

The Home Executive's Guide to Computer Security

Book Questions

1. *Who should be concerned about home computer security?*

Everyone who connects to the Internet and doesn't want their lives disrupted. This is especially true of home businesses and people who take work home. Most people don't know that civil law can be used to hold some accountable for not securing their business information. If you haven't protected your system fully, you can be sued for revealing private facts unless it is a fact of public concern or public record, releasing of medical / financial information and the like that used to be confidential, not protecting the integrity of some data that may have been modified and can be viewed as defaming an individual in the course of releasing said information, or for any pictures of people stored on your system that are released improperly.

2. *Why is information security important?*

Information is valuable to all of us including businesses, governments, and criminals. Nowadays, the global telecommunication infrastructure allows near instant access to voice and data from nearly anywhere to nearly everywhere. Governmental and business databases continue to grow containing all aspects of our lives. Every major sector of the economy relies heavily on computer systems to be competitive globally. With over 500 million computers in use world-wide, and over 145 million Internet hosts world-wide with over 8 trillion web pages, it doesn't take long to see that we open ourselves up to everyone using the same systems we are using. Issues such as identity theft, stalking, surveillance and other privacy issues are but the tip of the iceberg. Information is power, and as such, can be used to both make our lives easier and a living hell.

3. *What are the most common attacks on computer systems?*

According to the CSI / FBI 2003 Computer Crime and Security Survey, it was reported that cyber attacks occurred by Viruses (82%), unauthorized access by insiders (45%), Denial of Service (42%), system penetrations (36%), sabotage (21%), telecom eavesdropping (6%), and active wiretapping (1%) of all participants. These percentages are based on 530 respondents in a diverse set of key industry sectors such as local, state, federal governments, transportation, telecom, utilities, medical, financial, legal, education, retail, manufacturing, and high-tech. These attacks occurred despite the fact that most of the respondents had security policies and mechanisms in place as part of their prevention and response plans. Just imagine the number of successful attacks that went unnoticed and/or unreported, and by entities that were not even part of the survey.

4. *In plain English, what are the foundational concepts of information security?*

There are 7 basic concepts: confidentiality, integrity, availability, authentication, access control, accountability, and non-repudiation. Confidentiality is about encrypting data and communications. Integrity is preventing the unauthorized changing of data and communications. Availability is making data or information available to authorized users or systems. Authentication is the confirmation of an authorized user or system's credentials. Access Control is just that, controlling the access to resources of an authorized user or system. Accountability is being made answerable for an activity. Non-repudiation is the ability to provide non-refutable evidence that an activity took place and by whom/what. For a system to truly be secured, it requires all seven.

5. *What can we do to secure our home computers?*

There are a number of things that must be considered. The physical location and protective mechanisms of the computer itself, Browser Security, Anti-Virus programs, Firewalls, E-mail Practices and Encryption, Remote Software Security, Staying Backed Up & Updated, Multiple Accounts with limited permissions and child proofing, Wireless Security, Encrypting Stored Data, and staying away from Shareware & Freeware are the primary items that need to be addressed. All of these and more are discussed in my book in simple, easy to understand language.

6. *In the book, you discuss child-proofing a computer. Why is this important?*

Children, and immature adults, have shown a consistent tendency to explore places in cyber space that can create security vulnerabilities in computers. I remember a friend of mine that applied for a job with the local police. She went to the interview only to find out that the interviewing officer had a serious, direct question. Why was she participating in occult activities on the web. In reality, it was her younger sister who had regularly visited several occult sites and chat forums. There really isn't an easy means to distinguish between users of the same computer. In addition, children may inadvertently accept infected pictures, be solicited with malicious coded e-mails, or download games that are Trojan horses. These activities can compromise a computer's security and embarrass the real owner. Lastly, I think some content is just plain unacceptable with or without parental supervision, and the child protection software on the market today does a pretty good job of eliminating this exposure.

7. *How safe is online banking?*

Online banking is now available for most accounts free of charge. It reduces the number of tellers a bank needs, and speeds the paying of bills and funds transfers. Anyone with Internet access can enter a user name and password, and have nearly complete access to all the funds in an account. There's just one small problem. Unlike credit cards, when someone gets into your account by a *VARIETY* of means, the money is gone and the bank is not liable in most cases.