Minimizing Data Access

Welcome back! The previous lesson asked the question: *"Who can you trust?"* Now, here's another question: *"How do you avoid revealing information?"* Do you walk around with a tin foil hat? Do you take an oath to not speak outside the home? What do you do? Well, let's cover different ways you can minimize access to your data in the digital and real world.

Now, I ain't minimizing the promos, so get ready for another one :)

Promotional Spot

Many of us unknowingly give out too much information. *We see a web form and want to complete it to its full extent;* we want services and people to know who we are. The problem is we aren't aware of how others will handle your information, we talked about this in the previous lesson. *I worked as a cashier in a retail store, where customers were offered discounts for joining a rewards program--which required personal information. In general, the older crowd would say very uninformed things about the way the internet works, like thinking giving out their phone number would lead to their houses being broken into. But what they always had right was the instinct of being overprotective with their information. This was quite the opposite with the younger crowd, who was typically more than willing to give up sensitive data.* If that retail store suffered a hack, those customers would have their information available online. *Even a study done by Risa Puno in New York found people were okay handing over the last 4 digits of their social, face pictures, and even their fingerprints for a cookie--yes a cookie! Many people aren't aware of how much their data is worth.*

So let's first go through digital tips you should know to minimize the information you hand out, and then we'll move over to the real world.

The first digital tip is to go back to the previous lesson and make sure you're following those rules. They are very important and will teach you who to trust.

The second tip is to restrict the amount of information submitted to websites. *If there's no asterisk, it's not required--leave it blank. If something requires an email and you don't intend to use the service again, use a temporary email. If they don't require your real birthday, put a fake one.* Any information that doesn't need to be valid--shouldn't be valid. This means *picking gender-neutral emails that don't have your name and birthday built into them, using usernames which are arbitrary and reveal nothing about you, removing metadata from your photos*

before publishing them, and many more techniques we've covered throughout the course.

Third, establish emails and phone numbers used for different purposes. *Get a secondary phone number for work, get an email for spam, do everything possible to separate different sides of your life. I'm going to teach you how to do this in the next lesson.* On the topic of phones, if you can...refrain from having a voicemail message, because this will confirm a phone number belongs to you.

Fourth, *Don't, and I repeat: DON'T* send DNA to websites...it can be shared with third parties and is overall a huge risk. *MyHeritage leaked millions of account details, although thankfully no DNA leaks*, but it's only a matter of time until it happens. *23andme shared DNA without customer permission to a drug company.* If you're wondering why you should care about your DNA, *a researcher was able to recreate the face of an adult with only their DNA.* Pretty soon in the future, access to someone's DNA means you'll know a great deal about that person--*very similar to Gattaca.*

The fifth and final digital tip is to opt out of services and delete unused accounts. Go back and *rewatch lesson 2.3 and 2.4* that teaches how to delete your local and online identity, it'll go into this much more in-depth.

Okay! That summarizes the digital side of things, but what about the real world? Throughout this course, I've been trying to show that people want your data. It's more valuable than you think, and you should value it. The problem is, outside sources aren't always the biggest risk to your privacy, you are. It's not uncommon for us to walk outside and reveal too much information about ourselves, and this is a risk to our privacy and security goals. Let's cover the rules for the real world...

First, John Boyle O'Reilly wrote in Rules of the Road, "Be silent and safe--silence never betrays you." It's better to give no information, than too much information. This doesn't mean you should remain quiet in public, but think about what information you're giving out. This means sacrificing discounts at stores, not telling ultra personal stories at work or school, keeping your family and friends private, and *Never EVER bragging about your wealth, or this may happen to you.* Now, how do you respond to someone asking for your information in public? First don't make it sound like you're trying to hide anything, because you aren't. Just tell them identify theft is on the rise and you're not comfortable giving out that information. Be firm, and most people will back down. If someone from a company is asking for sensitive information, ask questions, don't give answers. *"Why do you need this information?" "Where will you store this information?" "How long will you store this information?" "What recourse will I have if this information falls into the wrong hands?"* Ask to speak to a supervisor to find out if the information is

required or if there's an alternative verification method. And don't be afraid to take your business elsewhere, we'll discuss advocacy later in section 6.

Second, you may be silent, but what about people who know things about you? They can potentially be just as dangerous. Tell people you know to keep certain parts of your life confidential. We discussed this in the previous lesson.

Third, cars! Be very careful with them, *especially those family stickers. They reveal how many kids you have and how many adults are in the home.* A stranger can see you have 3 kids, but you leave your home without them, signaling they are home alone. This could also reveal you're a single mom, making you a larger target. Be careful with custom plates as well, don't have them reveal anything too personal.

Fourth, trusts. *Trusts allow a third party or trustee to hold assets on your behalf.* For what we're trying to achieve, they are an excellent way for you to properly protect your car, home, or any other item you want kept private, and separate from your personal identity. But, you have to be careful with them, because if you put all your eggs in one basket, it can make you more vulnerable. *For example, if a trust gets sued, and all your items are in that trust, you might lose everything you have. But, if you transfer items into different trusts, your risk is heavily reduced.* If you get into a car accident and you have a trust that solely handles your car, none of your other trusts are at risk, and your privacy remains intact. Never let your personal life and the trust intermix. If you get a check for yourself, don't deposit it into the trust's account. If a salesman asks who the owner of the house is, say they aren't home, because you aren't the owner. This is all VITAL to properly maintain privacy in a trust.

To continue the discussion on homes, let's discuss *the fifth* and final tip. Get a *PO box or private mail box. They each have pros and cons which may be better or worse for certain people.* Use these as your shipping and return addresses, avoid giving out your actual address. You can make this even better by opening a third box belonging to your trust--if you have one. The last housing tip, which I know can't necessarily always be avoided, but just something to keep in mind, is avoiding renting. Renting allows landlords to understably perform background checks, credit checks, and more if needed. Try to own your properties or put them in a trust, if possible.

To summarize the lesson, a lot of us give out way too much information that doesn't need to be given out. We have the tendency to be honest and undervalue the worth of our data. Your personal information is extremely important, so treat it like so.

Queue Outro Promos

That is all that is to be said about minimizing data access; I hope this changed your perspective on data collection. Thank you for watching and I'll see you in the next lesson discussing two great techniques to further improve your privacy: *anonymization and pseudonymization.*