DBHDS

Information Technology Security Awareness

Our Environment

- DBHDS employees deal with various types of sensitive data on a daily basis.
- Employee information, patient data, financial records - either in electronic format or printed documents.
- This data is critical to the department and its mission.
- To ensure safekeeping of this data, employees need to be aware of and practice some basic security skills.

Awareness is the Key

- Be aware of and secure your equipment.
- Be aware of your surroundings, especially when working out of the office or traveling.
- Be aware of strangers in your work area, question people who don’t have their badge displayed or those you don’t recognize.
- Be aware of the data you access making sure to secure any output.
- Be aware of your email - what you open, what you send and who you send it to.
- Be aware of your internet activity, what sites you access (are they secure) and what information you share.

Equipment Awareness

- Be sure to secure your system by pressing the Ctrl-Alt-Del keys to lock your computer when you leave for lunch or are away from your desk.
- Never share your password with anyone. If you suspect that your account has been compromised contact your Facility Information Security Officer (FISO) or the agency Information Security Office (ISO).
- Portable device users must always be aware of where their device is, especially when traveling.
- No personally owned USB storage device (external hard drive, thumb drive, PDA, etc.) can be connected to a COV owned computing device without an exception being approved by the agency ISO and COV Security.

Environment Awareness

- Portable device theft happens. As a user your job is to minimize the chance of that happening to you.
- When traveling never check your device as baggage, always take it as a carry on. The best practice is to carry it with you at all times. Never lock it in the car.
- Be aware of the people around you when you are accessing your laptop in public. Shoulder surfing can compromise sensitive information.
- Any questions can be directed to your FISO or the agency ISO.

Environment Awareness
VITA/NG Remote Control

- VITA/NG has installed remote control software called Carbon Copy (CC) on your computer in order to improve the VITA Service Desk's ability to quickly identify and resolve standard PC problems. The new software will allow technicians to remotely connect to your computer (with your permission) and often resolve basic PC problems over the phone so that you don't have to wait for a desk-side visit.

Environment Awareness
VITA/NG Remote Control

How does a remote control connection work?

- When you call the VITA Service Desk (1-866-637-8482), the technician on the phone will first determine if your particular issue can be resolved using a remote control connection.
- The technician will then ask for permission to access your computer and advise you to close any sensitive documents.
- You will be guided through a few simple commands to verify your IP address and get your permission to connect remotely.
- You will approve the remote control connection by clicking yes to the Carbon Copy request (shown to the right).
- The technician will be able to see your desktop and use your cursor to access software and scripts to resolve the incident.
- You will see everything the technician is doing and can choose to end the session at any time.

Environment Awareness
VITA/NG Remote Control

Who can remotely access my machine?

- All remote control connections require customers' verbal and electronic permissions.
- Only a select number of help desk and desktop technicians have administrative rights to perform remote control connections.
- These individuals have gone through background checks and received extensive training to ensure that they understand and will uphold strict policies and procedures established for this service.

How do I disconnect from a remote control session?

- The technician will always disconnect from your machine following a remote control session.
- Customers also can formally end the session at any time by right clicking on the CC (Carbon Copy) icon in the system tray and choosing *disconnect.*

Environment Awareness
Social Engineering

- Social Engineering is the practice of obtaining confidential information by manipulation of legitimate users. The principal behind this practice is that users are the weakest link in security. The underlying principle is that it is easier to trick people into providing you information than it is to hack into computing systems. Social engineers get personal information or access to computing systems by taking advantage of people's natural tendency to want to trust strangers and be helpful.

Environment Awareness
Social Engineering

- Impersonation: Attackers typically pose as someone in authority or an IT representative in order to obtain information or direct access to systems. For targeted attacks these individuals will go through great lengths to gain as much credible information as possible so they know enough to get you to trust them.
- Dumpster diving: This is the art of going through trash to obtain valuable information. Any sensitive information (paper or electronic) that is discarded improperly is valuable to a dumpster diver.

Data Awareness

- Treat all data as if it were sensitive and protect it as if it contained your own private information.
- Do not store sensitive information on portable devices or desktops unless the device or data is encrypted.
- Secure all sensitive documents when you are not using them.
- Shred all sensitive documents when you are done with them.

Email Awareness

- Pay close attention to the attachments you open and who they are from. Never open web links embedded in email messages.
- Delete spam or chain email messages. Never forward, open or reply to them.
- Avoid sending large attachments in your email messages.
- DO NOT SEND Protected Health Information (PHI) or Personally Identifiable Information (PII) or any sensitive data via email UNLESS IT IS ENCRYPTED.
- Do not send password protected files as attachments, this is not considered secure.

Email Awareness High Risk Areas

- Outlook Web Access provides DBHDS employees the ability to access their work email from a non COV computer via the internet.
- When using this application you can not save any emails or attachments to the local machine.
- Please be aware of what you are doing and who is around when you use this application. The possibility of sensitive information being compromised is increased when using Outlook Web Access.
- Remember do not download attachments when using Outlook Web Access unless you are downloading them to a COV owned encrypted device. If you download to a COV encrypted device please make sure there are no residual copies of that data on the computer you are using.

Email Awareness High Risk Areas

- Spam

  Spam scams are deceptive emails designed to get people to reveal personal, financial or log-in information. You will be asked to click on links or open attachments that can infect your computer or get you to send money.
- Classic examples of spam include:
  - Phishing
  - Phony Security Alerts
  - “Nigerian” bank account scam.

Email Awareness High Risk Areas

- Phishing:
  - Phishing schemes typically involve email pretending to be from someone in authority or from trusted businesses such as Citibank or Paypal.
  - It can even appear to come from a government agency.
  - The email will ask you to click on a link to validate or confirm personal, financial, or password information or face negative consequences. The email links and websites can look legitimate, but they are really designed to steal your information.

Email Awareness High Risk Areas

- Phony Security Alerts:
  - These are usually emails or pop-up windows that claim to be from a reputable software or hardware manufacturer (Microsoft, HP, etc.) or from a trusted name like “IT Security”.
  - They will warn you that your computer is at risk of being infected or hacked and you need to click on a link that will execute a patch in order to fix the problem. That link is really malicious code that loads on your computer infecting your machine and possibly others via email and other network connections.

Email Awareness High Risk Areas

- Nigerian Bank Account Scam:
  - This highly successful email scheme looks like it comes from a VIP in another country.
  - They claim to have access to a large sum of money but need your financial assistance to access that money. They promise a large return for your small investment.
  - You are asked for your bank account information; and to transfer money so they can get the process started.
  - The goal with this scam is to collect money and to gain access to your bank account.

Email: Final Thoughts

- Suspicious email…here's what to look for:
- Attachments with suspicious or unknown file extensions (e.g.: *.exe, *.vbs, *.bin, *.com, *.pif or *.zzx) should be deleted. If you are in doubt contact your FISO or the agency ISO.
- If the subject or topic line looks suspicious don't open the email. Delete it or contact your FISO or the agency ISO.
- Sure signs of scam email:
  - It's not addressed to you by name
  - It asks for personal or financial information
  - It asks for a password
  - Do not give out personal information.
- Always remember: when in doubt either delete the message or contact your FISO or the agency ISO.

Internet Security Awareness

- Always remember the Internet is not private. Don’t take security for granted or assume that your connection is secure.
- At a minimum, look for “https” in the URL and check for the little lock that appears in the corner on most browser windows to indicate that there is a secure connection.
- Never put sensitive information in locations that are accessible from the Internet.

Reporting Security Incidents

- DI 1002-06 addresses the steps you need to take when reporting potential security violations.
- The DBHDS Computer Security Incident Report Form needs to be filled out within 24hrs of the event happening or its discovery.
- COV Security must be notified within 24hrs of the event happening or its discovery.
- Notify your immediate supervisor or manager, your FISO and the agency ISO.
- Read and understand the departments policies and instructions regarding IT security and HIPAA security.
- Lost or stolen portable computing devices (laptops, notebooks, blackberries, etc) must be reported to your FISO, agency ISO and COV security within 24hrs of discovery.

Computer Security Awareness

- Computer Security is the protection of computing systems and the data that they store or access.
- Good security allows DBHDS to provide the services needed to our community and our employees.
- It protects employee information, financial data and patient records from being compromised.

Computer Security Awareness
Who's Responsible?

- Computer Security is not just an IT problem.
- Good Security Standards follow the "90 / 10" Rule: 10% of the safeguards are technical; 90% of the safeguards rely on you to adhere to good computing practices.
- Example: The lock on the door is the 10%. You remembering to lock the lock, check to see if the door is closed, ensuring others don't prop the door open, keep control of the keys, etc. is the 90%. Both parts are needed to have effective security.

Computer Security Awareness
What Does This Mean for Me?

- Everyone who uses a computer needs to understand how to keep their computer and data secure. Information Technology Security is everyone's responsibility.
- DBHDS employees are responsible for familiarizing themselves and complying with all department IT policies, procedures and standards relating to information security.

Computer Security Awareness Objectives

- Sec-U-R-IT-y
  - Yes, you are it!
  - Learn good computing security practices.
  - Incorporate these practices into your everyday routine. Encourage others to do so as well.
  - Report it. If you become aware of a suspected security incident contact your FISO or the agency ISO.

Computer Security Awareness
Consequences for Violations?

- Risk to security and integrity of personal or sensitive confidential information.
- Loss of valuable business information.
- Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports.
- Costly reporting requirements in dealing with the compromise of certain types of personal, financial or health information.
- Internal disciplinary actions up to and including termination of employment as well as possible penalties, prosecution and the potential for sanctions / lawsuits.

Awareness Scenario #1

- Your supervisor is very busy and asks you to log into a special account using their user-id and password to retrieve some reports. What should you do?

A: It's your boss, so it's ok to do this.

B: Ignore the request and hope they forget.

C: Decline the request and remind them that it's against DBHDS policy.

Scenario #1 Answer

- Answer: C

  User ID's and passwords must not be shared. If you are pressured further, report the situation to management, your FISO or the agency ISO.

Awareness Scenario #2

- You receive an email with an attachment from “IT Security”. The email states that your computer has been infected with a virus and you need to open the attachment and follow the directions to remove the virus. What should you do?

  A: Follow the instructions ASAP.

  B: Open the attachment to see what it says.

  C: Reply to sender and say “remove me from this list”.

  D: Delete the message from the unknown source.

  E: Contact the VCCC HelpDesk or the FISO or agency ISO and ask about the email.

Scenario #2 Answer

- Answer: D or E.

Attachments can contain viruses and other malicious programs that can infect your computer. Opening or clicking on unknown attachments is very risky.

A good rule to remember is never open, reply to, or forward any suspicious email or attachments. Delete them.

Awareness Scenario #3

- A family member sends you an email at work with a screen saver they say you will love. What should you do?

  A: Download it onto your computer since it's from a trusted source.

  B: Forward the message to friends to share it.

  C: Call the HelpDesk and ask them to help you install it.

  D: Delete the message.

Scenario #3 Answer

- Answer : D

  Delete the message.

  Things to think about. Screen savers can contain malicious code.

  Email addresses can be faked. Just because the email says it's from someone you know, you can never be 100% sure.

Awareness Question

- Which workstation security safeguards are YOU responsible for following and/or protecting.

  A: User ID

  B: Password

  C: Log-off system or lock system when not in use.

  D: Lock-up office or work area when leaving.

  E: All of the above.

Awareness #4 Answer

- Answer: E

All the above.

Remember…Sec-U-R-IT-y. You are it!

Personal Use of Computer Resources

- Personal use means use that is not job-related. In general it is occasional and incidental and is prohibited if it:
  - Interferes with the user's productivity or work performance, or with any employee's productivity or work performance.
- Can adversely affect the efficient operation of DBHDS network (bandwidth consumption)
- Be sure to close any browser windows after you are done viewing the site. Do not minimize the window and keep the connection open terminate your internet connection when you are finished.
- Do not access radio stations on your work machine unless you have a legitimate business need to do so and have approval from your supervisor or manager.

Personal Use of Computer Resources

- Do not view videos on your device unless they are work related. Radio stations and video (streaming media) are the #1 cause of bandwidth consumption.
- Private or personal, for-profit activities (e.g. consulting for pay, sale of goods such as Avon or Amway products, etc.) is not allowed.
- Abuse of this privilege violates any provision of DHRM Policy 1.75 (Use of Internet and Electronic Communications Systems), agency DI 703 or policy or any other regulation law or guideline as set forth by local, State or Federal law.

Personal Use of Computer Resources

- While browsing the internet, do not go to any web site that would mask or hide your internet browsing activity. These types of sites are considered Proxy Bypass Sites and circumvent any COV or agency security measures that may be in place.
- Employees are not permitted to use COV resources to promote “for profit personal business”. Use of COV resources is permitted for “non profit” organizations so long as it does not interfere with the employees regular work and does not waste COV resources.
- If you have any questions or concerns about the web sites you have viewed or are wanting to view, contact your FISO and the agency ISO.

Final Thoughts

- Security is everyone's responsibility. Take it seriously.
- Treat confidential or sensitive information as if it were your own. Secure documents when you are not using them. Shred documents when you are finished using them.
- Do not connect personally owned external devices to COV computing equipment.
- There is no such thing as privacy on the internet.
- With email, when in doubt don't open it. Delete the message.
- Any questions contact your FISO or the agency ISO.
- If requesting remote control assistance from VITA/NG staff, make sure to close any sensitive information that is visible on your screen before allowing remote access.