

AARPBulletintoday

Scam Alert: Protecting Your SSN

How to keep scammers from decoding your Social Security number

By: [Sid Kirchheimer](#) | Source: AARP Bulletin Today | October 12, 2009

Proud of your hometown? Keep it to yourself when you visit social networking websites and fill out surveys and questionnaires, if you want an extra level of protection against identity theft.

Along with your birth date, your place of birth may help scammers guess most, if not all, of the nine digits of your Social Security number, suggests a [recent study published in the *Proceedings of the National Academy of Sciences*](#).

Those two pieces of information were all that Carnegie Mellon University researchers needed to discover patterns in how SSNs are issued, resulting in impressive success in guessing exact numbers.

SSNs are commonly used as identifiers by banks, credit card companies and other financial institutions, as well as in many health and government records.

As Scam Alert has long warned, a scammer who knows your name, current address and birth date can buy your SSN from any of a dozen websites that sell them for about \$50 to private investigators, businesses conducting credit checks and others. Although in recent years these websites have required additional proof that the numbers are being sought for legitimate purposes, savvy scammers can still get them.

Birth dates easy to find

It's easy to find someone's birth date, says the study's lead researcher, Alessandro Acquisti, an associate professor of information technology and public policy. "There are many websites and databases where one can access the birth dates of thousands of

people easily and cheaply," he says. Voter registration lists and other public databases also include such information.

It takes more legwork for scammers to learn the hometown of an intended victim. But if they find it, guessing a SSN is much easier.

The reason: The first three digits of the SSN are an "area number," issued according to the ZIP code of the mailing address provided on a Social Security application form. High population states have many area numbers—New York has 85, for example—but Delaware and Alaska have only one, notes Acquisti.

The fourth and fifth digits of the SSN are a location-based "group number"; those digits change periodically, usually in increments of 2. For instance, Acquisti explained to Scam Alert, for people born in 1966 in Oregon, those middle numbers started at 47, and 60 days later, switched to 49. "Because of this, knowing a birth date and hometown makes the first five digits of a SSN the easiest digits to guess," he said.

The last four digits, the ones most often used as identifiers on accounts, are issued sequentially. But they're harder to guess because they depend on how long it took to process a Social Security application. "In some states, it takes two weeks; in others, 10 weeks or longer," Acquisti said.

The people most at risk of having their SSNs guessed are those born since 1988, when the Social Security Administration began forcing many families to order SSNs at birth.

"The good news for people age 50 and older is that it is harder to predict their SSNs because they did not necessarily receive their number at birth," notes Acquisti.

The professor said his findings stress the need to stop using Social Security numbers as passwords or unique identifiers. The Social Security Administration says the threat of guessing numbers is not significant. In a move unrelated to this study, it plans to start assigning SSNs more randomly starting next year.

Four easy safeguards

Still, at a minimum, you can help avoid potential problems:

- Don't post birth dates, hometowns or other personal identifiers such as the name and location of your high school on Facebook, MySpace. etc. [Remove such personal](#)

[information on social networks](#) if it's already posted.

- Never use a birth date or any part of your SSN as a password for online accounts. They can be stolen if you inadvertently download malware, which can happen [if you click on attachments in e-card greetings or other incoming e-mails from unknown senders](#).
- Avoid online security questions that ask for your hometown.
- Omit hometowns and other personal information in the obituaries of loved ones. [The deceased are frequent victims of identity theft.](#)

Sid Kirchheimer is the author of Scam-Proof Your Life.

[Copyright 1995–2009, AARP. All rights reserved. A Member of AARP Global Network](#)

