NOVEMBER 2014

XperText

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

XPERIENCE THE DIFFERENCE. WE’LL MAKE ALL OF YOUR COMPUTER PROBLEMS GO AWAY WITHOUT THE COST OF A FULL TIME IT STAFF

Here’s A Perfectly Legal Way For You To Save A Bundle Of Money On Taxes While Updating Outdated Computer Equipment … But You Have To Act FAST!

Please forgive me for the headline if it seems a bit “sensational.” I really needed a way to get your attention about a perfectly legal way to save quite a bit of money on taxes while updating outdated computer equipment that is going to quickly pass you by if you don’t act soon.

Thanks to the **recently updated** tax deduction titled “Section 179 election” (see www.section179.org for details), the Federal Government allows you to buy **up to $25,000** in machinery, computers, software, office furniture, vehicles or other tangible goods and take the full expense deduction in the current year, thereby REDUCING your taxable income on your **current year’s tax return**.

It’s important to note that this is significantly less than the 2013 deduction allowances, but is still real money in your pocket! But you have to act now, as once the clock strikes midnight on December 31st, Section 179 can’t help your 2014 profits anymore.

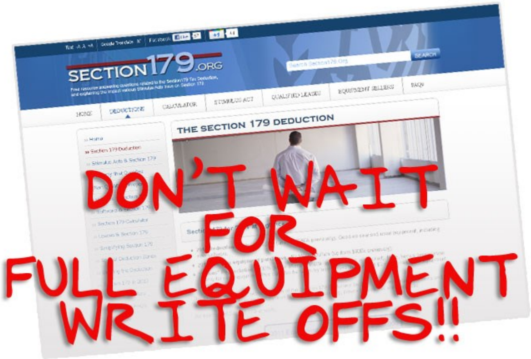
Here’s How XPERTECHS is “Sweetening the Pot”

If you schedule an upgrade for your network with XPERTECHS **before November 21, 2014** we will include:

1. *TWO (2) FULL MONTHS of our XperCARE Proactive Managed IT Service (up to a $3,000 value) absolutely FREE!* All computer networks need ongoing maintenance to keep them running problem-free, and with XperCARE you’ll not only enjoy faster and more reliable service from your computer network, but you’ll gain incredible peace of mind knowing that your network and the data it holds is safe from loss, corruption, downtime, viruses, hackers, spyware, and a host of other problems.

2. We’ll allow you to continue your XperCARE Proactive Managed IT Service at a special discounted rate that will easily save you thousands in IT support! After the two months are up, you can continue to receive regular maintenance, critical updates and security patches, fast, remote support, and 24 x7 watch over your network and data at a discounted rate. Of course, you are under no obligation to continue this maintenance, but I’m certain you are going to want to after you see how we guarantee to keep things up and running.

Call Michael at (410) 884-0225 or go online and sign up www.XPERTECHS.com/upgrade


SECTION179.ORG
THE SECTION 179 DEDUCTION
DON’T WAIT FOR FULL EQUIPMENT WRITE OFFS!!

XPERTECHS®
"Xperience the Difference"

8 Steps To Take Now To Be Certain Your Finances Are Protected Online

Seems like we've been inundated over the past 6 months with rampant cybertheft. Target, Neiman Marcus, Yahoo and even mysterious $9.84 credit-card charges. Unfortunately, in the world we live in, this is most likely the norm going forward and not just a blip on the radar.

While there is no way to absolutely, positively, 100% stay safe online, by taking these 8 steps, you will be as safe as possible.

1. **Only Shop On Secure Websites.** Before you type your credit card into a website, ensure it is secure. Look for "https://" in the address bar of your web browser when you are checking out.
2. **Use A Secure Network For Financial Transactions.** Protect your computer with a firewall, antivirus and anti-spyware software.
3. **Setup Banking Alerts For Unusual Or Large Transactions.** Ask your bank to notify you of any suspicious or large transactions.
4. **Use Credit Cards Instead Of Debit Cards.** Most credit cards offer better fraud protection.
5. **Pick Complex Passwords.** Never use repeat passwords or words in the dictionary for your financial accounts.
6. **Never Directly Answer Or Respond To An Email From Your Bank.** Never rely on links in emails to access your financial accounts.
7. **Install Available Security Updates On Your Computer, SmartPhone and Tablets.** Many cybercrimes target known security holes on your computing devices.
8. **Check Your Bank Balances And Statements Regularly.** Good ol'-fashioned visual checks on your balances and a scan of your transactions are the best practice to be sure that nothing has slipped through the cracks.

Password Security: How Hackers Steal Data & Savvy Users Keep It Safe

Digital security has never been more essential than it has been this year. Cyber crimes are becoming more creative and more devastating. Here are several examples of recent cyber criminal attacks:

- Russian hackers stole 1.2 billion unique password and user name combinations.
- Two US supermarkets announced they too had been hacked. Customers' credit card information was stolen from 180 stores across seven states.
- Hackers targeted the healthcare industry. Over 200 hospitals across the US suffered from a major security breach. The criminals took 4.5 million patient records by exploiting a flaw in a system made vulnerable by the Heartbleed bug.

How Hackers Are Doing It

This latest generation of cyber thieves are spending time and energy creating more tools to cause more attacks. Currently, the most newsworthy method is breaching the security of a major corporation or organization. Unfortunately, there's nothing that the average person can do to protect his or her information from this type of attack.

Hackers also steal their victims' information by cracking passwords. They do this by systematically running through every password possibility. Criminals can narrow down the search using known details about the password or user.

Another popular hacker trick is phishing; when hackers pose as trustworthy companies to trick people into giving up their sensitive account information.

How Users Are Staying Safe

One effective way a user can stay safe from cyber attacks is to revisit password strategies. In order to properly use passwords, one must understand the concept of password strength. IT professionals evaluate the durability of a password by classifying it in terms of bits. In short, the more bits a password has, the stronger it is. The use of symbols, numbers, and case-sensitive letters can substantially improve password strength. A single strong password isn't enough protection, but the best strategy is to use a unique strong password for every account.

Password Managers

Password managers offer a convenient solution for the handling of complex passwords. These applications typically provide features for the generation and storage of passwords. Many password managers also provide automatic password auditing to identify weak or shared passwords. Some even issue alerts in the event that a password is compromised.

Multi-Factor Authentication

Standard authentication, or logging in, relies on a username and password. If an attacker obtains the password associated with a username, they can easily compromise the related account. As its name suggests, multi-factor authentication (MFA) instead relies on multiple pieces of information, providing an added degree of protection.

Typically, MFA requires two pieces of information: something you know and something you have. For example, in order to access your bank account through an ATM, you need something you know (your PIN) and something you have (your card). Similarly, accessing an MFA-enabled account requires not only a password, but also interaction with something you have, such as a mobile phone or digital fob.

Shiny New Gadget Of The Month

Pebble Steel

Pebble Steel does more than just tell the time — this smart watch displays e-mail, text messages, caller ID and other notifications from your favorite apps, reading them straight from your iPhone or Android phone. Pebble cleverly vibrates on your wrist to alert you of incoming calls, meeting reminders or approved notifications. Leave your phone in your pocket as you go about your day-to-day activities.

The long-lasting battery life and the easy-to-use design makes this watch both stylish and necessary in this day and age, and its e-Paper screen makes it easy to see in both direct sunlight and even underwater.

Pebble Steel is available on Amazon.com for $149.99. With this gadget, whose battery can go for a week without charging, the integration of technology in your life will be smoother and much more hands-free.

XPERTECHS®
"Xperience the Difference"

BYOD - Bring Your Own Device

In the consumerization of IT, BYOD is a phrase that has become widely adopted to refer to employees who bring their own computing devices – such as smartphones, laptops and PDAs – to the workplace for use and connectivity on the corporate network.

The BYOD phenomenon is reshaping the way IT is purchased, managed, delivered, and secured. And because it's part of the growing IT consumerization trend, Business leaders can't ignore it. Nor should they want to. From something as simple as allowing workers to access corporate email on their personal smartphone to a full-blown program in which the company subsidizes the purchase of personal laptops, BYOD has the potential to increase worker productivity, create a more flexible working environment, and even reduce IT costs. But BYOD also brings significant challenges. IT must secure data on devices the company may not own. Help desks may need to support a larger selection of devices and operating systems than they currently do. And you may need to develop new policies and procedures for device procurement and management, application deployment, and data ownership.

In the 1980s and 1990s, the PC revolution freed business computing from the centralized world of the mainframe (and its minicomputer offspring), but companies generally retained tight control over the personal computers their employees could use—especially in the earlier "desktop" part of the PC era. As computers became increasingly affordable, mobile, and connected around the turn of the millennium, more and more people began using home computers to work on after office hours.

From this point, it was almost inevitable that the process called "consumerization of IT," which includes the BYOD trend, would occur. After all, who wouldn't prefer to work with a notebook, tablet, or smartphone that they had carefully chosen to fit their own requirements over a device selected according to a set of corporate IT purchasing guidelines?

But consumerization of IT doesn't just mean bringing your own device to work and using consumer apps and services. BYOD also brings significant challenges and you may need to develop new policies and procedures for device management and data ownership. To learn more about BYOD and how it affects your company, call us at (410) 884-0225.

Microsoft® Partner

XPERTECHS Ranked 17th in the Mid-Atlantic Region For Microsoft Partners and Office 365 Integration

Microsoft announced the Mid-Atlantic Regional Partner Award winners at their recent Worldwide Partner Conference in Washington, DC. XPERTECHS was recognized at the 2014 Microsoft US Mid-Atlantic awards, as one of the top 20 Office 365 partners in the region.

Awards were presented in multiple categories, with winners and finalists chosen from a set of more than 200 organizations across the Mid-Atlantic Region. XPERTECHS is honored to be mentioned among the top Microsoft partners for demonstrating excellence in innovation and implementation of customer solutions based on Microsoft technology.

The Lighter Side…

How Balloons Teach Teamwork

Once, in a seminar of about 50 people, the speaker decided to change his presentation to prove a point. He decided to do a group activity. He gave each person a balloon and asked them to write their names on it with a marker.

All the balloons were gathered up and put into a small room. The attendees were all let into the balloon-filled room and were asked to find the balloon with their own name on it within 5 minutes. As expected, everyone was frantically searching for their name, colliding with each other, pushing around others and creating utter chaos.

At the end of the 5 minutes, no one had found their own balloon.

The presenter then asked the attendees to randomly pick up one balloon and give it to the person whose name was written on it.

Within minutes, everyone had their own balloon.

"This is what is happening in our lives," the presenter explained. "Everyone is looking frantically for their own happiness, not knowing where it is."

Our happiness lies in the happiness of others. Give happiness to other people, and you shall find your own.

This is the purpose of human life.

Crypto Locker: What You Need To Know To Protect Your Business

Crypto Locker is a type of computer software malware that began spreading rapidly last fall. Over the past several months, there has been a widespread increase in the distribution of Crypto Locker. It is being delivered via email. Though the messages may seem innocuous, any user or company can be a target, making it difficult to spot.

The biggest threat is users opening emails from unknown senders and then following the instructions and/or clicking links to external sites. It is of utmost importance to instruct your employees and colleagues to follow your email security standards by only opening messages from known senders. Daily virus scanning and remote backup also prove critical to preventing this malware from affecting your business.

Feel free to call us anytime if you have questions about Crypto Locker, or think your computer may have been infected.

Does The Thought Of Your In-House Computer Expert Leaving Scare You To Death?

Most businesses don't think about what would happen if their computer guy suddenly quit. Most business owners think it would only be a temporary inconvenience when, in fact, the opposite is usually true. Want to know how much you are at risk? Ask yourself the following 5 frightening questions:

1. Do you have written network documentation about your computer network? What software licenses do you own? What are the critical administrator passwords to your systems and devices? How is your computer network structured? What hardware do you own and when do your equipment warranties expire? Are there cloud vendors for email, online storage, hosted line of business applications, etc. that you don't currently have? You should NEVER allow a single IT person or company keep this information under their full control over your network and company. If they suddenly left for any reason, this could lead to huge consequences for your company.
2. Do you know where your backup files are stored and if they are being stored properly? Do you have a written plan for restoring your network fast in the case of a disaster? If you don't have a fully tested disaster recovery plan for your office, you could be at serious risk without ever knowing it until something happens.

3. Do you know where all of your software is stored? Taking a minute to organize and store your software in a secure place can save you a considerable chunk of money in the event that you need to restore a program on your systems. If you don't have access to the software or don't know where it is located, you might be forced to buy the software again.
4. Do you know what routine maintenance is being done on your network? If your in-house expert leaves, who will take over?
5. Do you know how to protect yourself from an ugly security breach if your in-house computer expert leaves? What happens if your in-house expert splits with no warning AND has access to your company's network? As soon as humanly possible, you should disable his or her access, including remote access to your network and all cloud-based applications.

So how did you do? If you answered "no" to even one of these questions, you need to get the answers now before it's too late.