Bits & Bytes

Insider Tips On How To Use Technology To Make Your Business Run Faster, Easier, And More Profitably

Technical Action Group Inc
TAG
we're I.T.

Volume V, Issue V May 2013

"As a business owner , I know you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems forever."

Joe Stoll, President
Technical Action Group (TAG)
JStoll@TechnicalActionGroup.com

Inside this issue:

Can Apple MACS Get Viruses?

A very common misconception is that Apple Mac products cannot get viruses. Not true! There is no such thing as a 100% safe computer. Devices running OS X, Windows, Linux, Android or any other operating system are all capable of being infected with a virus or other malware.

However, the likelihood that an Apple Macintosh user gets a virus is much lower than for Windows users. In fact, many Apple users don't even run any antivirus software on their computers. Whether that is a smart strategy is debated by many IT professionals. A few of the reasons why Macs don't get as many viruses as PCs are:

1. Mac OS X is based on the Unix operating system, which is one of the oldest and most secure operating systems around.

2. Microsoft Windows is used by many more people, so it's a bigger and better target. Plus the way that Windows is built makes it easier for viruses to spread across computer networks.

3. Many of the tools designed to create viruses or malware are written for the Windows operating system.

Windows Threats Even For Macs

Many Mac users find themselves having to use Parallels, BootCamp or other virtual software to run Windows only programs such as Microsoft Publisher. Because these Macs are now running a Windows operating system, they are now susceptible to Windows viruses. In addition, an Apple computer can become a "carrier" of a Windows-based virus. This virus would not infect the Apple machine, but could infect other Windows machines on your network if it were to send that virus via e-mail or across the office computer network.

And Even More Threats…

Any software, plug-in or other 3rd party add-on that is installed onto any computer that connects to the internet can introduce its own security risks. One of the most common ways that the "bad guys" are able to attack a Mac is through browser applications and browser plug-ins such as Adobe Flash, Adobe Reader, Java and others. Just about every Mac user has all three of these plug-ins installed on their computers (and many more). These are a necessary part of business, but do introduce additional security risks for all computers.

The Human Factor

Although Apple Macs are less vulnerable to viruses, they are still operated by flawed humans who can still be the victim of Trojan Horses, phishing and other fraud. Your best bet is to keep everyone informed about online security risks, no matter the computer they're using.

Shiny Gadget Of The Month:

Intel Ultrabook Convertible

The Intel-based Ultrabook Convertible is one of the most cutting-edge on-the-go laptops to date. Quite simply, it's a laptop when you need it and a tablet when you want it.

Ultrabook with touch display, using Windows 8, delivers stunning graphics and the ultimate in precision and control. And unlike an iPad or Android tablet, this convertible turns into a powerful laptop in an instant.

Additionally, models with Intel Smart Connect Technology continually update your email and social networks even when your Ultrabook is shut down. You'll wake from sleep mode in less than 7 seconds and already be completely updated so that you can resume what you were doing in the blink of an eye.

And with Intel's Anti-Theft Technology, if your Ultrabook is ever lost or stolen, you can instantly disable the machine from anywhere, ensuring that your data is safe and secure!

Learn more today at

intel.com/Ultrabook

6 Questions You MUST Ask Your IT Support Provider—ASAP

Ugh—I'm shuddering just remembering this appointment….During a recent sales meeting with a professional services firm, I asked them for details regarding their backup system and how data is being taken off-site. "Our current guys are doing a full backup off-site once per week and every night they are doing an incremental backup, so we don't have to be involved whatsoever". Sounds like a good stress-free approach right? **WRONG!**

Just Because Your IT Guys TELLS You Backups Are Done Off-Site, It Doesn't Mean They Are Actually GETTING Done

Upon further investigation on our part we determined that backups were only happening within the office which means that NOTHING was going off-site. So if there was a catastrophic physical disaster such as fire, flood, or theft of their server and backup hard drive, ALL of their data would be GONE. They were very surprised and rightly, concerned because this backup solution was purchased from their IT provider only a few months previous and moved them from a solution where they were taking tapes off-site, to not taking anything off-site. So they invested in this solution THINKING they were protected which in fact it was quite the opposite. How did this happen? We really don't know. Miscommunication in expectations, we assume.

How to Avoid this? Ask your IT provider these SPECIFIC questions

1. What is being backed up.
2. What is the frequency of the backups.
3. What is the backup storage location (i.e. tapes, hard drives, off-site)
4. Is the success and failure of your backups being regularly monitored?
5. Are test data recoveries being conducted at least once monthly to make sure your backup system is functioning?
6. Who's responsible for getting the data off-site? You, or your IT provider?

When both sides have a clear understanding of the answers to these questions, you'll minimize the risk of forever losing your valuable data during a catastrophic event.

Is Microsoft's Cloud Based Office Licensing Model Going To Affect Your Business?

Microsoft announced earlier this year that they are going to place all of their Microsoft Office desktop and cloud-based Office 365 software applications under one umbrella in a renewed effort to push their cloud-based subscription model.

Microsoft will still sell their existing desktop versions, but these will not be as "fully featured" as the upcoming cloud-based versions (note that any Microsoft software that ends in 365 is their cloud based software). It's becoming very apparent that whether you're a home user or a large company, Microsoft wants you to buy the cloud version of their products going forward. If you don't want the cloud version on a monthly subscription, you'll have to settle for a dumbed down version of the product instead.

Here's what this potentially means for you:

♦ The new "Office" family covers all different editions of Microsoft Office, from Student and Home Editions to the most powerful tools that Microsoft offers.

♦ You will never have to worry about buying CALs (Client Access Licenses) for Office 365.

- ♦ Things should be getting easier for you to manage. Whether you are starting from scratch or updating software licenses for your office, you'll be able to get everyone running on Office, Exchange, Sharepoint, Lync, Word, Excel and even Skype under one single license.
- ♦ Microsoft is also preparing a half-dozen bundles for Office and Office 365, many aimed at small business.

Drop Box—Is It Secure For Your Business?

A question that we often get around here is whether or not file-sharing services such as DropBox, YouSendIt and Google Docs are secure enough for business. If you use any of these services for your business, here's the scoop…

Treat DropBox As A Public, Shared Environment.

DropBox (and the others mentioned above) is designed to easily share very large files – ones that are not optimal for e-mail because they're so huge. Examples include videos, audio files, large PDFs and graphics files. These services are typically free (or very cheap), and you shouldn't have the expectation of great security for this price.

But an increasing use of these tools, even for legitimate reasons such as collaboration, is putting a lot of private information at risk. According to a recent Ponemon study, 60% of organizations have employees that frequently put confidential files on services like DropBox without permission. In fact, companies such as IBM have banned the use of these services completely.

When Does Or Doesn't It Make Sense?

When you have a file that doesn't need to be secure and simply needs to easily and quickly get from point A to point B, then DropBox can be a viable solution. On the other hand, you would not send or store any sensitive files, such as contracts or financial statements, on DropBox. These services are also not safe for any files subject to government compliance regulations such as PCI, HIPAA, SOX, Sarbanes-Oxley or HITECH. These file-sharing solutions are NOT compliant.

What To Use Instead

If you need to transfer files outside of your network and need to do so securely, some options to consider are:

- ⇒ Creating a secure FTP site
- ⇒ Use 2-factor authentication rules
- ⇒ Be sure to have audit logs involved to monitor the security of your data.

I bring my computer in from home. Why can't I bring my tech support in from home?
Dad, when are we gonna eat?
IRONIC T-SHIRT
Blazek
©2011 Dave Blazek

Android Tips

ADD A WEBSITE SHORTCUT TO YOUR HOME SCREEN

Have a favourite site? Drop a direct-access shortcut on your home screen for quick access.

1. In the browser, navigate to the site for which you want to create a shortcut.
2. Tap the **Menu** key, choose **Bookmarks** and then **Add.**
3. Tap and hold on the newly created bookmark and choose **Add shortcut to home.**
4. Tap the **home button** to return to your home screen and to see your new quick-access shortcut .

Tip: If the site has a "favicon" (a little image that appears in your browser's address bar), this image will be used in the website shortcut on your home screen.

USE VOICE CONTROL

Speak, and your Android device will listen; dial by voice, pull up a map, send a text or transcribe a note.

- Add the Google Search widget to any home screen.
- Tap the microphone button.
- Speak your online search terms or other voice commands such as "**Navigate to"** followed by the address. "**Call"** followed by the contact name. "Set **alarm**" followed by the time. "**Note to self**" followed by the dictated text. "**Send an e-mail**" to (name), "**subject**" (subject line), "**body":** body of the e-mail.
- On the **Speak Now** screen, tap **Help** for a list of available voice commands

How To Send Virtual iTunes Gift Cards

If you have a family member or friend who has an iPhone, iPad, or iPod touch, buying iTunes gift cards make a nice present or thank you gesture. But, buying physical cards is a whole process unto itself, and there's an easier way. You can easily send people an iTunes gift card virtually from iTunes on a Mac or PC or directly from your iOS device. **Note:** Make sure to update to the latest version of iTunes and iOS on your device.

Send a Gift from iTunes

On Mac or PC, launch the iTunes Store, and click Buy iTunes Gifts under the Quick Links on the left. You'll need to verify your billing info if it hasn't been already.

On the next screen select the amount you want to send. Enter the recipients email address and an optional message. You can have it sent right away or schedule a date in the future.

For a bit of flare you can select a Theme for the card – Celebrations, Birthday, Thank You, or the standard iTunes. Select Next, verify the amount and click send.

Send iTunes Gift from iPhone, iPad, or iPod touch

To send an iTunes Gift from your iOS device, launch the App Store and scroll all the way down on the Featured screen. Tap the Send Gift button, and navigate through the onscreen instructions.

If You Are Still Using Business Cards, Here Are 8 Keys To Using Them Effectively!

At gatherings I sometimes collect business cards. By "sometimes" I mean only if I have a reason to. Believe it or not, I don't put everyone I've ever met on my mailing list. So when I collect a card I either intend to contact that person or (on occasion) I intend to add them to a list.

If you are going to use business cards, here are some key things that will maximize their effectiveness…

1. Your Name (you personally) should be clear and visible and readable from arm's length. That means it is also easy to find. Everyone hates a business card with strange font combinations so you have to scan all over the card to find the person's name. Where's Waldo? Or whoever I'm talking to.

2. Your Company name should be clear and easy to find.

3. Contact information is up to you. Some cards only have e-mail or only have a phone number. It depends on how you want to be contacted. If you want to give your entire mailing address, fax number, and extension that's fine. Decide WHY you would hand out this information and what you really need on that card to fulfill your needs.

4. Company logo and slogan. If you have a nice logo or a slogan that really helps you differentiate yourself, then find a place for them on your card. Remember: They should contribute to the goal of making your card useful and easy to use. If they detract, get them out of the way, make them smaller, move them to the side, or drop them altogether.

5. Titles . . . hmmmmm. Some people need titles. But most of us don't really need titles on our cards. They're just one more thing that needs to be changed if you change jobs. Does a title do something for you? If yes, put it on the card. If not, leave it off. Sometimes we feel obligated to put something on the card for a title. If so, make it descriptive and useful. Or bland and boring. But whatever you do, do it intentionally and not because you feel you need to put something there.

6. Other Information (QR Code, Facebook ID, Fan Pages, LinkedIn, Twitter, Google+, AIM, Pinterest, 4Square, Yelp, Flickr, Reddit, RSS, Technorati, StumbledUpon, Digg, Yahoo Instant Messenger, Jagg, blog, Klout, etc.). I bet you know where this is going. There is simply too much miscellaneous stuff to fit it all on a tiny little business card. So if you want to put something else on there, be picky. Choose a few things that don't take up much space AND that contribute to your marketing goals.

7. Use the back wisely. Or leave it blank. Remember, the back of the card is not for ten little tips, quotations, IP Subnet calculators, etc. The back is primarily for notes. You can use some of the back for links, logos, QR code, etc. But leave at least half of it blank—or lined for notes.

8. Make your business card scan-able. You should have a business card scanner. If not, visit your more successful competition and borrow theirs. Make sure that your business card is clean and clear enough that it scans well.

Reproduced with permission from www.smallbizthoughts.com