

Cell Phones the Next Big Target for Hackers

September 19, 2011 â€“ We all know that computers can be easily hacked. Thatâ€™s the primary reason for telling our readers regularly that they shouldnâ€™t be storing sensitive data on laptop computers and that they need to have secure, hard to crack, passwords. But what we havenâ€™t talked too much about are cell phones. That changes right now because cell phones are becoming the new darlings for hackers.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

You may not think of your cell phone as a powerful computing device. Just keep in mind that even the most basic cell phones on the market today possess more computing power than the Apollo rockets we used to put a man on the moon. They are not as powerful as desktop or laptop computers, but they are a lot more powerful than any computers that were available in the 1990â€™s. And they are catching up fast with their more powerful cousins in terms of both usefulness and capability.

Millions of people today use their cell phones to check e-mail, surf the web and run powerful business applications. Many under the age of 30 use their cell phone as their primary computing device and only use a larger laptop or desktop when they absolutely have to. This switch in usage patterns is what is driving many hackers to change their focus.

To give you an idea of what is at stake, banks are now running advertising for mobile applications to deposit checks, pay bills and move money around in various accounts. There are brokerage applications for cell phones, credit card applications, etcâ€¦ The list is virtually endless. This means that if a hacker can break into your phone and steal information on your bank accounts, that hacker may be able to clean out your accounts and get away with the money without ever having to come into contact with your phone.

The internet browsers on cell phones are also a point of vulnerability. As with their computer based cousins, these browsers can store sensitive information like passwords and your browsing history. If you log onto your PayPal account and the password is saved, a hacker may be able to get his hands on your account information. And if you lose your phone, anyone who finds it may be able to use that information to rack up charges on purchases that youâ€™ve had nothing to do with.

Because of their rapid growth in the market, Android based phones are currently the most popular target of hackers. But any phone can be vulnerable. There are however things that you can do to make yourself less vulnerable.

Don't store passwords on your cell phone. As convenient as it may be to avoid typing in your user name and password every time you visit a particular website, if you are storing this information on your phone you are only asking for trouble.

Don't store sensitive files on your cell phone. These phones can now store virtually any type of file. If you are keeping tax files, or spreadsheets with sensitive information on them in your phone, you are vulnerable. If you do need to store this type of data on your phone for a short period of time, make sure that the files are encrypted and have strong password protection. And remove them from your phone as soon as they are no longer needed.

If you install third party applications on your phone, only get them from a trusted source. Some hackers are using software known as malware to gain access to cell phone data. Once malware is installed on your phone, it could give a hacker access to all of your passwords and every file stored on your phone, including your pictures. The hacker can even potentially monitor your calls and any future activities that you conduct on your phone.

If you sync your phone with a computer, you also want to make sure that the software you install on that computer is also from a trusted source. If it is not, then the next time you connect your phone to your computer, the computer can be used to infect your phone with a virus or malware. Also, any computer that you connect your phone to needs to be regularly swept for viruses using a good antivirus program.

The bottom line here is that the same protocols used to protect data on computers should also be used in conjunction with cell phones. Not doing so could cost you both time and money.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#).

Registration is easy and free.

Follow me on Twitter: