Tech Solutions INC.
Managed Services
Computer Consulting
Network Administration

TechPoints

November Newsletter 2012

In This Issue

---

4 Easy Ways to Keep Your Computer Safe

Most of us don't think about computer security until our desktops and laptops are suddenly infected by viruses. When we can't log onto the Internet or access our email messages because of malware, we suddenly wish we had taken the steps to protect our computers.

The good news is that protecting your computer is a relatively easy task. It mostly requires some common sense and a few quick fixes.

Business Insider recently provided some suggestions for computer users who want to boost the safety of their machines.

1. Turn off Java
Business Insider led with this for a reason. Java, software that runs interactive functions on some web pages, often opens the doors to hackers. Business Insider cited the 700,000 Apple computers that were —earlier this year—infected with the Flashback Trojan malware. All of the computers were running out-of-date versions of add-ons that let their web browsers run Java.

Turning off Java requires different steps depending on what browsers you are running. If you need assistance, check your browser's Help section. (Or get in touch with us.)

2. Stay current with all software updates

Busy computer users sometimes forget to check their operating systems for updates. This can be a key mistake: Updates often include protection from the latest viruses. If you ignore software updates, you might be leaving your computer vulnerable to hackers.

If you work on a Mac computer, your updates will be delivered through a system called Software Update. PC software updates come from Windows Update.

3. Lock your computer
Business Insider recommends, appropriately, that computer users lock their computers when the machines are sleeping. Doing this requires that you create a password that users must type in to access your computer.

This might seem like an inconvenience. But, as Business Insider points out, what if someone steals your laptop? If this thief can access your computer without a password, the criminal could easily rummage through your personal files and information.

4. Change your passwords
Business Insider recommends that you change your passwords every month. The site also advises you to create passwords that are difficult for others to guess, like ones that contain letters, numbers, and symbols.

Read more at Business Insider.

Top ↑

Protecting Your Mobile Devices While Traveling

We take our offices with us when we travel, toting tablets, laptop computers, and smartphones as we meet with clients across the globe, attend seminars hundreds of miles from our offices, and train new employees in remote locations.

Our mobile devices allow us to scan the web, send and receive emails, access PowerPoint presentations, and work on company reports while we're on the road.

That's the good news. The bad news? Our mobile devices can also put our businesses at risk. What happens if you lose one of your devices while on the road? How much sensitive company information will you put in the hands of outsiders?

Fortunately, the staff at Smallbiz Technology provide some important strategies that businesspeople can use to protect their mobile devices while on the road.

Protect the device

The best way to keep your company's information and data secure? Don't leave your tablets, smart phones, or laptops out of your sight. Always know where these devices are when you are traveling. Smallbiz Technology recommends that you store these devices in a safe when you're staying in a hotel room.

Turn to the cloud
The cloud provides business travelers with a secure place to store their company's reports and sensitive data. This way, even if someone steals a traveler's laptop or tablet, they won't find any sensitive information stored on the device. Of course, business travelers must make sure to limit access to their cloud storage with a difficult-to-guess password.

Login passwords are your friends
Smallbiz Technology recommends that business travelers protect their devices with login passwords. This way, if someone steals their device, this thief won't be able to access the files stored on it unless they crack the password that allows them to log onto the device.

This means, of course, that business travelers must create complex passwords that consist of letters, numbers, and special characters.

Unfortunately, there is no way to completely protect your mobile devices while taking business trips. However, those travelers who follow these three simple rules will at least make it less likely that their tablets, laptops, or smartphones will fall into the wrong hands.

Read more at Smallbiz Technology

Top ↑

It's Time to Disable Java on Your Computer

Want to protect your computer from hackers? Slate technology writer Will Oremus has one suggestion: disable Java.

If you don't know, Java is software that runs interactive functions on some web pages. The software has also been roundly criticized for being an open door of sorts to hackers. In a recent story, for instance, Business Insider pointed to the 700,000 Apple computers infected earlier this year with the Flashback Trojan malware. All of these computers were running out-of-date versions of add-ons that let their web browsers run Java.

The best way, then, to protect your computer? Oremus says it's all about disabling Java.

Security flaw
Hackers recently found a flaw in Oracle's Java software that allowed these cyber criminals to break into

users' computers and install malware. At the time, the threat was considered a "zero-day" one, meaning a threat that exploits a vulnerability that wasn't previously known and for which no fix is available.

Since the security hole was discovered, Oracle released a new version of Java that the developer says fixes the vulnerability.

But the fact remains: Hackers frequently use Java to break into users' computers. Turning it off, then, makes the most sense, especially since Java is no longer needed for the vast majority of websites.

Turning off Java
Turning off Java requires different steps depending upon what web browser you use.

For instance, as Oremus writes, in Firefox users must first select "tools" from their browser's main menu. They should then click "add-ons" and the disable buttons next to any Java plug-ins.

Safari users must first click "Safari" in the main menu bar and then "Preferences." Once they've done this, they can select the "security" tab and make sure that the button next to "enable Java" is not checked.

Google Chrome users need to type "Chrome://Plugins" in their browser's address bar. They can then click the "disable" button listed below any Java plug-ins.

Don't touch JavaScript
Here's a warning, though: Java and Javascript are not the same thing. If you mistakenly disable Javascript on your computer, you won't do anything to protect yourself from hackers. However, you might make it so that the websites you visit no longer work properly.

Read more at Slate.

Top ↑

Don't Bust Your Budget While Traveling with a Smartphone

You wouldn't think of traveling around the globe without your smartphone. After all, that little device can help you quickly change plane reservations, find the trendiest new restaurants, and determine just how busy the highway to your hotel is.

However, there's one problem: Using your cell phone outside the United States can cost you big bucks.

The pain of international texting
The New York Times' Frugal Traveler blog recently covered the outrageous costs that smartphone users might encounter when traveling abroad.

Among them? How about 50 cents for every text message you send or receive? Then there's international roaming rates that can soar to $2, $3, or $5 a minute. It could cost you $15 to retrieve a megabyte of data through your smartphone, according to the blog post.

Fortunately, there are ways travelers can save when traveling. And the Frugal Traveler blog was kind enough to list some of them.

Stay disconnected
Of course, the easiest way is to stay disconnected to your cell phone during your trip overseas. The problem is, that's easier said. As the blog points out, many international hotels no longer have in-room phones. And pay phones are becoming scarce across the globe.

A more practical solution might be to rely on your hotel's free Internet connections or on Wi-Fi networks to check emails and send messages. Of course, even if your web browsing and email activity is free, phone calls can still be a problem. A solution? Set up an account with an app such as Skype or Google Voice so that you can make your calls. This won't be free, but as the Frugal Traveler blog says, it's far less costly than making standard roaming calls on your cell phone.

In general, expect to pay one-tenth the price of a standard cellphone plan when you're relying on services such as Skype and Google Voice.

International SIM cards
If your phone allows you to use other providers, your best bet while traveling abroad might be to purchase an international SIM card. The Frugal Traveler tried Telestial's Passport card for $19 and OneSimCard's Standard card for $30. Both worked well while the blog's author traveled. Both will give you a main phone number that's not from the United States.

Read more at the New York Times.

Top ↑

The Worst Data Security Breaches in History

We all like to think that the companies that have our credit-card information—the banks, entertainment companies, and government agencies—are able to protect our valuable information.

Unfortunately, that isn't always the case.

CSO Online recently ran a list of some of the worst data security breaches of the 21st Century. And if you want to worry about the safety of your financial and personal information? This list gives you plenty of cause.

TJX Companies
For instance, the list covers the December 2006 security breach suffered by retail giant TJX Companies in which the credit-card information of 94 million customers was exposed.

There are two theories about how this security breach happened. One view is that a group of hackers took advantage of a weak data encryption system and stole credit-card data during a wireless transfer between a pair of Marshall's stores in Miami. A second theory is that hackers broke into the TJX network through kiosks inside actual stores that allowed people to apply for jobs.

The upshot? Albert Gonzalez, a legend in the hacking community, was arrested and sentenced to 40 years in prison for the scheme.

Department of Veterans Affairs
In May of 2006, hackers stole an unencrypted database with the names, Social Security numbers, birthdates, and disability ratings for 26.5 million Military veterans, active-duty military personnel, and spouses.

The database was, amazingly, stored on a laptop and external hard drive that were both stolen from the home of an analyst with the Veterans Administration.

This case ended with a fairly happy ending as an unknown person returned the stolen laptop and hard drive about a month after the theft.

Sony's PlayStation Network
PlayStation Network suffered what is still viewed as the worst gaming community data breach ever in April of 2011. Hackers compromised the accounts of 77 million PlayStation Network accounts, and Sony reportedly lost millions of dollars by shutting down the site for a month.

Sony says it has still not found the source of this hack, but as CSO Online says, the hackers gained access to full names, passwords, email addresses, home addresses, purchase histories, and credit-card numbers of PlayStation Network gamers.

Read more at CSO Online.

Top ↑