Bus 230 chap 5 exam 2

ASSIGN BUSTER

Any illegal act involving a computer generally is referred to as a computer crime. TrueCombating cybercrime is NOT one of the FBI's top priorities. FalseCybercrime laws are consistent between states and countries, making it easy to reach a consensus as to what is illegal. FalseA cyberextortionist uses the Internet or network to destroy or damage computers for political reasons. Programmers often build trapdoors into programs during system development. A rootkit can be a back door. Perpetrators of back doors trick their victims into interacting with phony websites. Personal firewalls constantly monitor all transmissions to and from a computer and may inform a user of any attempted intrusion. Both Windows and Mac operating systems include firewall capabilities. Many companies use access controls to minimize the chance that a perpetrator may intentionally access or an employee may accidentally access confidential information on a computer, mobile device, or network. TrueAudit trails only record unsuccessful access attempts. FalseMost operating systems require that users correctly enter a user name and password before they can access the data, information, and programs stored on a computer, mobile device, or network. TrueIf a program or device has a default password, be sure to retain it. FalsePINs are not the same as passwords. FalseIf you are nervous, a signature might not match the one on file in a signature verification system. TrueA digital forensics examiner must have knowledge of the law, technical experience with many types of hardware and software products, superior communication skills, and the like. TrueBiometric objects are entirely foolproof. FalseTo promote a better understanding of software piracy problems and, if necessary, to take legal action, a number of major worldwide software companies formed the BSA. TrueMany organizations and businesses have strict written policies governing the installation and use of software and enforce their rules by checking networked or online computers periodically to ensure that all software is licensed properly. TrueSome operating systems and email programs allow you to encrypt the contents of files and messages that are stored on your computer. TrueSecure sites typically use digital certificates along with security protocols. TrueDigital signatures often are used to ensure that an imposter is not participating in an Internet transaction. TrueAnalog signatures help to prevent email forgery. FalsePasswords and passphrases that are more than four characters, contain uppercase and lowercase letters, numbers, and special characters are the most secure. FalseAny device that connects to the Internet is susceptible to mobile malware. TrueOne way to reduce electrical waste is for organizations to use outside air to cool data centers and computer facilities. TrueWebsites often collect data about you so that they can customize advertisements and send you personalized email messages. TrueOnline shopping sites generally use a session cookie to keep track of items in a user's shopping cart as shown in the accompanying figure. TrueUsers can purchase a software program that selectively blocks cookies like the kind shown in the accompanying figure. TrueYour browsing history is a list of all websites you have visited over a period of time. TrueDuring virtual browsing, your browser does not keep track of the websites you are visiting. FalseProximity sharing gives websites access to your current location. FalsePhishing is an unsolicited email message or newsgroup posting sent to many recipients or newsgroups at once. FalseTo remove spyware, users need to obtain a special program that can detect and delete it. TrueInformation collected and stored about individuals should be limited to what is necessary to carry out the function of the business or government agency collecting the data. TrueTo protect yourself from social engineering scams, shred all sensitive or confidential documents. True`= Many businesses use spyware to limit employees' web access. FalseCOPPA protects minors from inappropriate content when accessing the Internet in schools and libraries. FalseThe Computer Abuse Amendments Act outlaws transmission of harmful computer code such as viruses like the kind shown in the accompanying figure. TrueThe ECPA protects consumers from disclosure of their personal financial information and requires institutions to alert customers of information disclosure policies. FalseFOIA enables public access to most government records. TrueHIPAA protects individuals against the wrongful disclosure of their health information. TrueThe PATRIOT Act gives law enforcement the right to monitor people's activities, including web and email habits. TrueThe Privacy Act forbids federal agencies from allowing information to be used for a reason other than that for which it was collected. TrueIt is illegal for employers to use software programs that monitor employees. FalseIf a company does not have a formal email policy, it can read email messages without employee notification. TrueContent filtering opponents argue that banning any materials violates constitutional guarantees of free speech and personal rights. TrueMany Internet security programs include a firewall, antivirus program, and filtering capabilities combined. TrueCOPPA requires that schools and libraries use content filtering software in order to receive certain federal funds. False ONBUS 230 CHAP 5 EXAM 2 SPECIFICALLY FOR YOUFOR ONLY$13. 90/PAGEOrder Now