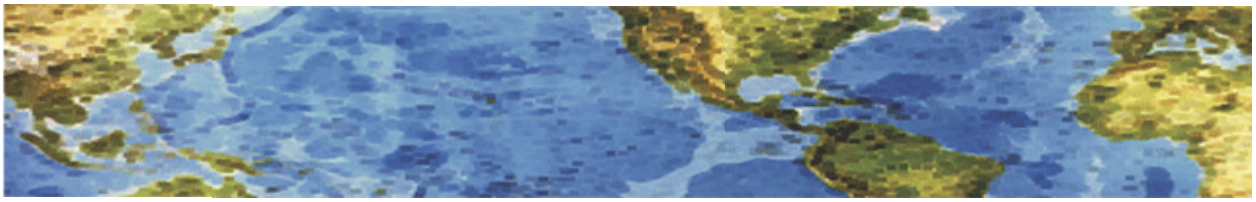
HALL ASSOCIATES



Risk-Based Decision Making Commentary
11 June 2013 Newsletter

Can Your Car Be Hacked??

You might be behind the wheel, but increasingly, computers control your car's every function. Microprocessors direct braking, acceleration and even the horn these days. There can be anywhere from 30 to 40 microprocessors in most cars and even up to 100 different ones running different functions in some vehicles. But could a hacker compromise these systems? Recently, several news reports have raised the issue of car-hacking risks, including: *Vehicle disablement.* After a disgruntled former employee took over a Web-based vehicle-immobilization system at an Austin, Texas, car sales center, more than 100 drivers found their vehicles had been disabled or their horns were honking out of control.

Tire pressure system hacking. Researchers from the University of South Carolina and Rutgers University were able to hack into tire pressure monitoring systems. Using readily available equipment and free software, the researchers triggered warning lights and remotely tracked a vehicle through its unique monitoring system.

Disabling brakes. Researchers at the University of Washington and University of San Diego created a program that would hack into onboard computers to disable brakes and stop the engine. The researchers connected to onboard computers through ports for the cars' diagnostic system.

Is your car at risk? Most of the danger right now may come from hackers who want to demonstrate their prowess and enhance their reputations. And the increased reliance on wireless systems makes your car more vulnerable to these attacks.

Protect your car from hacking. Security is largely in the hands of auto manufacturers, who are working to address concerns. In the meantime, you can take these steps to protect your vehicle:

1. Ask about wireless systems. Familiarize yourself with the wireless systems if you're purchasing a new car. For a car you already own, you can review your manual or check online. Find out if any of the systems can be operated remotely.

2. Go to reputable dealers and repair shops. It's possible for unscrupulous garages to manipulate your car's computer systems, making it appear you need repairs that aren't actually warranted. Don't cut corners when it comes to choosing a dealer or repair shop.

3. Protect your information. Of course, locking your car is always wise. And if you use OnStar -- the GM-owned auto security and information service -- make sure you don't leave OnStar-related documents or your password in the car. Since OnStar can remotely shut off your engine if you report the vehicle stolen, there's the potential for mischief if your password falls in the wrong hands.

4. Be cautious about after-market devices. After-market car systems may not be as rigorously tested or designed, opening you to vulnerabilities.

You can compare the use of computers in cars to the development in our use of personal computers. Hacking exploded when the Internet evolved, making it easy to access computers via networks. Wireless connections mean your car is no longer a closed system. Once you have connection to vehicles, you have an entry point for people to try to access. The only thing standing in their way now is a standardized piece of software. It's a concern we need to address. ***http://us.norton.com/yoursecurityresource/detail.jsp?aid=car_computer***

To subscribe or unsubscribe from this newsletter, send an e-mail to halld105048@yahoo.com.

HALL ASSOCIATES

5 Social Media Scams

We're wired to be social creatures. Facebook draws 175 million logins every day. But with this tremendous popularity comes a dark side as well. Virus writers and other cybercriminals go where the numbers are -- and that includes popular social media sites. To help you avoid a con or viral infection, we've put together this list of five social media scams.

5. Chain Letters

You've likely seen this one before -- the dreaded chain letter has returned. It may appear in the form of, "Retweet this and Bill Gates will donate $5 million to charity!" But hold on, let's think about this. Bill Gates already does a lot for charity. Why would he wait for something like this to take action? Answer: He wouldn't. Both the cause and claim are fake. So why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others. Break the chain and inform them of the likely ruse.

4. Cash Grabs

By their very nature, social media sites make it easy for us to stay in touch with friends, while reaching out to meet new ones. But how well do you really know these new acquaintances? That person with the attractive profile picture who just friended you -- and suddenly needs money -- is probably some cybercriminal looking for easy cash. Think twice before acting. **In fact, the same advice applies even if you know the person.** Picture this: You just received an urgent request from one of your real friends (or a relative) who "lost his wallet on vacation and needs some cash to get home." So, being the helpful person you are, you send some money right away, per his instructions. But there's a problem: Your friend never sent this request. In fact, he isn't even aware of it. His malware-infected computer grabbed all of his contacts and forwarded the bogus email to everyone, waiting to see who would bite. Again, **think before acting**. Call your friend or relative/family member. Inform them of the request and see if it's true. **Next, make sure your computer isn't infected as well**.

3. Hidden Charges

"What type of STAR WARS character are you? Find out with our quiz! All of your friends have taken it!" Hmm, this sounds interesting, so you enter your info and cell number, as instructed. After a few minutes, a text turns up. It turns out you're more Yoda than Darth Vader. Well, that's interesting … but not as much as your next month's cell bill will be. You've also just unwittingly subscribed to some dubious service that charges $9.95 every month. As it turns out, that "free, fun service" is neither. **Be wary of these bait-and-switch games.**

2. Phishing Requests

"Somebody just put up these pictures of you drunk at this wild party! Check 'em out here!" Huh?? Immediately, you click on the enclosed link, which takes you to what looks like your Twitter or Facebook login page. There, you enter your account info -- and a cybercriminal now has your password, along with total control of your account. So both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social site. You've just been had. To prevent this, make sure your Internet security includes antiphishing defenses and think before you act. Only go to your social media page by typing in the URL or using your favorites link. Don't click on an e-mail link.

1. Hidden URLs

Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer. URL shorteners can be quite useful. Just be aware of their potential pitfalls and make sure you have real-time protection against spyware and viruses. Bottom line: **Sites that attract a significant number of visitors are going to lure in a criminal element, too.** If you take security precautions ahead of time, such as using antivirus and anti-spyware protection, you can kinda defend yourself against these dangers.

http://us.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams