Millennials: Getting it Wrong About Identity Theft

Millennials have grown up on technology like personal computers, cell phones and the internet. And while they may be tech-savvy, millennials also are the most blasé about how technology can lead to identity theft.

Nearly half of this generation born between 1982 and 2004 are concerned about cyber crime, according to a TransUnion survey. But most of them aren't taking action to safeguard their personal information. Millennials also are:

- Most likely to engage in behavior that makes them susceptible to identify theft
- Most likely to fall for an online scam while searching for work
- Least likely to take advantage of the identity management and fraud monitoring services that can detect potential fraud and stop it before it wreaks financial havoc.

Some call it a "millennial malaise" about online security. On the one hand, millennials have been online and on social media so much throughout their lives that they don't think often enough about the impacts of their actions online—and the dangers. On the other, they see identity theft and fraud as inevitable, which leads to lax security behaviors making them even more likely to be victimized.

Millennials are more likely to use public Wi-Fi at coffee shops and other public places, share personal data on social networks, and disclose their passwords to others. All of those behaviors make them more susceptible to identify theft.

According to one survey in the United Kingdom, millennials are also the age group most likely to believe—incorrectly, of course—that data theft is a victimless crime. Thirty-four percent of millennials believe that, compared to 11 percent of Baby Boomers.

So, listen up millennials. Becoming more aware of the real dangers of identify theft is a first step. Then, there are a few basic steps to consider to help fortify your good name and credit:

- **Use strong passwords** containing uppercase and lowercase letters, numbers and special characters, and vary the passwords on each website.
- **Be careful when sharing personal information** on social media, especially addresses and birth dates, which identity thieves can use to commit further crimes.
- **Avoid public Wi-Fi**, especially to access bank and financial accounts.
- **Follow the three Ms** recommended by Adam Levin, chairman and founder of IDT911: minimize your risk of exposure; monitor your bank and credit card accounts daily; and manage any potential damage by using identity theft protection resources.

If you suspect you're a victim of identity theft or wish to proactively manage your identity, check with your insurance company, financial institution, or employee benefits provider. Many companies offer identity services from IDT911 for low or no cost.