Security Awareness Quiz Questions		
Category	**Question**	**Answer**
General Security	1. Why is backing up data files important?	▪ Backups ensure that the information you need is there when you need it ▪ If the information is damaged it can be recovered ▪ The business continues to operate
General Security	2. What can you do if you fall victim to identity theft?	▪ Contact the fraud department of each three credit bureaus and request a fraud alert be put on your file ▪ Contact the creditors for any accounts that have been tampered with ▪ File a report with your local police or the police in the community where the theft took place
		Be cautious – ask questions – secure your personal belongings
General Security	3. Name three general security rules you should practice for your building or office	1. Don't let anyone in if they can't get in themselves 2. Insist on seeing ID from people you don't know 3. Don't let strangers "mess" with anything even if they do have ID 4. If access into your area requires a badge, always keep the door closed 5. Employees required to wear badges should have them visible at all times 6. Escort visitors to departments. Don't let them wander around 7. Revoke access immediately when an employee or contractor is terminated or leaves for any reason 8. Follow your defined process for informing all necessary areas when an employee leaves 9. Don't leave data at printers, fax and other
General Security	4. What should you do if you see a stranger walking in the halls of your building?	▪ Always escort visitors. Have them wait in lobby for you and escort them back when your business is completed. ▪ Politely ask any stranger, "May I help you?" ▪ Encourage "sign in and out" and retturn of visitor badge ▪ Notify visitors of applicable security information (emergency exits etc.)
General Security	5. What is a Social Engineer?	• Social Engineer is a con artist – a person that will talk people into revealing passwords or information that will compromise the company security

Passwords	1. What is one of the ways that you can secure your password from disclosure	1. You can memorize it 2. You can write it down only if you keep it in a secure place like your wallet without header information. Password should "NOT" be kept in a computer file
Passwords	2. When constructing a password you should: a. You should use your family member name, sports name, pet name and add a number on the end b. Use phrases or misspelled words with embedded numbers and special characters c. Use sequenced letters and numbers from your keyboard d. All of the above	The answer is "b" You should use phrases or misspelled words with embedded numbers and special characters •Throw in digits and/or symbols here and there. Passwords that are like license plates,-alpha-numeric, are more effective (M3RC;76LT) •Numbers or unique characters are best interspersed in the middle rather than the end •Make new passwords that are not identical or substantially similar to ones you've previously used. Strike a balance between production - easy for you to remember -and protection - difficult for anyone to guess.
Passwords	3. How are passwords like bubble gum	▪ Passwords are strongest when fresh, they should be used by an individual (not a group) ▪ If you leave your passwords laying around, there's a good chance you'll soon have a **sticky mess**
Passwords	4. What should you do if someone asks you for your password	▪ Say NO ▪ Ask questions if it is a company technical support person – you may be able to type the password in yourself. If not change your password immediately at the conclusion of the work ▪ If it is someone outside your company – say NO and report the event as an incident
Passwords	5. What is an example of a strong password	▪ Use made-up words meaningless combinations you can remember: to2win+do ▪ Combine unrelated words: no!cand0 salt2try $outh&hart ▪ Employ themes – exact titles should be avoided Movies – gone-with-the-breeze Song lyrics – 75&trombones Books – 2killehummingbird ▪ Use misspelled words Business = Biz!ne2z Pattern = Pa#r1n Garbage = G*rbea8$e ▪

Security Smorgasbord	1. What are the three necessary components to develop positive security habits	1. Knowledge (what to do) 2. Skill (How to do) 3. Attitude (Want to do and Why) Increase awareness ▪ Know what to look for to identifying potential issues ▪ Use sound judgment Learn and practice good security habits ▪ Make then a part of your everyday routine ▪ Encourage others to do so as well as acknowledge those that are practicing them Report potential and actual security breaches
Security Smorgasbord	2. What are your responsibilities for the protection of company assets a. Assist with the protection and proper use of information assets b. Know the processes to protect information assets c. Build proper security practices into your day d. All of the above	The answer is "d" all of the above Remember when it comes to SEC-U-R-I-TY you are it This company needs your help in protecting company assets and to do that you must know and practice the appropriate processes.
Security Smorgasbord	3. Is it legal to copy software from your PC to your laptop or home PC?	The END USER LICENSE AGREEMENT will specify whether you are able to. If the EULA does not contain this clause, then you cannot make a second copy
Security Smorgasbord	4. What are some of the things that you have seen or heard which make being more aware of information security important?	▪ Passwords written on a post-it note and stuck on a computer monitor ▪ Computers left on, even while logged on to critical corporate applications, though the user has left ▪ Someone sharing a password with an official-sounding stranger just to be helpful ▪ Unauthorized modems connected to outside internet connections ▪ A co-worker inadvertently passing along a virus-infected e-mail ▪ A staff member complaining about how his laptop was stolen at the airport
Security Smorgasbord	5. Sharing games or programs with your co-workers is okay as long as you don't charge them any money – True or False	The answer is "False" Information is intellectual property. Unless explicitly stated in the copyright and license terms sharing programs, and even games are NOT okay even if no money changes hands ▪ You must comply with copyright and license terms ▪ Copying programs or games can be a violation ▪ Copying information from the Internet can be a violation

Email & Internet	1. When sending or forwarding email you should make sure that it does not: a. Create a chain mail situation b. Have an attachment file c. Follow general business practices d. All of the above	The answer is "a" does not create a chain mail situation. Chain mail consumes excessive resources and interferes with work productivity. In some case chain mail can also carry viruses.
Email & Internet	2. My email is private and no one can look at it – true or false and Why?	The answer is "false" ▪ The company email system is owned by the company and they are allowed to scan your email for inappropriate use or suspected policy violations ▪ Even your personal home email is vulnerable to hackers scan information on the internet. Any email on the internet unencrypted is exposed to scan
Email & Internet	3. You are sending confidential information to a colleague across the internet. How can you protect this message from being read by individuals other than the intended recipient	You can use encryption or a password protected zip file
Email & Internet	4. Name one potential legal risk to you and the company when using the internet	1. Going to sites with offensive material can present a legal risk to you and the company 2. Duplicating or downloading copyrighted material can present a legal risk to you and the company 3. Downloading information from questionable sites can put your company at risk to hacker probes
Email & Internet	5. There is a wealth of information on the internet and many people offering to help in chat groups. It is fine to take advantage of this help as long as the sites are not forbidden or blocked by the company – True or False	The answer is "false" It is easy to think because it is a legitimate business site that it is okay to participate in chat sessions using your companies connection to the internet. However in such a situation you become a spokes person for the company and the company can be liable for anything you say that could be misinterpreted.

Be Proactive	1. Name three ways to protect your laptop computer when you carry it away from your office	1. Never leave your laptop unattended 2. Utilize a security cable or similar device and attach to a solid fixture in a conference room 3. Never check your laptop as luggage 4. Make sure your path trough the metal detector at the airport is clear 5. Don't be distracted by a decoy while an accomplice grabs your computer laptop 6. At a hotel carry your laptop to the room don't let the bellman carry it.
Be Proactive	2. How can you protect yourself and your company from social engineering?	1. DO verify the ID of anyone who claims they are from your phone company, Internet provider, or MIS department support 2. DO get to know your MIS department if you have one 3. DON'T give out passwords, dial-up modem numbers, or any information about your company's systems 4. DON'T be intimidated especially by name droppers .
Be Proactive	3. How can you protect against viruses?	▪ Make sure you have virus protection on your computer and do not disable the virus protection tool ▪ Scan for viruses whenever you download or copy a file ▪ Never open unsolicited attachments especially from an unknown source
Be Proactive	4. What would you do if you encountered a security incident: a. Contact your security team b. Tell a co-worker c. Call the local newspaper d. None of the above	The answer is "a" contact your security team or appropriate incident report team. They will know how to investigate and respond to the incident and will contact the proper authorizes and the press if necessary
Be Proactive	5. Name a way that you can be alert to suspicious activity in computer use – Heads Up Computing	•Be aware of files in your home directory. If you find one that you don't recognize, someone else may have used your account •Never leave a session on a workstation without engaging a screensaver •When you login from somewhere else, always remember to logout when done
Bonus Question	Name one of the biggest virus that impacted companies in the US.	Melissa Virus Love Letter or I Love You Virus
Bonus Question	Who or what is the weakest link in the security chain?	Human beings – helpful, polite and trying to get their own job done fall victim to social engineers often give away important company information or inadvertently help these con artist to find and exploit system vulnerabilities