### (Approx. 605 words)

### Don’t Let Your Identity be Compromised!

### By Jeff Wilkinson, President Sun City Summerlin Computer Club <https://www.scscc.club>

### president.scscc (at) gmail.com

We should all be cautious answering those seemingly innocuous questions posted on social media sites such as “*What Year Did You Graduate High School,*” or “*What City were you Born in,*” “*Can you remember your childhood phone number*?” or “*Who was your first-grade teacher*?” and on and on. These interesting questions appear harmless and appealing as you develop friendships and reminisce with old and new friends on social media, but beware! Many of these answers can be used to answer or reveal security question answers you chose when you set up accounts at your bank, utility company, etc. For example, when you forget your password, as happens all too often, you will be asked to answer security questions from when you initially set up your account, in most cases some time ago! In addition, answers to these types of questions posted on social media or quizzes can be used to build a profile on you with the information needed to open a new account!

Keeping your identity secure on social media is essential to your financial and personal safety. Unfortunately, identity theft is evolving, with thieves using the latest technology to move from credit card counterfeiting to checking and savings account takeover. A May 2020 study by [Javelin Strategy and Research](https://www.javelinstrategy.com/) found account takeovers — identity theft where a criminal gains unauthorized access to an online account belonging to somebody else — are trending at the high loss rate, up a staggering 72 percent over the prior year.

Remember that when you first create a social media account, you provide personal information such as name, age, email address, etc. And I venture to guess that most of us have never read the small print terms of service provided by the host. As you traverse the various pages, forums, postings, etc., data mining creates a profile of your behavior, likes, and dislikes. This information is often monetized by the host sites you visit, meaning sold to third parties. Facebook collects data from all devices you have installed their app on. The language used and time zone can include your device location, data provider, or internet service provider. Data on sites you like or visit via a link on Facebook is also collected.

What can the consumer do to protect themselves?

* Keep your software up to date
* Log out of social media sites when finished, particularly when in a public location or using a public computer
* Use two-factor authentication wherever possible.
* Used strong passwords - keep track of them with a password manager
* Use a screen lock on portable devices
* Don’t conduct business or share critical information on public Wi-Fi
* Put a credit freeze on your accounts with credit bureaus. [Equifax](https://www.equifax.com/personal/credit-report-services), [Experian](https://www.experian.com/freeze/center.html), [Innovis](https://www.innovis.com/personal/securityFreeze), [TransUnion](https://www.transunion.com/credit-freeze)
* Protect your social security number – only give it out when absolutely necessary
* Be aware of billing cycles – if financial information is late or doesn’t come, follow up
* Be cautious of participating in viral memes such as “name your most memorable concert.”
* Set strict privacy settings on Facebook, Twitter, Pinterest, Instagram, and LinkedIn

If you are a victim of identity theft, report it to the [FTC online](https://www.identitytheft.gov/) and create an account to create a report and generate a recovery plan. You will gain access to recovery plan updates and prefilled form letters to send to creditors. You should also report medical identity theft to [Medicare’s fraud office](https://oig.hhs.gov/fraud/report-fraud/) and tax identity theft to the [IRS](https://oig.hhs.gov/fraud/report-fraud/).

It should be clear that you want to avoid this, so a little awareness and preventative steps can help prevent potentially serious problems.