West Texas Cyber Security Consortium

College Students: Ideal for ID Theft

Posted on 05/16/2014 by **Sid Kirchheimer** |AARP Blog Author |

If you have children or grandkids attending college, or about to graduate, it's time to school them on the dangers of **identity theft**.

Last year the Better Business Bureau deemed college students the "most at-risk" group for identity theft, and those in their 20s represented 1 in 5 of all victims (higher than any other age group), according to reports filed with the Federal Trade Commission.

College students and recent graduates are often targeted because they're ideal victims. Reasons:

- Many have access to credit cards and checkbooks — their own or held jointly with a parent — and, typically, a clean credit history that's attractive to ID thieves. But they're less likely than older folks to monitor their financial accounts.
- They're the most frequent and active users of social media and are more likely to post birthdates, hometowns and other personal information that can be pieced together by Facebook-trawling identity thieves.
- When victimized, they take longer to detect identity theft. Past studies have found that those ages 18 to 24 take an average of 132 days to discover they've been scammed – five times longer than the national average. Because of this delay, their financial losses have also been higher than those of older ID theft victims.

Maybe this explains why computer systems of universities are popular targets for cybercrooks.

So far this year, nearly 840,000 personal records were exposed in breach attacks against no fewer than 12 universities — including the University of Maryland, Indiana University, Johns Hopkins University, Iowa State, the University of Minnesota, Auburn University College of Business, a campus of the University of Wisconsin, Loyola Law School and the North Dakota University System.

Meanwhile, during the same period, fewer than 5,000 records were hacked in 10 data breaches of financial institutions, according to the **Identity Theft Resource Center**, which keeps tabs on reported breaches.

To reduce ID theft risk, teach your offspring to take the same protective measures as you do. That means:

- Monitoring their financial accounts, quickly and regularly. In addition to carefully reviewing bank and credit card statements for fraudulent charges, college students (like all Americans) should take advantage of the three free reports they are entitled to per 12-month period at **www.annualcreditreport.com**.
- Keeping checkbooks, bank and credit card statements, passports, and anything else with account numbers or other personally identifiable information (PII) in a locked filing cabinet, not a desk drawer. Ideally, sensitive documents, including credit card statements, should be mailed to the parents' home or a PO Box; dorm and apartment mailboxes may not be secure.
- Securely storing computers, smartphones and tablets (dorm rooms, in particular, can have "open door" access) when not carrying them. These devices should also be locked with PINs, and employ different passwords on

different accounts. Security software should be installed and regularly updated, and data should be encrypted, especially on smartphones. How-to info should be in the owner's manual or on the manufacturer's website.

- Avoiding Wi-Fi networks when shopping online — and never leaving payment cards "on file" at websites, in case a company is subject to a data breach. In general, it's safer to use retailers' dedicated apps than the phone's browser.
- Reading reviews before installing apps and sticking with trusted vendors, such as Apple's App Store.
- Declining free downloads for games, music and screen savers, and not opening links from strangers – especially those promising nude photos or videos of celebrities. All are popular ways to install malware.
- Realizing that social networks like Facebook can be a gold mine for identity theives. Studies show that commonly shared information, such as birthdates and birthplaces, can be used to accurately **guess most digits in a Social Security number**. A pet's name (often broadcast by young adults) is often used as a security question at websites – and also as an account password by young people. And hackers know this.
- Adjusting privacy settings on social network sites to make it difficult for strangers to view accounts or post material on your page.
- Using credit cards, which offer stronger liability protection, rather than debit cards. When using a debit card, especially at gas stations, choose the **"credit" option that doesn't require a PIN**.
- Shredding solicitations for preapproved credit cards and opting out of such offers at**https://www.optoutprescreen.com**.

For information about other scams, sign up for the Fraud Watch Network. You'll receive free email alertswith tips and resources to help you spot and avoid identity theft and fraud, and gain access to a network of experts, law enforcement and people in your community who will keep you up-to-date on the latest scams in your area.