

What Your Facebook Profile May Be Telling ID Thieves

by Jennifer Waters

Monday, January 10, 2011 MarketWatch

Seemingly harmless information can help ID thieves unlock key to your identity.

Your pet's name is a fraudster's best friend.

You may think you're revealing precious little when you tell your Facebook friends that you're dressing your pooch, Puddles, in your favorite color, red, for brunch at Grandma's on Sunday. But you've actually just opened a Pandora's box of risks.

[\[See Things to Stop Doing Now on Facebook\]](#)

The information consumers willingly, and often unwittingly, post on social-media websites can be a gold mine for fraudsters looking to steal everything from your flat-screen TV to your identity.

What's more, tidbits like your birth date, birthplace and the last school you attended are typically the challenge questions posed by bank websites and online retailers to verify your identity.

"Despite all the awareness that people have about identity fraud and privacy on social networks, there is a disconnect between [that and what they are] disclosing in online space and social environments," said Thomas Oscherwitz, chief privacy officer for ID Analytics, a San Diego-based consumer risk management firm.

More than 24 million Americans 18 years old and older are still leaving their social-network profiles mostly public, meaning they aren't activating privacy controls that limit who can see their information online, according to a Harris Interactive survey conducted in October for ID Analytics.

The survey also found that nearly 70 million U.S. adults on social-networking sites include their birthplace — one of the most common security questions asked by financial institutions — on their profiles.

"The information people are disclosing is not the entire piece of the puzzle but it's certainly helpful," Oscherwitz said. Thieves steal identities in pieces, he said, and layer them on each other for a clearer picture.

[\[See Stolen: True Tales of Identity Theft\]](#)

Say you post on a social-media site that you're at a tanning salon ahead of your week-long trip to the Bahamas the day after your birthday. You're telling potential burglars that not only are you away from home for an hour or so, but beginning Tuesday, your home likely will be empty for seven days.

"Even listing daily activities can let strangers know your routine and put you at risk," said Gail Cunningham, spokeswoman for the National Foundation of Credit Counseling.

Too much information can hurt you in other ways. John Sileo, a Denver-based identify-theft expert, said your online chatter could equip an ex-spouse with ammunition for a court challenge. Future or current employers could have a problem with information about your personal life that they deem inappropriate for a member of their staff, he said.

You also could be furnishing a would-be stalker with information about your whereabouts. "We are giving people the little pieces of our trust or access to our trust that allows them to get bigger things out of us," said Sileo, founder of the ThinkLikeaSpy.com newsletter.

[\[See 6 Things You Should Never Reveal on Facebook\]](#)

Tips to Stay Safe

Here's some advice from Sileo, who wrote the "Facebook Safety Survival Guide," about protecting online privacy on all social-networking sites:

- Never post your exact date and place of birth. It's invaluable information to identity thieves, particularly when the two are bundled together.

- Never post your address, phone number or email address. This is plum information to scammers and marketers who are looking for nuggets of your identity.
- Control who can see your personal information. Many social-networking sites have privacy features, but they change often. Know what they are, stay on top of them and restrict your page to your real friends, not friends of friends or someone you met in a bar.
- Limit information about your activities. If you must brag about a trip or a fabulous party, do it after the fact.
- Remember that what you post is public and permanent. Don't put up embarrassing photos that you wouldn't show your grandmother. Don't complain about your job or your boss. Don't say something to or about someone that you wouldn't say to his face. Don't threaten others.
- Know the four types of Facebook users: friends, outsiders, businesses and enemies.
- You should know exactly who wants to be your friend or is asking you to link into their network. Some people will befriend your friends to get to you or your company.
- Be wary of seemingly harmless quizzes. When someone invites you to take a survey, say, "10 Things Others Don't Know About You" or "My Favorite Things," it may be designed to harvest your data. The name of the street you grew up on or your favorite vacation spot could be clues to your passwords.
- Before you share any information anywhere online about yourself or your workplace, ask this question: What would the consequences be if this information fell into the hands of my boss, competitor or people who don't like me?

Jennifer Waters is a MarketWatch reporter, based in Chicago.