Who Can You Trust?

Who can you trust? That's a loaded question! Let's start with a disclaimer: I don't want to make it seem like everybody is out to get you, and no one is trustworthy in your life. But I do want to make you cautious with how other people can intentionally or unintentionally leak sensitive information about you.

Promotional Spot

Let's begin with the people closest to you--*family and close friends*. These are your most trusted peeps, but proceed with caution. Not because they're necessarily untrustworthy, but their habits can be improper. *For example, you and your wife are outside your home when she decides to take a selfie with you to share on Facebook.* What she doesn't realize is she included the house number in the picture, in addition to location metadata within the image. To top it all off, her Facebook account is public. A thief now has the necessary information to rob your home. *Another more common scenario is someone screenshotting a conversation between you and them,* or a friend gives out your personal phone number to a stranger without your consent. On the other hand, you should trust your family and close friends well enough for them to understand why you may want parts of your life kept secret. The key is *communication*, tell them transparently what information they can or can't share about you with others.

Moving on, *casual friends and strangers* are a much bigger concern. In the movie *Now You See Me, the 4 magicians ask the character Tressler casual questions, which he gladly answers. What he doesn't realize is he is gave them answers to his bank's security questions. The 4 magicians eventually break into his bank account, and steal his funds as part of their magic trick.* This is a form of social engineering, *"The manipulation of the natural human tendency to trust."* Social engineering is dangerous because it exploits the way humans function to achieve unauthorized access. How is this done? Well we talked about *phishing scams earlier in the course, which relied on you trusting a fraudulent website that steals your information--this is a form of social engineering.* **** show phone **** This can happen with your phone calls as well. *Hackers can call their targets from a "spoofed" phone number claiming to be someone needing your information.* It could be spoofed to be your AT&T provider asking for your account details, or the IRS asking you to pay "missing" taxes.

Tailgating is another form of social engineering where a person pretends to be a delivery service at a corporate office and asks an employee to hold the door

open for them. If you think these things don't happen, here's a fun story similar to tailgating: *A 17-year-old male from Oklahoma was fired from his job at Walmart for stealing money. Instead of considering himself lucky that he got away without being charged, he put his uniform back on and stole $30,000 from three other Walmarts by pretending to be a general manager from another store.*

Alright, so we've covered trusting individuals, both well-known ones and strangers, as well as how social engineering can be very dangerous. But what about trusting *companies* to handle your data? This course has already discussed dozens of different companies who have misused data—many times without user knowledge. So, can we trust them?

Toysmart.com made a pledge of privacy to its customers, promising not to share its database with other companies or third parties. *Then, the company went bankrupt and promptly put its user database for sale.* This practice continues to this day. *Hulu stated they will sell data if they suffer bankruptcy. In fact, this article from the New York Times found in the case of a merging, acquisition, bankruptcy, or asset sales, many companies, including Amazon, Apple, Facebook, Google, and LinkedIn may transfer user data to another entity without user consent. We saw this happen during RadioShack's bankruptcy, when they attempted to sell user credit and debit cards, social security numbers, dates of birth, and even phone numbers; luckily politicians stepped in before ALL of the data was fully sold, although some still was.*

Let these examples be a lesson that even when companies promise privacy, they could be lying, or they could unpurposely implement poor methods of securing your data.

The moral of this lesson is be careful with who handles your information. Don't give up data when it isn't needed, and don't trust everybody to handle your information as well as you would. Here are some general rules for you to follow:

1) Don't give up information that isn't required. RadioShack didn't need your social security number, Facebook doesn't need your home address, and a stranger in public doesn't need your date of birth.
2) Be aware. Ask yourself why a company needs a specific type of data. Don't be afraid to ask why something is needed, and be aware of the existence of social engineering attacks and how they can impact you.
3) Don't succumb to pressure. If you feel that a piece of information doesn't need to be collected, ask to go a different route, or deny access to the information and pick a different service if possible.
4) Make sure the people around you know what information they can or can't share about you. You can keep your life as locked down as possible, but if

your partner or best friend is sharing your phone number and email that's intended to be secret, well...that's not good.

Queue Outro Promos

And that wraps up this lesson. There will always be those you trust, but remember to educate and communicate with them about your privacy and security habits. As for companies and other entities, it's safe to assume the worst, because there are little to no regulations on how your data is shared at least in theUS, and most companies will take the opportunity to abuse your data for a quick profit. Thank you for watching, and I'll see you *in the next lesson: Minimizing Data Access.*