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.

"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:

Volume III, Issue VII **July, 2011**

Your Employees Could Be Your Company's Biggest Security Risk! *Even The Most Loyal Ones!*

If you're like most technology-reliant businesses, you've spend a great deal of time and money making sure that you have a good firewall, your servers are secured, controlling who logs onto your network and what they have access to. While all of these activities are a vital component in a secure network, very often the workstations (desktops / laptops) are least secured in the entire network and poses the greatest amount of risk because of users trying to get their work done as quickly as possible and don't understand the security implications of their actions.

In a nutshell, you're making sure you have a good lock on the door, good security system that protects the perimeter of your house (windows, doors), but very often little thought is given to who is let in when they ring the doorbell.

Due to the plethora of new and increasingly sneaky cyber criminals lurking for unsuspecting victims, the area that we most need to focus on is in securing each laptop and desktop in such a manner so that staff members can still meet their daily work objectives, while making sure that confidential business data is not vulnerable to leaving the company and falling in the wrong hands. In a nutshell, you need to protect yourself against those that you let in while your employees do their work.

How do you know if you're letting anyone dangerous into your network?

Obvious sign: When you get a virus infection and pop ups.

The most dangerous break-ins are the ones you don't even know happened.

Silent Thieves: When software is installed on your computer externally and sits on your computer dormant until it's activated from a remote location and then steals your confidential data which could be credit card information, passwords to any and all websites, client contact information. Very often you don't even know it's happened.

Who are you letting in? At the least, kids who are just trying to be disruptive. At worst: Cyber criminal rings located off-shore, who are impossible to find.

As Sony recently proved, you can't insulate yourself 100% from every cyber criminal out there, but you can drastically minimize your exposure by taking some basic steps. Protecting your network with a good firewall is just the beginning.

Here are some steps you need to take with your workstations and laptops to prevent your employees from unwittingly inviting danger into your network:

Shiny New Gadget of the Month:

If you're a Mac device junkie and have a Mac at home, a PC at work, an iPhone in your pocket and an iPad in your car, check out MobileMe. This software allows you to store e-mail, contacts and calendars — even shared ones — in the cloud and automatically keeps them in sync across all your devices.

Other cool features include the ability to remotely locate a lost iPhone or iPad. And if you're certain it fell into less-than-honest hands and you don't think you'll be getting it back any time soon, you can remotely wipe the device clean of all your data.

The Gallery enables you to create a beautifully displayed online gallery of your photos and share them with others in just a few clicks, allowing your friends and family to add photos of their own. And the iDisk app gives you the power to store and share large files online as well as access them remotely.

MobileMe costs only $99 for a year's subscription and $149 for a family pack that gives you one individual account with 20GB of storage and 4 family accounts with 5 GB of storage. Not sure if it's right for you? Then sign up for a free 60-day trial at:

www.apple.com/mobileme

1. Make sure users don't have any more access on their computer than they absolutely need. They shouldn't be able to install ANY software themselves. If anyone other than your key IT contact has administrator privileges, remove them immediately.

2. As a company, make it a policy not to allow any free or pirated software onto your network. Many of these have software imbedded in them that search for passwords, credit cards, and will launch attacks from your network.

3. Make sure you have good quality, up to date antivirus software installed on each computer (even Mac's).

4. Make sure you have good quality up to date malware. Malware looks at websites that your employees are visiting, and looks for phishing websites. Phishing websites look authentic (could even look like your bank) but their sole purpose (among other destructive goals) is to capture any confidential information you enter into the website (account numbers, credit cards, etc). Malware detects these types of sites and blocks them.

5. Keep all Windows software up to date with current patches and fixes to bugs.

6. Keep all third party software up to date with patches and fixes.

7. Enforce an Acceptable Use Policy and make your staff aware of the risks of not governing themselves appropriately while using their computers.

8. Make sure people have access to only the data they need to, and nothing more. For instance, prevent all non-finance staff from accessing financial information and HR folders. Only provide access to customer lists to the employees that need them to do their jobs.

9. Do not share passwords. Have an automated process in place to force your employees to change their passwords every 90 days. Use complex passwords using a combination of letters, symbols and numbers.

10. For users who need remote access, make sure you have the most secure solution possible, so as to prevent hijackers from intercepting information as it's being transmitted between your network, and your remote user.

Mobile Devices Can Also Invite Trouble

Asking employees to be more careful about where they keep their laptops, phones, and tablets IS a good step in the right direction, but accidents happen and thieves are always on the prowl. That's why it's so important to take measures to lock down and secure any mobile devices you and your staff use to access your company's network. Here are just a few things to consider:

Encrypt All Information – Drive encryption software such as BitLocker (which is included with Microsoft Windows 7) can secure all the data on your hard drive. Also, check your computer to see if it has a Trusted Platform Module (TPM) chip which is generally more secure than those without TPM.

Multi-Level Access Security – Don't rely only on passwords to keep your laptop safe. Hackers can usually break most passwords in a few hours. We recommend adding a second way for people to prove that they are who they say they are BEFORE they are able to log in. Some people use smart cards to do this, but fingerprint pads are gaining in popularity.

Log / Back-Up Information – It's critical to log and back-up all information on business laptops to ensure smooth operations in the event of loss or destruction. We can automate the backups so they are done ON SCHEDULE and in a way that won't interfere with the use of the laptop.

The Right Response - What happens when an employee loses a laptop? Do you have a next step action plan in place? If not, we suggest calling us or your current IT support provider immediately to report the loss. The sooner we know, the sooner we can take preventative actions to lock that laptop out of the network. A blame culture where people are afraid to report losses is actually much worse for security.

7 Simple Ways To Keep Your iPad Secure

1. **Don't leave it lying around**. Although this is common sense, you've probably violated this rule more than once. iPads are easy targets for thieves, so don't let it out of your sight when in a public place – and don't leave it in plain view in your car or you might end up with a broken window in addition to a stolen iPad.

2. **Use a passcode.** Although it's not 100% hacker-proof, it will block unauthorized users from accessing your information.

3. **Consider enabling automatic data erasing.** You can configure your iPad to erase your data after 10 failed passcode attempts. Clearly this is not a good solution for anyone who constantly forgets a password or those who have kids who might try to endlessly log in to use your iPad.

4. **Sign up for MobileMe.** As mentioned in the "Shiny New Gadget of the month" article on page 2, this software will allow you to locate a lost iPad and, if it's not recoverable, you can remotely wipe the device of your private information.

5. **Limit its capabilities.** You can set your iPad to restrict certain functions such as access to Safari, YouTube, installing applications and explicit media content using a passcode. In the corporate world, an IT administrator could set these restrictions for company owned devices. At home, you can use this to restrict what your children can do with your iPad.

6. **Install software updates.** As with all software, make sure you have the latest security updates and patches installed to protect against hackers and viruses.

7. **Only connect to trusted WiFi networks.** Public WiFis are open territory for hackers and identity thieves. Whenever you connect, make sure it's a legitimate, secure connection.

How Exposed Are You Online?

Is privacy in North America dead? With all the camera phones, online tracking software and social media sites, you can pretty much bet on it. But that doesn't mean you can't protect yourself.

For starters, go to Google Maps and search on your name to see if they have a picture of your home mapped out. If so, you can request to be removed. Next, set up a Google alert for your name (and company name if you're a business owner). Google will e-mail you any time something is posted about you with a link so you can keep an eye on reviews, photos, etc. Next, go to www.Spokeo.com (note: this is primarily a US site) and search on yourself – you might be shocked at how much information is posted about you, your home, your income and personal life. You can request to be removed from this site by going to www.spokeo.com/privacy.

Tools to Drive Productivity Using Your Smartphone

New apps are constantly emergency for iPhone, BlackBerry, Palm webOS, Windows Mobile and Android that help boost productivity in business. I've listed 2 of them here. Check back next month for more!

App: Gwabbit

Why You Need It: Gwabbit's patent-pending semantic technology simplifies contact capture and management, automatically scanning incoming e-mails and transforming sender information into contact records in your address book.

Features: Address book management prompts, alert services for contacts who've been "gwabbed"

Available On: Blackberry,

Price: Free

App: Vlingo

Why You Need It: Got your hands full? Vlingo's voice interface technology lets users dictate texts and e-mail, look up contacts and search the web by speaking directly into their devices.

Features: Twitter integration, Google maps

Available On: iPhone, Android, Blackberry, select Windows Mobile phones, Symbian

Price: Free

How To Get A List of Ideal Prospects *For Free*

With LinkedIn.com, you can build lists of people who match your ideal prospect – and even get introductions – all for the cost of a few clicks.

For example, if you want to reach the HR managers at companies in a certain geographic area, simply go to LinkedIn and follow these steps:

1. Set up an account and connect with your clients, friends and vendors. The more "connected" you are online, the easier it will be to get introduced to new prospects.

2. Click on the "Advanced Search" link located near the main search form.

3. Customize your search by entering in the industries, title, location and keywords that would be related to the prospect you are looking to find. For example, you could enter "HR" or "Human Resources Manager" in the title search, and then narrow your results down using the "Postal Code" lookup and "Within X Miles" setting.

4. Unless you want a particular industry, leave that area unchecked.

5. When the list comes up, do a sort by "Relationship" so that those with the closest relationship to you or your contacts are ranked towards the top. If you find someone you want to connect with, look for people YOU know who can introduce you.

Careful! Phishing E-Mails On the Rise!

A phishing e-mail is an e-mail sent by a hacker designed to fool the recipient into downloading a virus, giving up their credit card number, personal information (like a social insurance number), or account or login information to a particular web site. Often these e-mails are well designed to look exactly like an official notification from the site they are trying to emulate.

For example, a recent phishing e-mail was circulated that appeared to come from Facebook stating that videos or photos of Osama Bin Laden's death were posted online. These e-mails looked exactly like a legitimate Facebook e-mail and even appeared to come from "Facebookmail.com." Once you clicked on the e-mail the phishing site would attempt to install a virus on your machine.

And now due to recent security breaches with Sony and e-mail marketer Epsilion, phishing attacks are going to increase – and they are going to get more sophisticated and harder to distinguish from legitimate e-mails. That's because the hackers that were able to access the private databases of the above mentioned companies now have the name, e-mail and interests of the subscribers, and in some cases birthdays, addresses and more. That means a phishing e-mail can be personalized with relevant information that the user provided to Sony, making the e-mail appear to be more legitimate and the user more likely to click on the links provided and take the actions requested. Now more than ever it's critical that you are wary of e-mail notifications and the actions they request you take. Even having good anti-virus software installed won't protect you if you give your account information away freely.

Are You Making These "Summertime Mistakes" With Your Server"?

How To Ensure The Heat Doesn't Fry Your Server (And Your Data!)

With the "dog days" of summer upon us, many business owners are looking for ways to keep their company's sales and profits HOT, while keeping their IT expenses COOL. But if proper attention is not given to your server and network equipment during the summer, all that heat outside can actually cause serious damage to your server, causing your system to crash and burn - literally! Excess heat IS a big problem for all computer equipment including laptops and PCs. But since your server is carrying the load, overheating will cost you more in electric bills and problems. And once a server gets too hot and blows out, it weakens components so that they are more susceptible to failure forever afterward, not just during the particular moment they overheated.

9 Steps Every Business Owner Must Know To Prevent A Server Crash

Here are a few simple things you can do to prevent your server and network equipment from overheating and crashing this summer:

- Tidy up the server room; a neater room will increase air flow.
- If you have more than one server, arrange them in a row so that the cold air comes from the front and is expelled out the back.
- Keep the doors to the server room closed and seal off the space to prevent dust buildup which can contribute to electronic equipment overheating.
- Make sure cold air reaches all the equipment.
- Have a redundant A/C that is specifically designed for computers.
- Buy a rack enclosure where the cooling is built in to thebottom of the rack.
- Keep the temperature at no more than 77 degrees.
- Use blanking panels over any empty spaces on your server rack.
- Consider virtualization so you are generating a lower amount of heat in the first place.