

TECHNOLOGY TIMES

“Insider Tips To Make Your Business Run Faster, Easier And More Profitably”

5 Ways To Safely Shop Online

Have you ever made a purchase online? The vast majority of people who regularly use the Internet have. E-commerce has become so popular and convenient that many people have come to prefer it to more traditional shopping. Those who eschew the idea of buying stuff online tend to do so because they view the various platforms as not being secure enough, and therefore putting highly profitable information, such as credit card numbers, at risk. If you do shop online though, there are some precautions you should take.

Below are five ways to ensure that e-commerce transactions remain secure:

1. Watch what you share

Many security experts continually want this for social media usage, but it is also relevant to e-commerce. Often, when you make an online purchase you will be asked to provide some personal information. This might include your shipping and billing address, birthday, etc. Did you know that many sites will often ask for more information than they really need to complete the order?

The reason companies ask for this additional information is often so they can get to know you better, and provide more relatable, targeted product recommendations. Some dubious sites may ask you for this information and later sell it to a third party. When purchasing online, you should be aware of what information that is required – usually indicated by an asterisk – and what isn't. In order to remain as secure as possible, only share information that is absolutely necessary.

Beyond that, if you are planning to link a digital wallet to your mobile phone, you should be careful who you share or lend your phone to. These services are set to take off in a big way, and there has already been instances of people with digital wallets being duped by strangers asking to borrow their phones in order to find their wallet. It is a good idea to restrict wallet access and not store any valuable information on your phone's hard drive. Instead, store it on a password protected cloud storage site.

Continued on Back Page...



“Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere”

- Rick Johnston,
Information Management Systems

August 2013
Fargo, ND

Inside This Issue...

5 Ways To Safely Shop Online.....	1
A New Favorite Way Hackers Are Gaining Access To Your PC...	2
Shiny Gadget Of The Month: It Really Is Quite Shiny.....	3
10 Ideas You Need If You Want To Succeed.....	3
The Lighter Side: Did You Know?.....	4



*Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY!***

A New Favorite Way Hackers Are Gaining Access To Your PC

Do you have Java turned on in your web browser? If your answer is “Yes” or “I’m not sure” then it’s time to take action to find out. Why? The biggest threat to your computer systems in 2013 (and beyond) is no longer Microsoft Windows - it is Oracle Java.

After 20+ years as the poster child for insecure software, Microsoft’s newest operating systems (Windows 7 and 8) have gotten their act together. Cybercriminals like to get the greatest bang for their buck and therefore they’re attacking the Java platform because of its huge market share and because it’s an easier platform to hack than the Microsoft operating system. Java is now installed in over 1.1 billion desktops and 3 billion mobile phones. That’s a big target that is very attractive to hackers. Hackers also love that Java is multi-platform, which



means it’s capable of corrupting PCs running Windows, Mac OS X or Linux. And since many Mac users don’t have anti-virus, hackers were able to infect over 600,000 Macs with serious malware via the Java software installed on their machines.

Right now, cybercriminals are aware and exploiting any security flaws in Java that could lead to infections on your computer. There are even automated kits now available to capitalize on any security hole found within days, if not hours

of them becoming known. It’s not unusual to see hackers use Java as a first attack to weaken the defenses before serving up an Operating System specific attack. Even the Department of Homeland Security suggested that “To defend against future Java vulnerabilities, their users should consider disabling Java in web browsers.”

Here are 3 steps you can take today to minimize your risk:

1. Disable or uninstall Java **wherever you can.** *If you don’t need it, remove it.*
2. Where Java is necessary, use a separate web browser only used for Java based websites and be sure to patch Java regularly.
3. Have your staff report the first signs of slowness, possible infections and web browser popups to your IT contact as soon as they happen.

How To Pick A Good Password

What’s the most common password? You guessed it...”password.” Obviously this is not the best way to protect yourself against hackers and online thieves. But even if you don’t use the word “password,” you might be using an equally easy password to decipher.

We suggest you DON’T use the following passwords for really important web sites, such as your online banking web site or other financially related sites.

- Your name or your spouse’s name
- Your pet’s name
- The last four digits of your Social Security number
- Your address
- A single word that would appear in a dictionary.
- Your children’s names
- Your birth date
- Your phone number
- A series of consecutive numbers, such as “1, 2, 3, 4.”

Your best bet for creating a strong password: Use combinations of letters, numbers and special characters.

Shiny New Gadget Of The Month:



IFI (I Found It)

This day and age we have so many electronics to keep up with. Now there's a simple way to track where you've left them and keep them from getting stolen.

The iFi Systems Smart Tags work like a two way pager between you and your valuables. The iFi utilizes a Bluetooth connection through an app on your iPhone or Droid device. It can easily be attached to a handbag, camera case, or just about anything else you'd like to protect. These Smart Tags can also act as a handy reminder that you've forgotten something or, worse, that your valuables are walking off with an opportunistic thief!

You can attach multiple tags to multiple items and check the status of each one directly from the home screen. You can customize the names and the alert sounds for each item individually, and you can even monitor battery life via your smartphone. Can't find the phone you say? Simply use your tag to track it. The communication system works both ways.

iFi Systems Smart Tags come in both iOS and Android models and the associated app can monitor up to 6 different items at a time. It gives a Google map of where a tag was at the time of separation. You can also set up safe zones, like when you're at your office, so you do not have to endure alerts every time you walk to the water cooler. Get yours at www.amazon.com So if you want to keep your belongings safe, primarily from yourself, get some iFi Smart Tags. Around 30 to 35 bucks, depending on your operating system, from ifisystems.com

10 Ideas You Need If You Want To Succeed

1. Do what you need to do now so you will eventually get to do what you want to do later.
2. Discipline is the ability to get things done regardless of how you feel about doing them.
3. Passion only pays off when channeled into productive effort.
4. Others may believe in you, help you and support you, but ultimately nobody will do it for you. You are responsible for your own life.
5. If you don't do your job any differently than anybody else who does it, you won't get paid more than anybody else.
6. More often than not, you succeed in spite of not because of your circumstances.
7. If you think a little better and work a little harder you will always accomplish more than others.
8. If you can't control it, get over it.
9. If you don't appreciate where you are at, you won't appreciate where you are going.
10. Get clear on what really matters to you and then get busy pursuing it.

If you want more insights into how to turn the ordinary into the extraordinary, go to Mark's site at www.marksanborn.com

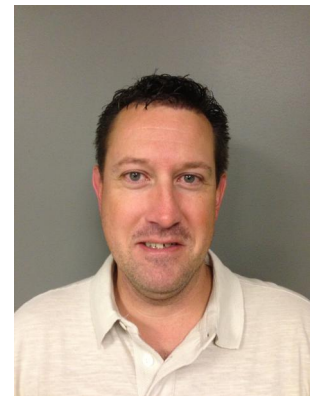


Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international bestselling author and noted authority on leadership, team building, customer service and change. Mark is the author of eight books, including the bestseller *The Fred Factor: How Passion In Your Work and Life Can Turn the Ordinary Into the Extraordinary* which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com

Consultant Spotlight:

Neil Schmidt

Neil Schmidt has joined IMS as a consultant. He has over 12 years of experience working in nearly every phase of IT service and support. Neil holds degrees in Microcomputer Specialist from NDSCS and Management Information Systems from NDSU.



In Neil's spare time he enjoys spending time with family and fishing.

Continued from Front Page

2. Watch how you connect

People are using their phones, tablets and laptops for online shopping in an ever increasing number. This is largely because the devices are convenient and portable – you can shop from wherever you may be. But, what many people fail to realize is that they are connecting to public Wi-Fi if they are on the go. Sure, it is cool to be able to buy your groceries on Amazon from the coffee shop at lunch, but if you have connected to public Wi-Fi, your information is likely wide-open – anyone with the right tools can access it.

You need to be careful when you shop. Don't enter any valuable or important information like passwords and credit card numbers while connected to public Wi-Fi. If your mobile device has a data plan, switch to that instead. Or, wait until you are connected to a secure network.

3. Verify all sites

When you are shopping online you should verify that the site is in fact legitimate. The easiest way to do this is to take a look at your browser's URL bar, and more specifically the website's address. You are looking for it to start with, https://. What this indicates is that the website has been authenticated as being legitimate. Most websites like Amazon, Google, Apple, Facebook, etc. all have https protocols. If you don't see this in the address, you may be looking at a fake website.

4. Don't pay with your bank account

One of the benefits of e-commerce is that it is easy. Because of this, the number of users buying stuff online is growing exponentially. Banks are aware of this trend and have launched services that allow you to pay for transactions with your debit card. The problem with this is these cards are directly linked to your bank account, often with higher limits than credit cards. It can be incredibly tough to get money back if something happens, largely because as soon as your account has been debited, the money is gone.

5. Don't link accounts

For convenience, many online retailers like Amazon, Apple, etc. offer to store your credit card number. It is highly recommended that you don't allow these sites to store your credit card numbers, especially if you use the same account name or email address as other accounts.

If you get hacked, and the hacker finds that you have say an Amazon account with the same username and password, they will likely go on a shopping spree, which could cost you time and money.

Taking precautions while shopping online is a good idea, and could help mitigate the risk of having your identity or money stolen.

By: Editor: This entry was posted in General Articles A, Security, News and General and tagged 2013, July 22, Security_A, E-Commerce, Online Security, Online Shipping, QS_3, Secure Online Shopping, Security

The Lighter Side: Did You Know?



- ◆ A can of diet coke will float to the top of water, but a regular coke will sink to the bottom. (Try it.)
- ◆ The fourth richest man in the world (Warren Buffett) still lives in the house he bought for \$31,500 in 1958.
- ◆ The Munich Technical University has a 3-story slide used for students to get to class faster. (See photo above.)
- ◆ The "I'm Feeling Lucky" button costs Google \$110 million each year.
- ◆ There are already more than 250 cryopreserved (frozen) in the hope that someday technology will be invented to revive them to extend their lives.
- ◆ Peanut butter, under high (very, very high) pressure has the probability to turn into a diamond.