A Few Thoughts on Safety From Your Security Committee

Security Tip #20: Safeguarding Personal Information

Critically important in maintaining a safety-conscious lifestyle is limiting the availability of your personal information, such as home address, social security number, date of birth, and identification of family members. This precaution applies not only to you, but your family and other friends with whom you may be closely associated. In today's world, the most common source of such information is the Internet—making your personal identifiers literally at the fingertips of a potential assailant or antagonist.

Your Security Committee has frequently reminded you to exercise caution in revealing personal identifiers on the Internet or to inquiring merchants. Stores frequently attempt to solicit your name, address, phone number, and email address. Contrary to their representations, this information is often sold to an information integrator or broker and is destined for commercial distribution.

The United States Marshals Service (USMS) reports that in many instances those who seek to cause harm to members of the judiciary or other protectees obtain personal information about their targets from Internet sources. The USMS recommends the following precautions:

1. Know your Internet footprint—you may wish to use simple search engines and information broker websites such as Google, PeopleFinders.com, or Spokeo.com, to determine what information is available about you or your family.

2. Take steps to remove it—truepeoplesearch.com is a website that purports to search the entire Web for information concerning the name entered. Once identified, delete it.

3. Avoid providing or verifying information to surveys, merchants, newsletters, or marketing promotions. When necessary, provide your business address and phone number.

4. Be sure to install and periodically update antivirus software.

5. Use strong, creative passwords—the longer the better—with multiple character types (upper case, lower case, numbers, and symbols), and words and phrases not commonly found in the dictionary.

6. Periodically check your privacy settings, especially on social media sites and mobile applications.

7. Judges should also avoid any form of personal presence on social media, and encourage their family to do so as well. That includes postings of photos of a judge, even within a family setting, on a social media site. Available face recognition software enables a user to search the entire

Internet for any entry that contains a particular image, such as a judge's face. This facilitates potential access to other related social media sites containing personal and family information.

Computer hackers and information pirates are typically bright and innovative. Staying one step ahead can be a constant challenge. These simple precautions are a good start.

If you have additional questions or need advice related to safeguarding your information online, you can always contact your local USMS office or email usms.ncjs@usdoj.gov.

Security Committee
Federal Judges Association

Produced in association with the United States Marshals Service's
National Center for Judicial Security