8/29/16

Reprinted from an August 25, 2016 post on Credit.com by Adam Levin, Co-Founder of Credit.com and IDT911

For adults, home is a refuge, but for children it is a never-ending treasure hunt. While you're out — you know, paying for the place — it's a safe bet your kids are getting into your stuff, and when it comes to things digital, that can be a serious problem.

As a seasoned parent, you've had that shock a thousand times, looking up from your phone, tablet or computer to the sight of a child holding something you thought was hidden or well out of reach, or wearing an old college hat you haven't seen since you packed your dorm room on graduation day.

The fact of the matter is that while home may be where you hang your hat, it's your children's habitat and finding things in it, for them, is, well, old hat.

Depending on the child, you may be living with someone who knows every single item in the house, even the unmentionables. But at issue here is not the hidden stuff. What matters is your mindset.

The Bottom Line

If you have something that is not supposed to get into your child's paws, whether that item is jewelry, a financial statement or a digital storage device, it needs to be kept behind lock and key, or preferably (since keys can be found and copied) in a safe that requires a biometric data point, such as a fingerprint, to disengage the lock.

Sound extreme? At a time when a few errant clicks or taps can cause an incredible amount of damage — either by exposing you to identity-related crime or compromising the security of a financial account — there are more ways your kid can get you got than ever, and some of them can put you in near-extinction-level trouble that takes a long time to sort out. (You can keep an eye out for signs of identity theft by pulling your credit reports for free each year at AnnualCreditReport.com and viewing your credit scores for free each month on Credit.com.)

Here are five items that could cause you headaches when shared with your kids — and ways circumvent any issues.

1. Access to Your Computer & Other Devices

If you pay bills or buy things online , or use social media, your computer is a gateway to really complicating your already complicated life if your child gets in there. The same goes for your smartphone and tablet.

While it is an easy toy/pacifier to otherwise engage a toddler, it is an even easier way for things to get messed up if the wrong app gets activated, an email gets accidentally forwarded or some other mishap of random tapping or clicking occurs.

While there is no easy fix for smartphones and tablets, there is for computers — even for families that have only one device. Set up different user accounts for each family member, and make sure no other member of the clan knows your password.

2. Login Information

Your children — and pretty much everyone else in your universe — know half your login information if you are like most and may even use your email address as a user ID. Get in the habit of designating a different user name known only to you, when given the option, and never share your password with anyone.

It's also good practice to change your passwords frequently. If you feel that creates too much margin for error, consider using a passphrase or password manager.

3. Access to Your Data Storage

You use some form of encrypted data storage, right?

If the answer is no, you're not alone. That said, it is a best practice to store all your most sensitive information — medical, taxes , employment, insurance — in an encrypted format on an air-gapped device (a storage device such as a flash drive or other external drive). Air-gapped simply means that it is not connected to the internet.

You get extra points for storing the device in a safe or behind lock and key.

4. PIN Numbers & Combinations

What's the point of having a safe if your children know the combination or passcode to open it? The same goes for PIN codes. This is a simple one. Do not share this information with your children.

5. Answers to Your Security Questions

This is another tricky area, because security questions are meant to be the kinds of information that close family members can answer.

Mark Twain is famous for saying, "If you tell the truth, you don't have to remember anything." Mark Twain also never did any online banking. When it comes to security questions, you need to do something that is morally wrong to do it right — lie.

Step two: Remember your lies.

Step three: Don’t tell your kids.