

Information Security 101: What Employees Should Know

How does employee knowledge impact the security of an organization's electronic information? One answer can be found in the Symantec Internet Security Threat Report, a 2003 publication by Symantec, a leading provider of information security services. Covering more than 400 companies in ten countries, the 2002 report reveals that "greater than 50% of all incidents to which Symantec responded involved abuse or misuse of company resources by employees. In addition, the amount of self-reported financial damage in these cases was significantly greater than that caused by external breaches."*

While the employee knowledge gap is proving to be a significant and expensive risk in today's business environment, the question remains, "What should employees know about information security?" Few employees want to spend time doing research to learn about information security.

Fortunately, basic information security knowledge can be summed up in a concise format, as shown by the security awareness reference booklet developed by the Information Technology Association of America (ITAA). (For more about the ITAA Program, see the feature article in the April, 2002 issue at www.brainbench.com/business.) Below is an overview of major information security subjects as covered in the ITAA certification test and educational handbook.

What Every Employee Should Know About Information Security

The ITAA Information Security Awareness Certification handbook simplifies the complex world of information security into actionable topics that most users can understand, regardless of technical background.

Computer Security—Logging off networks. Shutting down computers. Backing up information. These are all practices that are often taken for granted.

Internet Security—Using email. Accessing the Internet. Sending sensitive information. Handling cookies, firewalls, and attachments. Employee knowledge can dramatically decrease the risks posed by Internet access.

Passwords—What is a good password? Should passwords be changed, written down, or shared? Password-related best practices are very basic, but frequently ignored.

Viruses and Other Harmful Software—The threat of the virus is well known. And while company systems may be well protected, viruses are on the increase. Awareness is the key to preventing their spread.

Computer Ethics and Misuse—How can an employee recognize an attack or simple computer misuse? What should he or she do about it? Employees should know their roles and the role of their network administrators.

Physical Security—Who has physical access to the computers on your system or your electronic files? What can they find? A locked door is as important as an effective firewall.

Sensitive Information—What kind of personal information should employees keep to themselves? How can they protect that information? Everyday tasks present opportunities for accidentally giving away key information.

ID & Data Information Theft—The urge to be helpful is natural, but where should employees draw the line? By knowing the answer, employees can easily avoid the costly ramifications of data theft.

* From The Symantec Internet Security Threat Report, VIII, February 2003. p. 26
Available at <http://www.securitystats.com/reports.asp>