular government resource you want to use. Before using this privilege, you should discuss your limits and responsibilities in using it with your supervisor and Information Security Officer (ISO).

Ethics

Ethics deals with placing a "**value**" on acts according to whether they are "**good**" or "**bad.**" Every society has its rules about whether certain acts are ethical or not. The same thing is true when using a VA computer system to access confidential information.

"Ethics is about understanding how your actions affect other people, knowing what is right and wrong, and taking personal responsibility for your actions..."

- Winn Schwartau

Misuse or Inappropriate Use

- Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, continuous data streams, video, sound, or other large file attachments that degrade performance of VA's network.
- Using VA systems as a staging ground or platform to gain unauthorized access to other systems.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

Misuse or Inappropriate Use

- The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.
- The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any illegal activities or activities otherwise prohibited.
- Use for commercial purposes or in support of "for profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).
- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

Misuse or Inappropriate Use

- Posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a VA employee (unless appropriate approval has been obtained), or uses that are at odds with the agency's mission or positions.
- Any use that could generate more than minimal additional expense to the government.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information; copyrighted, trademarked, or material with other intellectual property rights beyond fair use; proprietary data; or export-controlled software or data.

Risk Awareness

Even though every reasonable precaution is taken to protect users and systems in both usage modes, it is always better to keep personal use of systems to a minimum, thus reducing the likelihood of any vulnerability being exploited and resulting in the system being compromised.

If business systems are used for personal purposes it may increase the risk these systems have to bear.

Congratulations !

You have successfully completed the VA Cyber Security Awareness Course. To receive credit for this training activity, you must complete the test (10 questions).

One hour of educational credit will be automatically recorded for you in SynQuest if you complete the following procedures and successfully pass the test:

1) Press the “enter” key twice at the end of this Power Point. This brings you back to the SynQuest box.

2) Click in the grey box that reads: “After you have finished the course, click here to continue.” Then check “yes” to the question on your screen: “Did you complete the course.”

3) Answer “yes” to the next question: “The course has a test, would you like to take the test now?” Another message will appear that reads: “Sorry, you have to complete the course first”; click OK. Be sure the Cyber Security Awareness Training course is highlighted in the Computer Assignment screen that now appears.

4) If the test does not automatically launch, select the “take the test” button on the right of the Computer Assignment screen. The first question on the test will now appear.