Cyber Security Newsletter

October 2016 **Infotainment Systems and Cars**

In This Issue

Other Interesting Links

- Best Practices
- FTC Warning
- Security Risks
- Tips
- More Tips

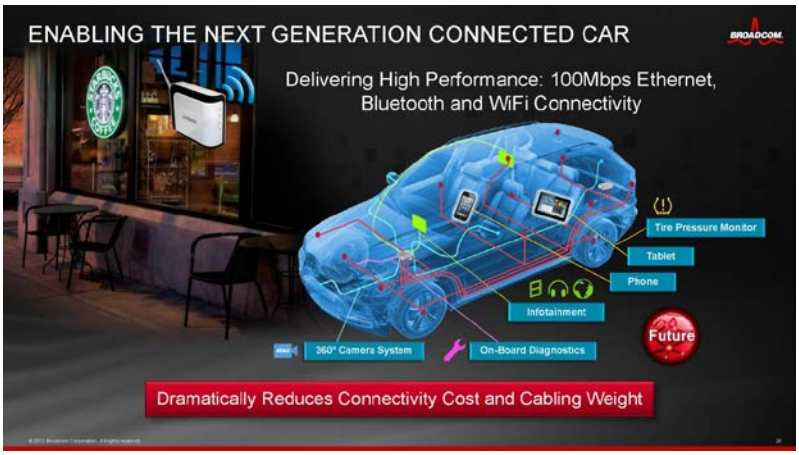
Contact Us

Cyber Security Site

Introduction

Happy Halloween and Cyber Security Awareness month. For those who don't know, October is not only the time for ghost and ghouls but is also Cyber Security Awareness month. So in the spirit of the season, let me try to scare you.

Does your car have an infotainment system or have you rented a vehicle that does? How often have you rented a vehicle and plugged your smartphone into the car to charge? Have you ever thought about what information might be passing between your phone and the car? What happens to that information when you return the rental car or sell your car?



These are just some of the questions you should probably ask yourself anytime you connect your smartphone (or other mobile device) directly or through Bluetooth to any system. This month's Cyber Security Newsletter will focus on Infotainment Systems in cars and their dangers, specifically rental cars.

Rental Cars

There are several reasons why people rent cars. Maybe your car is in the shop being worked on. Or you are on vacation or on a business trip. Or maybe you are taking a road trip and don't want to put the miles on your car, etc. These are all common reasons and people think nothing about it because they don't see any danger beyond the normal physical dangers of driving. But there are other hidden dangers when renting a car which most people never think about. These dangers can potentially put you and your family at risk.

In an effort to provide conveniences to drivers and passengers, it has become the standard for car manufacturers to include such features as Bluetooth for hands-free communication and built-in entertainment systems for passengers. Car rental companies are continuously upgrading their fleets to provide these conveniences to their customers. This means that many of the cars you might rent now have the latest infotainment systems which let you connect, or "pair", your smartphone with the car. This is often done via Bluetooth but can be done by connecting to a built-in USB port. This allows the vehicle occupants to do things like make and receive phone calls, dial from the central console, get directions, stream music, look up contact information, etc.

So why are these things an issue? When you connect your phone or other mobile devices to a car, the car stores information from your phone on its hard drive. Things such as call logs, contact information, app information, etc. It is even possible that pictures, user names and passwords for apps, and other personal information that is on your phone could be downloaded to the car. This makes all of the information on your phone potentially available to people you wouldn't want to have the information.

How to protect yourself

If you are like me, you often make it to the rental car company to turn in the car with just enough time to catch your flight. You are in a hurry and you know the plane will not wait for you. However, if you have attached your mobile device to the car you need to give yourself at least 10 minutes to remove your personal data from the car. You do this by going into the car's settings (this will vary per manufacturer) and looking at the list of paired devices. When you find yours, delete it or "unpair". When you do this it should delete all logs and saved contacts from the car's memory.

But does it really? Just like all other devices with a memory, the infotainment systems are just specialized computers. Like all computers, the data isn't really deleted when you delete it. The information is still on the hard drive until the system overwrites the data storage area. A better option might be to look in the car's settings to see if you can clear all user data. If possible, the best option would be to do a complete factory reset. That should completely wipe out all stored data or at least make it very difficult for someone to retrieve.

One more thing to think about is if you used the car's navigation system. Most people don't realize that navigation systems keep a history of searches and where the vehicle has been. Unless you really don't care if someone knows the locations you visited (such as your home, friend's homes, etc.), it is suggested that you go into the system's settings and clear your location history. This will make it more difficult for someone to track you.

Best practices

Because of the advances in conveniences in cars, they have become another threat vector that must be protected against. To do so, here are some best practices to consider:

1) **Be careful about syncing data**: Do you really need or want your information on a rental car's hard drive?
2) **Watch out for malicious applications**: Most manufacturers generally have their "app stores" locked down, but there is a push to move to open source operating systems for cars. There is also malware that can migrate from your phone to the car. This should scare anyone because it has already been demonstrated how easy it is to hack into a car and control it making it do things like not stop when you push on the brakes or turn your engine off while driving.
3) **Think before you plug in**: Do you really need to connect and risk compromising your data or the agency's data if you have a department phone?
4) **Be sure system updates come directly from the manufacturer**: If you aren't positive the update is coming directly from the manufacturer, don't install before you validate.
5) **Choose a safer car**: It is smart to be aware of the dangers to you, your information, and the vehicle itself. Here is a good read about **car hacking**.

As always, being informed and trained lets you make educated decisions.

Cyber Security at work

Are you curious about what kind of things Cyber Security is dealing with and protecting the agency from? Below are some of the more important things we dealt with in the last month.

- Blocked emails – 8,200,000
- Ransomware emails stopped – 25
- Detected malware – 528
- Vulnerable applications detected – 40,064
- Phishing connections stopped – 5,748,585
- Malicious macros detected – 417
- Macros signed – 37
- SANS Securing the Human training complete – 5,141

Important Information

SANS Securing the Human Online Training: Don't forget that everyone is required to take the SANS Securing the Human online training. Anyone with an ACID who has access to the DPS system is required to take the training. If you haven't completed it then please do so before the end of the month.

Cyber Security Awareness Training Officer: For those who don't know, I am also a pilot in the Texas Army National Guard. Last week I got notified that I will be deploying in a few months. This means that my duties and the **newsletter** will have to be split between Cyber Security team members while I am gone.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber.**"

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.