Tips to Prevent Online Identity Theft

Although "dumpster diving" is still a big problem, thousands of identity theft cases originate online. Malware scanning helps, yet sometimes it is the information you post online that makes fraud easier for an identity thief and puts you at risk. It's important to take preventative measures online, too.

- **Press the log out button when you're finished** with accounts on websites like Facebook or Twitter. Even if you've closed the window, certain websites may keep you logged in.

  Tip: The "log out" or "sign out" link is sometimes hard to find, but it's usually in the top right (or upper left) and always worth the effort.

- **Do you have a cellphone or tablet?** Take advantage of your phone's lock and privacy settings. If you lose your phone, the lock feature will provides an initial level of protection for your personal information.

- **Don't publish personal information in social media.** Could any information in your profile be used to answer a security question? According to a study by Javelin Strategy and Research, 68% of people with public social media profiles shared their birthday information--and 45% shared the year, too.

- **Consider using a "false" answer that you would know.** For example, you might use "orange" as your first pet's name, even if it was really "Fido."

For more information on how you can protect yourself and your household from identity theft, visit www.SecurityFirstFlorida.com/idtheft

Phishing & E-mail Scams

One of the sneakiest tricks used by identity thieves is called *phishing.* Phishing scams are used by cyber criminals to trick the user into entering their personal information (or the user name and password) into a fake web page designed to look like the real one, which is known as *spoofing*.

Do not click links in an e-mail unless you are absolutely certain the source can be trusted. Remember, these e-mails can be very tricky to distinguish from the real thing.

- Use caution if the message contained urgent language suggesting you take immediate action.
- If the e-mail contains threats to close your account, or if it contains multiple grammatical and spelling errors, there's a very good chance that the source is illicit.
- Remember, e-mails alerting you to "act now" on a security risk are sometimes the e-mails containing security risks. If you're concerned about the content of the message, it's better to contact the referenced company directly or visit the website by typing in the trusted ".com" URL yourself.

Password Security

There is no substitute for a quality password. When creating a password, follow these simple security steps:

- **Password should never be only 6 characters in length**.
- **Passwords should not contain only lowercase letters.**
- **Add symbols.** Keyboard characters such as #,!,$,%,& provide significant security. Whereas "spooky" is instantly cracked, an adjustment like "Thats$p00ky!" could take years to break.
- **Add numbers.** Ideally your password contains at least one number—and not just at the beginning or the end.
- **Don't use an actual word.** At 4 billion calculations per second, computers detect dictionary words quickly.
- **Use a different password for different websites.**
- **Avoid common passwords.** Following the above tips isn't enough if your "trick" is common. *QWERTY*, and its lowercase counterpart *qwerty*, is one of the most used passwords. So is 1234567.