September 2024

Time to Lock it Down

By Mark Costlow

We've seen a series of ever larger data breaches for the past couple of decades. It's not very surprising. Putting all of our data online has concentrated it and made it a juicy target for bad guys. As **Willie Sutton** said, that's where the money is.

A **2013 Yahoo data breach** leaked info on 3 billion people. The **2017 Equifax breach** exposed half of the US. population's data. Now the latest news is that "**National Public Data**", a for-profit data broker, was **compromised in December, 2023**. The data was offered for sale in April, 2024, and then leaked in July, 2024. It is making headlines now because of the large amount of data and the fact that it has leaked so that any scammer who wants it can have it.

Of particular concern in this data dump is Social Security Numbers (SSNs), combined with other significant data points (name, birth date, previous addresses and phone numbers, etc.). Experts warn that this data can be used to impersonate people to open new accounts or take out loans in your name.

We don't want to encourage panic. After all, much of this data has leaked before, and even this specific dump has been in the wild for months. It is likely your data is in the hands of criminals already. If they haven't used your data yet, it is probably luck of the draw. But, why wait for your luck to run out? Take some steps to protect yourself instead. Here are the actions experts recommend to keep you safe from fraud.

Protect Your SSN

Everybody should establish a "my Social Security" account at **https://ssa.gov/myaccount**. This lets you "claim" your SSN and view activity related to it. This is the best way to find out if your SSN has been used by identity thieves. Note that if you have an account already, but you created it more than 3 years ago, you need to take action to convert to their newer system, which is detailed on the site.

Everybody should do this, whether currently receiving Social Security benefits or not. A common SSN is to report wages for another person, which can make the IRS think you have not reported all of your wages when you file. With an account, you can also set up blocks to prevent anyone from viewing your SSN information or making any changes to your Direct Deposit settings. The site also has a **blog post** and a **pamphlet** with suggestions to prevent, discover, and recover from fraud.

Freeze Your Credit

Freezing your credit prevents identity thieves from opening new accounts or taking out new loans in your name. There are three major consumer credit reporting agencies in the US. and you have to freeze your credit with each one separately. The links to set up an account and freeze your credit at each company are as follows:

- Transunion: **https://www.transunion.com/credit-freeze**
- Equifax: **https://www.equifax.com/personal/credit-report-services/credit-freeze**
- Exeprian: **https://www.experian.com/freeze/center.html**

What to know about a credit freeze:

- You must freeze it at all three agencies to be effective.
- The credit freeze will not affect your credit score.
- Credit freezes are FREE. But beware that these are profit-seeking agencies and they may try to steer you toward accounts with a monthly fee. The links above lead directly to the free account sign-ups.
- If you apply for a new credit card or a car, home, or personal loan, you need to "thaw" your freezes for your credit checks to succeed. This is also free, and you can re-freeze as soon as your new account is established.
- **DO NOT LOSE** your passwords and/or PINs for the credit agencies. Recovering them is possible but quite difficult. Print them out and keep them with your other secure documents.
- The process is easy and takes about 5 minutes per agency.
- It may give you pause that one of these companies is listed as both a source of an **historically enormous data leak** and someone who can help safeguard your data. Rest assured that the information you have to give the agencies to get this protection is not new to them. They already know much more about all of us. So yes, they are susceptible to future leaks, but it still makes sense to ask them to lock your credit down to protect you from the fraud that could result from that and other exposures.

Monitor Your Credit

During the COVID lock downs, scams of all kinds spiked. The credit agencies introduced a temporary program to make weekly free credit reports available to everyone. As of September 2023 that program has been made permanent, and now every person is entitled to free weekly credit reports

from all three agencies. Visit **annualcreditreport.-com** to sign up, and keep an eye out for unexpected activity.

That site requests reports from any or all of the three agencies on your behalf. However you can also request reports from them individually using the accounts you have created to freeze your credit. Just know that the free report option is intermingled with offers of subscription services so you have to pay attention while navigating the sites.

Fraud Recovery

If you believe your identity has been stolen, visit **IdentityTheft.gov**. This site, run by Federal Trade Commission, is a one-stop service to make a report and get a recovery plan. You can also call them at 1-877-IDTHEFT (1-877-438-4338).

The Internet of (Broken) Things

By Mark Costlow

The term Internet of Things, or IoT, refers to our ultra-connected world, where every device is connected to the Internet. The connections let the devices, the cloud-based services, and the human end-users talk freely with each other with minimal configuration.

A common example given to explain how IoT will help us all is the **smart refrigerator**. Grand promises where made: the fridge will tell you when you are (almost) out of eggs, or the milk is going bad, and even order the replacements automatically. Most people just shake their heads at the idea. On the other hand, those connections enable some truly valuable features, such as informing you about a failed component so you know as soon as it happens, instead of finding out after your groceries have spoiled.

For better or worse, consumer manufacturers have embraced IoT fully, and are building it in to everything: cars, appliances, toothbrushes, kid toys, adult toys, light bulbs, thermostats, medical devices and **anything with a power switch**.

IoT Risks

IoT gadgets have embedded computers with Internet connections. **All computers have bugs in their software**. Over the years, bad people find the bugs and exploit them. Ideally, good people also find the bugs and fix the software. But many IoT device makers ignore this and leave their devices out in the world without any way to update. If you invite one of these into your home, you just have to hope that it won't someday turn on you.

Another risk is loss of connectivity. People diving into home automation are often **surprised how much of their home becomes an inert lump** if their Internet connection fails. For most people that's a rare occurrence, but it does happen and it can be quit a surprise to realize you can't turn on the kitchen lights if Alexa can't phone home.

The main risk we will look at right now is IoT Abandonment. IoT devices often require a cloud-based service to operate. For example, consider checking your home security camera while at work. The app on your phone contacts the camera maker's service in the cloud. The camera at home has already contacted the service to upload its footage. The cloud service functions as a well-known meeting place where your camera and your phone app know to go so they can talk. The advantages of this arrangement is your phone app doesn't have to know how to get into your home network, and the initial setup when you bought the camera was quite easy. The camera is "ex-filtrating" your video footage to the cloud so your phone app can easily access it any time.

The same negotiation happens for any number of other transactions: closing your garage door from afar; unlocking your front door to let in a friend; telling the robot vacuum get busy; having your doctor check your cardiac monitor; when your semi-autonomous car needs to find the nearest charging station. The cloud service is a critical component of these products. They are "bricked" (IoT parlance for "useless, dead, inert") without it.

With this in mind, here are a few recent IoT Abandonments:

Amazon Echo Show 8: the primary feature of this 1-year-old device is to display the user's photos on its home screen. **Amazon is ending the service** which managed the pictures so the device will now show ads instead.

Snoo "Smart" Baby Bassinet: it rocks and plays soothing sounds for the baby, costs $1,700, and has a phone app to control it. **This summer they "pay-walled" many of the features** with a $20/mo subscription fee. People who bought new before July get to use it free for 9 months. Anyone who buys a used one is stuck with a new monthly fee. It's likely many used buyers and sellers will not even know the buyer will have to pay to use it.

Peloton, maker of expensive stationary exercise bikes, is restricting the market for their used bikes. **Activating a re-sold bike will now cost $95**. Nothing of tangible value is provided for this fee. You still have to pay a subscription fee for the "extras" but now a second-hand owner can't even use the basic features without paying $95 more and likely opting in to Peloton marketing.

AVTECH AVM1203 Surveillance Camera: an unpatched bug in this 5-year-old camera's software is allowing unknown attackers to install "botnet" software (used to attack Internet sites). **The AVM1203 is no longer sold or supported so there is no fix**.

PowerDale Electric Vehicle Chargers: The Belgian **company failed in July 2023**. Some chargers are now inaccessible, and others are forced to the slowest charging speed with no way to change it.

Right now the only protection is to ask questions before you buy. Think about how the product is used, and what it will do when the router is turned off or if the phone app goes away. Then decide if you will be left with something useful or just expensive e-waste.

Southwest Cyberport - swcp.com

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on bold blue type in browser for links.