Do you know who has your data? Do you know what they’ll do with it?

By Dr. Doug Jacobson

There is a new cybersecurity event nearly every day. Terms like ransomware, data breach, and threat actors become common to hear, leaving more people wondering what they can do to avoid them.

There is a lot of advice on keeping data in your possession safe, but what about the data you have entrusted to someone else? How can you protect that data, and what happens when they lose your data?

An attacker’s goal is to make money, and your data has value. Attackers target companies that possess customer data, because if they are successful, they can get thousands—if not millions—of records, which increases their potential payout. To acquire customer data, attackers steal it, which is referred to as a data breach. Additionally, attackers can hold customer data for ransom. This event is referred to ransomware—where attackers threaten companies that if they do not pay the ransom, attackers will not return the customer data and, perhaps, sell it to someone else.

So how can we make sure that the data we provide to companies is still safe? Well, we rely heavily on the company to keep our information safe, but we still have some control over where and how we share our data. Here, we will introduce common types of data, how their loss affects us, and how we can prepare for the possible loss of data by a third party you entrusted with your data.

Three Types of Data

Think of the information you have provided to third parties—passwords, credit card information, and personal information. To boil it down, data categorizes into three types:

1. Money
2. Data that unlocks something
3. Data that represents you

Money

Data that can convert into money is the easiest threat to understand. Credit card numbers and banking information pose great risks if not handled with care.

Credit card companies limit monetary loss; however, it takes time, stress, and effort to change your credit card information that has been used for automatic payments. Plus, if forgotten to be updated, late fees and penalties can arise. Attackers that acquire bank account information can drain money from the account, and financial institutions may not cover the loss.

While there is no way to stop an attacker from using your credit card information if stolen, you can make it easier to recover.

1. **Use a dedicated credit card for online purchases and automatic payments.** It is easier to identify any misuse when checking your statements, and you can set the limit on the card to a lower value to limit the damage.
2. **Use a third-party payment system.** Third-party payment systems, like PayPal, reduce the number of websites that have your credit card number. Instead of typing your credit card number on each website, websites can use whatever credit card is tied to the third-party payment system.

Data That Unlocks Something

This data type provides access to other data. Examples of this data type are usernames and passwords. They are meant to protect access to other valuable data. Attackers often steal files containing usernames and passwords. While this file contains an encrypted version of your password, attackers can still figure out simple passwords. Then, they will either sell the username and password, or they will use it themselves on another website. The loss of usernames and passwords can lead to the loss of other data or information.

Luckily, it is easy to make it strengthen passwords.

1. **Use long and complex passwords.** They are difficult for an attacker to guess or figure out, even with a stolen password file.
2. **Do not reuse passwords.** Unique passwords limit attackers' access if they happen to get a password. In other words, a Facebook password may not be the same password to the same user's online bank account, which means the attacker would not have the correct password for another website. Fortunately, there are safe password-keeping programs—LastPass, 1Password, or Bitwarden—to help remember our passwords.

Data That Represents You

Data that identifies you is often called personally identifiable information (PII). Attackers use this data to convince others that they are you. The loss of this data can lead to identity theft, false accounts, loans, or anything that requires this highly sensitive information. PII comes in two categories:

1. Private, unique identifiers—social security numbers, medical records, etc. These records are the best ways for attackers to create a fake identity.
2. Shared, unique identifiers—contact information, social media, etc. Attackers use this information to create fake messages such as phishing emails.

The most effective way to avoid the loss of this information is to not give it out. There are instances in life where you will need to provide this information but be aware of where and who you give it to. Make sure that you only provide this information to companies that you trust and not to those you do not know.

The loss of any type of data can be substantial, but it is easy and worth it to take precaution and do what we can to keep any of our information safe—whether it is in our possession or in others' possession. If it is your information, it is still possible to avoid and mitigate issues.

Be Proactive

Here are common things that everyone should do to minimize the effect of data loss.

1. **Use Multifactor Authentication (MFA).** Enabling MFA on websites that have highly-sensitive information—such as your banking information—makes it nearly impossible for attackers to access your account. Attackers would need your cell phone or email account information in addition to the correct username and password to the site. Check with each website that has your sensitive information—such as your banks, credit cards, loans—to see if they support MFA.
2. **Set up credit monitoring.** Check your credit and set up credit monitoring. Credit monitoring will alert when someone is trying to use your identity—like your social security number—or when new credit cards are establishing in your name.
3. **Consider freezing your credit.** If you implement a credit freeze, your social security number cannot be used to open new lines of credit—loans, credit cards, etc. Therefore, attackers would not be able to use your social security number to do so. Remember that you will need to unfreeze your credit if you need to open credit. To freeze your credit, you will need to create accounts with the following credit bureaus:
   a. Experian: https://www.experian.com/help/login.html
   b. Transunion: https://service.transunion.com/
   c. Equifax: https://my.equifax.com/membercenter/#/login
4. **Move accounts online.** Everything has moved online, but that does not mean your accounts—social security, pensions, investments accounts, etc.—have yet. Make an account for yourself before an attacker creates one on your behalf. Here is where to make your My Social Security account to protect your personal information: https://www.ssa.gov/myaccount/
5. **Watch your statements.** Regularly monitoring your statements every month makes it easy to spot an abnormality or an action that wasn't you. Additionally, you will catch it before there the time to file a claim is up.