Memphis IT Solutions
IT support that fits

TECH PIECES

☎ 901.457.4230
www.MemphisITSolutions.com

MARCH
2016
In this issue...

Denys Prykhodov / Shutterstock.com

Apple's Wi-Fi Assist might be increasing your phone bill

Over the last few months, iOS 9 has received some negative media coverage surrounding its Wi-Fi Assist feature.

Wi-Fi Assist automatically switches your iPhone to cellular in the event of a weak or unreliable Wi-Fi connection. This switch should provide a stronger connection to keep your online presence unaffected. However, this can have an unintended consequence on your phone bill.

Since you're switching over to cellular, you will use more data than if you were on Wi-Fi. On Apple's website, you will see this:

> *Because you'll stay connected to the internet over cellular when you have a poor Wi-Fi connection, you might use more cellular data. For most users, this should only be a small percentage higher than previous usage.*

The key part to remember here are the words "for most users." You see, for those smartphone users who download apps as much as they breathe air or stream a never-ending supply of YouTube videos, Wi-Fi Assist is not a good idea. This feature will deliver you a phone bill that is double the amount you're used to paying.

Macworld says it's probably better just to turn it off. To do this, go to Settings, Cellular, and then scroll down to the very bottom of the page to tap off Wi-Fi Assist.

However, if you're willing to leave the feature on, then you might want to consider restricting the apps that can use cellular data. In the same Cellular tab, scroll down to tap off the apps that tend to barrel through the most data like Netflix and Spotify. After doing this, you might fall into the "small percentage higher" category that Apple refers to in their statement.

Oksana Kuzmina / Shutterstock.com

4 Smart Toys with Serious Security Flaws

Toys aren't just toys anymore – they're smart, connected and potential victims to hacking and security breaches. And this threat means more than simply creating an all-access pass to your children; it can put their identity (and even their location!) at risk.

Toys offer smart capabilities starting around age three – hardly the age of a security expert. Is your young child using a smart toy? If so, here are four toys that have recently been victim to a hacking:

1. VTech Digital Toys

VTech – the maker of child-friendly, high-tech devices – serves as a recent example of the security holes in smart toys. Almost five million parent accounts and over six million kid profiles were hacked, leaking private information and exposing children to potential threats. The names, addresses, passwords, genders, birthdates, and photos of millions of children were stolen. In the wrong hands, this information could lead to some serious issues.

2. Hello Barbie

Much like Siri or Google Now, Hello Barbie uses voice recognition software and artificial intelligence to provide a call-and-response function. A corresponding app connects the toy to Wi-Fi, making it a potential risk for hackers. What's disturbing is that Barbie is always listening and always on call for the next response. And just where does all this back-and-forth between Barbie and your child go? Into the cloud. And just how secure is the Barbie cloud? Hopefully we'll never have to find out.

3. herO GPS Watch

This GPS watch connects to a parent app to provide real-time tracking. The parent app allows you to establish geo-fencing boundaries and to set up instant alerts that notify you and your child when an unsafe location is nearby. The problem with this is that if the parents know the child's location, so could just about anyone else with the right skillset. Hackers have already found vulnerabilities in herO accounts and were able to gain access to every family member's location and location history. They could even manipulate notifications. Suddenly, an unsafe location is safe. How does that make you feel?

4. Smart Toy Bear

This smart bear has a serious bug that's anything but adorable. Hackers have discovered a vulnerability that allows them to access basic information like names and birthdates—but that's not all you should be worried about. This Fisher-Price smart toy can talk to your child, listen to what your child says, and learn all about your child from a connected smartphone application. If hackers have already found a vulnerability that should be relatively easy to avoid, what's not to say that hackers aren't listening to your child right this very second?

3 Reasons to Love Dome Alert

Save your home from fire, flooding, carbon monoxide and freezing temperatures with a simple smart system that keeps you connected and protected. Get real-time alerts, immediate rescue response and non-stop connection with easy DIY setup and without the hassle of long-term contracts. Here are three reasons Dome Alert is everything your home has always wanted and more.

2 sensors + 1 hub = 24/7 protection

One sensor detects floods and freezes and the second sensor detects fires and carbon monoxide leaks. These two sensors combine to give your home seamless, 24/7 protection. To top things off, the installation of these three elements is so simple that any person can do it themselves. The fire/CO sensor attaches to the ceiling to listen for alarms emitted from your smoke detector, and the flood/freeze sensor can be placed anywhere on the ground, preferably near a potential flood risk like the dish washer. After proper installation, the sensors communicate with the hub to deliver around-the-clock protection.

Pays for itself

Since many in-home alarm companies charge hundreds of dollars for installation, this 15-minute DIY set-up is a huge cost saver. Not to mention, you'll save money with an average home insurance discount of about 10 percent, freedom from long-term contracts, and of course, there's that whole benefit of preventing a home disaster.

Smarter disaster prevention

The Dome Alert system is connected via Wi-Fi, allowing it to send information to the corresponding app if a sensor is triggered. Get immediate text or email alerts so you can respond quickly to potential damages. And if an alarm is activated, you can turn it off, contact first responders or call a neighbor – right from the app.

domealert.com

Syda Productions / Shutterstock.com

4 quick tips to make your coworkers like you more

What would it be like to be the most popular person in the office? The one coworker that everyone likes and no one can ever chastise? While this probably wasn't a dream of yours as a child, it can be a reality of yours as a working adult, and here's how.

Help your coworkers out.

If you want your coworkers to like you, then you need to do something they actually like. And what's something that most people like? Help. If you ever have free time during the workday or you feel that one of your coworkers simply has a lot going on, then offer up your assistance. Helping someone out even once can drastically change the way that person perceives you, as well as how your other coworkers perceive you. And even if they don't accept your assistance, they'll still appreciate the notion.

Show some interest.

People like to talk about themselves, and if you want your coworkers to like you, then you need to remember this. Ask your fellow office mates how things are going, what projects they're working on, and if they have any ideas they'd like to bounce off you. Make this a daily part of your workday, and your coworkers will start treating you differently—as a friend, as a confidant, and as a trusted ally.

Be mindful of time.

If you want people to dislike you, then ignore the idea of time. Be 15 minutes late to work, trickle into meetings after everyone else does, and leave work 10 minutes early. Not only will your coworkers dislike you, but they might even try to get you fired. And although being sensitive of time might not be a reason to like you, it will at least keep you from being the most despised person in the office.

Do something nice.

Every so often, go out of your way to do something nice for your coworkers. Bring donuts to work for your department, take a coworker out to lunch, or send everyone a random, motivational card. The key to this is to do it enough for people to know that you're "just that kind of person" and not too much where people start to expect a monthly treat from you.

Internet's Infamous: Hackers Who Have Made Cyber History

From ruthless cyber criminals to creative hacktivists, the digital realm has seen its fair share of online geniuses who can hack their way into even the most secure corners of the internet. Think your information is safe from prying eyes? Think again. After reading about these infamous hackers, you'll be questioning everything you've ever known about online security.

Kevin Poulson

Poulson overrode the LA-based KIIS-FM phone lines to guarantee he was the 102nd caller and the winner of a new Porsche. He didn't win the car, but he did win a prison sentence. Poulson is now a news editor at Wired.com.

George Hotz

Ever jailbreak your iPhone? Thank George Hotz for that. He's the hacker known for unlocking this popular smartphone, allowing it to be used with other carriers. He also reverse-engineered the PlayStation 3 console, leading to a settled lawsuit with Sony.

Albert Gonzalez

The mastermind behind one of the largest frauds in history, Albert Gonzalez, stole $170 million via credit card fraud from BJ's Wholesale Club, DSW, Office Max, Boston Market, Barnes & Noble, Sports Authority, TJ Maxx, and Dave & Busters. Gonzalez is currently serving a 20-year prison sentence, due for release in 2025.

Gary McKinnon

In 2002, Scotland native, Gary McKinnon, successfully shut down 2,000 computers, gained access to 97 US military and NASA computer systems, and deleted a significant amount of critical files. All under 24 hours. Considered one of the largest military hacks of all time, McKinnon's extradition order is still being argued over to this day.

Michael Calce

Known as MafiaBoy, Michael Calce shut down some of the largest websites with massive denial-of-service attacks. Some of the websites he victimized included the likes of Yahoo, Dell, CNN, Amazon, Fifa and eBay.

Syrian Electronic Army

This hacking group first formed to support Syrian president Bashar al-Assad, but now they are known for cyber-attacks in defense of Syria. They have targeted organizations that are neutral to the conflict in Syria, as well as government websites in Europe, the Middle East, and the United States. The SEA uses website defacement, malware, spamming and phishing to openly attack their enemies.

Anonymous

Known as a group of hacktivists, Anonymous is arguably one of the most well-known hacking networks of the century. Their most notorious hacks have targeted the Church of Scientology, ISIS, government agencies and Westboro Baptist Church – earning them nicknames like "digital Robin Hoods" and "freedom fighters." But their critics see them as cyber terrorists, as their cyber-attacks also include major corporations like PayPal, MasterCard, Visa, and Sony.

oneinchpunch / Shutterstock.com