DRAPER

NEIGHBORHOOD WATCH

ISSUE #5
May 2019

DraperCityPD
@DraperCityPD

Smart Toys, Your Privacy, and Cybersecurity

Did your child receive a "smart toy" this holiday season? If so, be aware these internet-connected toys may present privacy and safety concerns for children and their families, according to the Federal Bureau of Investigation (FBI). Internet-connected, or smart-toys, combine computer technologies into very passive looking toys, like a stuffed bear. The toy is designed to have an interactive relationship with the child. According to the FBI, the immediate danger is a child may innocently share sensitive data an adult would never share. These include family schedules, activities, and passwords

This exposure could place a child, a family, and their home in danger. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information being unwittingly disclosed.

These "smart-toys" are designed to gather and analyze data, then provide a response to a child. On a simple level, it's a cute idea to have a teddy bear talk to your child. But where do you draw the line between safety and enjoyment? The potential problems include:

- Information being collected – Information such as the child's name, school, likes and dislikes, and activities may be disclosed through normal conversation with the toy or in the surrounding environment. Personal information (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses / IPs.
- Security of data – the WiFi signal (connecting the toy) can be hacked.
- Who is collecting that data? "Data collected from interactions or conversations between children and toys are typically sent and stored by the manufacturer or developer via server or cloud service. In some cases, it is also collected by third party companies who manage the voice recognition software used in the toys," according to the FBI.

In short, the potential exists to have a tremendous amount of very personal data shipped out of your home to unknown parties. If you have one of these toys in your home, be aware of potential associated risks.

Upcoming Events

Utah Law Enforcement Memorial

May 2nd 11am

West Lawn State Capital

Utah Special Olympics Law Enforcement Torch Run

May 22nd 9:30 am

Start: Harmon's parking lot

11400 South 700 East

End: Draper Police Dept.

1020 E. Pioneer Road

DRAPER

NEIGHBORHOOD WATCH

Neighborhood Watch 101

Secure your home. Look around the outside of your home, pay close attention to windows and doors. Where would you break in if you were a criminal? Do the doors and windows lock. Ensure deadbolts and door locks are anchored deep enough, penetrating deep into the doorframe. Do windows and sliding doors have wooden dowels placed into the tracks, especially those on the main level or basement? Train your family on how to remove the dowels and open windows from the inside in case of fire.

Porch light on and leave on all night. Contrary to urban legend, this will not increase your electric bill dramatically when using regular wattage bulbs, but it will increase the security of your neighborhood dramatically. Criminals hate to be seen. Install motion detector lights to illuminate all possible points of entry into your home and to keep any cars, boats, sheds, etc. illuminated as well.

Secure your garage. Close your garage door any time you are not in the garage. At night, as well as when you are in the backyard doing yard work or just running to the store for a few minutes. A passing burglar can quickly remove bicycles, skis, golf bags, or power equipment. Do not leave these items lying on the lawn or unsecured outside at any time.

House numbers are clearly visible. Police and emergency personnel will need to find your address quickly in the event of an emergency. House numbers need to be visible on your house or mailbox. Numbers painted on the curb are difficult to see at night and during inclement weather.

Vacation Plans

Now you can add a little peace of mind to your travel agenda. As staffing permits, Draper Police Department will check your house periodically while you're gone. It is best to ask a trusted neighbor or relative to check the exterior of your home while you're away, making sure doors and gates are secure and any unwanted papers or advertisements are removed from the front porch. If they see a problem, they should notify you. If appropriate, they should call 911 if a crime is in progress or call 801-840-4000 to have a police officer respond for a situation not in progress.

To submit a request for a vacation house check: http://www.draper.ut.us/propertycheck We ask you submit a request at least a week before your departure date. For more information, please call the Draper Police Department 801-576-6300.

WiFi Safety While Traveling

When your family is traveling this summer, you need to be careful while using use your mobile phone. Traveling in another state or another county often leaves you without a secure data connection. Often we select the first open (unlocked) WiFi network we see listed on our phones. This could be at a hotel, restaurant, or airport. The risk in using these service providers is we often don't know who created the WiFi link. The best rule of safety is: if you don't know the source of the WiFi, don't use it. Confirm with employees at an establishment or event if they provide a WiFi and the **exact name** of their WiFi hotspot.

A very common form of attack is the "Man-in-the-Middle" (MitM) model where a hacker creates what looks to be a genuine WiFi hotspot. You can't see it, but all of your data is at risk to be intercepted by data thieves.

A great protection against these potentially compromised communications is called a Virtual Private Network (VPN). These allow you to connect to the internet, but your phone's background data is scrambled to protect your identity and location. It's an extra layer of protection between you and the bad guys.

Check reputable websites such as PCMag.com for lists and description of free VPNs. Hackers have plenty of time and creativity to contemplate ways to breach your security. We need to protect ourselves. Think of it this way: If you drive out of your garage, someone can follow your car and track where you went, how long you were there, and when you returned home. We call that stalking. Using a VPN service is like driving into a closed parking garage, switching to a different car, and then driving out a different exit. Anyone following your original car now has no idea where you went after entering the garage. A VPN service keeps the stalkers at bay. VPNs provide another layer of protection between yourself and the people who actively working to steal your data. Remember the simple law of online security: If you are online, you are under attack. It's up to you to take a few extra steps to ensure you are safe.

If you would like more information on any of the material mentioned in this month's newsletter, contact Draper's Neighborhood Watch Coordinator at 801.576.6342 or crimeprevention@draper.ut.us