WINTER 2018 HERSHEYSMILL FRAUD PREVENTION NEWSLETTER
SPECIAL EDITION

In the Fall Newsletter I spoke about the issue of Identity theft with the purpose of helping you to understand it and giving some advice on steps to protect yourself to the degree possible. This was in keeping with all the previous issues which are based on fraud protection by describing scams and ideas to protect yourself.

In this issue I want to give some background on an issue highly related to protecting your identity that goes much beyond that. In fact, it will be one of the hottest issues in the media, the legislature and affect many of America's largest businesses.

The overall issue is referred to as PRIVACY, but it has multiple parts. But before beginning to discuss it, you should know two things. First, I will be describing the issues. I will not be recommending anything. Second, this is a bi-partisan issue. This affects all Americans – Republicans, Democrats, Independents etc.

What is PRIVACY and What Does it Mean to You?

The heart of the issue involves these questions:

- Who owns the data about you?
- Who has a right to collect it?
- Do you have a right to view and correct data collected about you?
- Can you restrict who sees this data
- Do you have a “Right to be forgotten?” In other words, can you request or demand that your data be deleted?
-

In case you think you really don’t care about this think again. With the dirt-cheap cost of storage and the use of sophisticated software techniques that combine your data from all over the internet, companies can know way more than you want them to such as your religious beliefs, your political beliefs (much deeper than Church or party affiliation), who your friends are etc. Also, while you may not remember all these things, they will never forget them. For an example of a significant practical use, all political parties and their PACS used this information to tailor the ads that you saw in the 2016 election on FACEBOOK and elsewhere based on this data.

So the primary question is: Who Owns Your Data?

Thus far in America it is the people who collect it. You really have no say in what they do with it. The companies may have published Privacy Policies but no one reads them because the lawyers make them difficult to understand. Also, if you don’t accept them as is you can’t use the product. Further, if they violate their policies your only recourse would be to sue which is totally useless and expensive.

So what can you do about this? Really nothing as an individual. Only government regulation on this can make any difference. If you think I’m being liberal here just know that current hearings are being held in the Republican House and Senate. Also, the big boys (Google, Facebook, Amazon) are asking for regulation (their version of course) to protect them from State DA lawsuits and other criminal prosecutions.

Finally, these American companies face the EU’s position on Data Ownership. Over there you own your own data. Facebook and Google are facing heavy fines for treating European user’s data the American way. Again, this issue will be a hot news and business issue.

That’s a summary of the issue. It is a complicated one that will have an impact on everyone when it is resolved.

Now back to our regularly scheduled program.

ROBOCALLERS Getting More Creative.

On this issue I am speaking from personal experience. They are trying two new tricks to get you to answer their call which they want you to do for one of two reasons. Either they just want to ensure yours is a valid number which they will then sell to telemarketers, or they are telemarketers (or scammers) who want you to give them money for a doubtful purchase or a scam.

Their first new trick is to use fake people's names. They feel that a real name combined with a Neighborhood Spoofed Caller ID will get you to answer. Neighborhood spoofing simply means the Caller ID is local. In my case, the Caller ID is 267-228-xxxx where the Area Code and Exchange match my phone exactly.

Their second new trick is that they have been able to pair your land line and cellphone numbers where a landline call is immediately followed by a call to your cellphone. This make it look like someone who knows both your numbers is calling so you're more likely to answer.

Here are some tricks you can try to help reduce these calls:

If you have a land line press *77 to block ANONYMOUS and PRIVATE callers. Deactivate by pressing *87. This works for Verizon. Your carrier may be different.

Don't fall for the one ring trick by calling back to see who it was

On your cellphone you can pay your provider a monthly fee to block many of these calls.

If you do pick up the phone, don't say anything. Often the call will disconnect.

A Modern Twist on an Old Scam - WORK AT HOME

Back in the day there were many variations of this scam. Being paid to stuff envelopes at home was a notable example. But scammers evolve with the times. The pitch now is to start a home business selling whatever appeals to you, by having them set up a website for you at a very low cost, say $50. Alas, you still get what you pay for.

To show you the degree of financial risk that you will be exposed to, telemarketers will pay the company that signed you up $150 to $200 for your name. Remember these guys don't expect to lose their money.

The blizzard of calls you will receive will tell you you can't do anything with your $50 website. However, if you pay them a fee (thousands of dollars) they will upgrade your site and you will see a certain amount of sales. They will upgrade your site, but now

they say you won't show in web searches which of course they can fix for another large fee. Eventually, people realize it's a scam and drop out.

My advice here is very simple. If you can build and support your own website give a home business a try. If you can't, run, don't just walk away from these scammers.

SMART TOYS

By now you have heard, or should have heard about the IOT. The IOT is the Internet of Things. This refers to the internet connectivity of things you might not expect. For instance, today many major appliances and home heating systems come with internet, so they can notify the service company of an impending malfunction. In addition, others such as smart thermostats allow you to control them remotely. This is all great but remember that in most cases there is little or no security with these systems.

Well, who cares if someone hacks my thermostat? All they can do is twiddle with my temperature. Well that may not be true, but let's move to the issue that SHOULD concern you – toys for your grandchildren.

The Danger of Smart Toys

Let's start with the first problem. These toys are often the most requested.

The second problem is that the more lifelike these toys become, the more children confide in them.

So what are the issues of concern?

These toys contain microphones, and increasingly cameras, to enhance their ability to relate to the child playing with them

To start, the FBI has warned consumers that these toys pose "concerns for the privacy and physical safety" of children. Also, toy companies are not computer companies with computer security departments. They are driven by low price and time to market which pretty much rules out security.

The crucial issue here is what happens to the words and images the toy is collecting from your grandchild. If, as is probably the case, the data goes back to the toy maker so they can sell it others. These OTHERS can use the information to commit identity theft on children which is especially bad because no one is checking. Also, since these

devices have no security, pedophiles and criminals could easily get location information on children, and they might actually be able to talk to them and ask questions about their routines.

Finally, we can't put much faith in the toy makers. In January, toy maker VTEC was fined $650, 000 by the FTC for a data hack that revealed the following information about children and their parents:

- Name
- Sex
- Birthdate
- Email Addresses

An even worse situation occurred in Germany where a smart doll was specifically designed to collect children's information. It recorded conversations, converted speech to text and shared that information with unknown 3rd parties. German authorities asked all owners to remove all electronics from the dolls.

In the area of direct hacking, researchers at Indiana University were able to gain unauthorized access to the nose camera in Fisher Price Smart Toy Bear. They stopped manufacturing the toy, but it is still available at Amazon and Walmart for $55.99.

One last "toy." The Amazon Fire HD kids Edition. The tablet has a walled garden called FREE TIME which allows parents, and Amazon to see everything the child does. Amazon says they don't share this data but they have it. Also, if the parents give permission to the child to use third party applications they can collect the child's information. PS. Amazon says the tablet is "not a toy."