Identity-Related Misuse

Perhaps you lead an honest life and have nothing to hide. Does an invasion of privacy seem more or less irrelevant to you? Maybe you want to publicize everything you do on your Web page, and don’t care about security? The World-Wide Web can make information instantaneously accessible globally.

Unfortunately, there are also some social and technological risks to your personal well-being and integrity. One is that of computer-aided identity fraud and its extreme form—identity theft. Identity-related misuse can range from a one-time event to someone acting pervasively as a doppelgänger—taking on the identity of the victim for malevolent purposes. Although computer access is not essential for such activities, remote, global, and possibly anonymous access can greatly increase the risks. The infrastructure is inherently weak with respect to system and network security, Web site integrity, personal authentication, and accountability. Although it may not seem to be a serious problem yet, identity-related misuse has been increasing in the past few years, and has the potential to escalate dramatically unless checked.

Identity and authentication of Web site users. Whenever misuse is a potential problem, the absence of strong user authentication throughout most of the Internet makes it very difficult to ascertain a perpetrator’s true identity. It is relatively easy for one user at one site to masquerade as another user at another site. Of course, even if some sort of strong authentication were to be invoked, most Web sites do not enforce any differential access controls—once you are there, you typically have implicit permission to access everything that is accessible to any other Web browser.

Inference, aggregation, and secondary use. A serious risk arises in databases containing individuals’ identities and personal information that can be used for purposes other than those for which it was intended. Also, an individual’s information in different databases can be easily combined to provide detailed dossiers that may be detrimentally misused, either via further computer manipulation or by “social engineering” (the manipulation of people using partial knowledge and clever subterfuges). Collections of information may be more sensitive than the individual data items.

Identity-related misuse. Theft of one’s identity is a risky form of malicious masquerading. For example, knowledge of your social security number (SSN) and mother’s maiden name may be sufficient for someone else to dishonestly manipulate your financial accounts and to obtain credit in your name—with or without computers. There have been numerous cases of doppelgängers, sometimes very painful. Victims include Terry Dean Rogan, Richard Sklar, and Teresa Stover, noted in our January 1992 column. Since then, the RISKS newsgroup has reported similar cases involving the identities of Clinton Rumrill and Charles Crompton (RISKS 18, 91), Kathryn Rambo and Caryl Fuller (RISKS 19, 05). Rambo’s doppelgänger acquired a $35,000 sports utility vehicle, a $3,000 loan, new credit-card accounts, and a rented apartment in her name. In other cases, life savings and all social security benefits have been lost. These names may mean little to you today. On the other hand, if this ever happens to you, your life may be permanently altered, and efforts to regain your credit rating, your livelihood, and indeed your mental stability may be very difficult.

A recent article by Simson Garfinkel, “Social Insecurity: Few Key Bits of Info Open Social Security Records” (USA Today, Apr. 7, 1997 and RISKS 19, 07), describes the Social Security Administration’s Personal Earnings and Benefit Estimate Statement (PEBES) system, a Web site developed and maintained by the SSA. Because of widespread complaints relating to the potentials for serious misuse, including identity theft, PEBES has been removed from the Internet to permit study of some of the implications. See my statement on this subject for an SSA panel (www.csl.sri.com/neumann/ssaforum.html).

System and data integrity risks. A different kind of risk to individuals and organizations arises when information is maliciously altered (or even unintentionally corrupted). In various cases, serious harm has resulted from incorrect data. Also, Web site penetrations have resulted in the insertion of bogus Web pages for the CIA, NASA, the Justice Department, the Air Force, and even the National Collegiate Athletic Association. However, subtle changes less immediately obvious can be much more insidious—for example, implanted Trojan horses that trap users into yielding passwords and other sensitive information.

In general, many people seem oblivious to these risks; I hope regular readers of this column are exceptions. Risks involving your identity should be particularly important to you. Identity-related misuse represents a significant threat to the fabric of our existence. Greater awareness as well as technological, social, and legal approaches are needed to minimize the risks.

CALPIRG (watchdog@pirg.org) has a new guide, What Can Consumers Do to Avoid Becoming Theft-of-Identity Victims?