

September 2005

What's  
Inside

**Shocking Statistics  
Of Online Abuse  
Towards Children:  
What You Need  
To Do To  
Protect Your  
Kids Online**

**Exclusive  
Report:  
Are You Doomed  
If Your In-House  
Computer  
Expert Quits?**

**FREE iPod**

See back page for details...

**SOON: Managed  
Services**

**Don't Forget To Check  
Out Our Insert For  
Even More Great  
Tips, Secrets, Special  
Offers, and FREEBIES!**

## Are Your Children In Danger Online?

### These Statistics of Online Child Abuse Will Shock You!



Now that school is back in, thousands of children will be surfing the Internet to conduct research, chat with friends, and complete homework assignments. Although the Internet provides a tremendous learning tool for children, when left unchecked, it can also expose them to inappropriate material and unscrupulous individuals who are looking for the chance to exploit innocent children.

The statistics of online abuse towards children are alarming. According to a survey conducted by NetAlert, nearly one child in every five using the Internet has been approached online by a stranger. Forty-seven percent of children have been exposed to material that is pornographic, sexually explicit, violent, hateful, or that encourages them to participate in dangerous or illegal activities.

#### One In Five Children Will Receive Sexual Solicitations Online

According to Highlights of the Youth Internet Safety Survey conducted by the U.S. Department of Justice, one in five children received unwanted sexual solicitations online; there are a growing number of pedophiles using the Internet to gain a child's confidence and arrange face-to-face meetings.

These cyber criminals trap children by using spam e-mails, online messaging, children's chat rooms, and misleading domain names. If your child is using the Internet, you must take measures to educate and protect them from these

dangers. As part of my back-to-school newsletter edition, I've outlined 3 things you should be doing now to keep your kids safe online.

#### 3 Ways You Can Protect Your Children Online

- 1. Install web and e-mail filtering software to prevent your children from viewing inappropriate material.** I have found a website to help called [www.bsafeline.com](http://www.bsafeline.com). Not only will this prevent your children from visiting inappropriate web sites, but it will also stop inappropriate spam.
- 2. Talk to your kids about online safety and proper Internet usage.** Set limits and guidelines about when they can go online, what they can do, and how long they are allowed to be online. Explain why it is dangerous for them to "chat" with strangers online or download suspicious looking files.
- 3. Give your children specific online guidelines or rules to follow when using the Internet.** It's not enough to warn them about potential risks; pedophiles know how to cloak their identity and gain a child's confidence to arrange face-to-face meetings.

#### Require your kids to follow these rules online:

- ♦ I will not give out personal information such as my address, telephone number, parents' work addresses, or our e-mail address to anyone online.

Continued on back page...



# Are You Doomed If Your In-House Computer Expert Quits?

Here's an important question that most small business owners don't know how to answer: what would happen if you suddenly lost your in-house computer expert?

Most small business owners believe if they lost that expert nothing important could go wrong. In fact, the opposite is usually true. Most small businesses have someone who holds the keys to their entire network; if that person unexpectedly quits, it could end up costing them time and money and could have a serious impact on the security and operation of the business. Want to know how much it would impact your company? Ask yourself the following questions:

## 1. Do you know all the passwords?

Every machine and internet related device on your network has (or should have) a password. If you don't know what they are, you cannot view, change, or update the system settings. You should also know the password to your company database and accounting package.

I highly recommend maintaining a password list that is updated whenever a new password is added or changed. Your technician might already have this list, but might not be sharing it with you. Check with them about obtaining a copy of all the passwords to your network and establish a system for obtaining updates.

## 2. Do you know where your backup files are stored, and if they are being stored properly?

Backing up your data is like brushing your teeth; it's boring, monotonous work, but it must be done every day. If you are like most business owners, you're too busy dealing with the "crisis of the day" to think about system backups and probably leave tasks to your internal expert. If your database gets fried and your tech is no where to be found, you might be in a lot of trouble. In fact, not only should you make sure your backups are being done

regularly, but you should also check that they are being done right. The absolute worst time to check the accuracy and reliability of your backup system is in a crisis situation. It's not uncommon for a backup system to become corrupt from an overload of data or a user mistake. If this happens, it could appear that your network is being backed up, even though it's not. My recommendation: have us remote in once a month to make sure your backup system is in working order.

## 3. Do you have all the product keys to your software?

Product keys are long, alphanumeric codes, usually printed on the back of the software's packing material, that are required to install the software. Once installed, you don't need them again...UNLESS your system becomes unstable and you need to reinstall the program.

To avoid losing these critical product keys, I recommend installing a free program called Belarc Advisor from [www.belarc.com](http://www.belarc.com). This program will scan your PC and list all of the hardware, the manufacturer's names, the names of all the programs installed, their locations, and their product keys. Once you activate this program, it will create a secure report that you can print and store in case of fire, theft, or system corruption. I will be able to supply you with a similar report when I get our Managed Services product started (see article page 3).

## 4. Do you know where all the software disks are stored?

As a follow-on to the above question, you should also know where all of your software disks are stored. Bad things happen to computers, and the situation can be made worse if you are not prepared. Taking a minute to organize and store your software disks in a secure place can save you a considerable chunk of money in the event that you need to restore a program on your computer. If you

don't have the disk, you might be forced to buy the software again.

**5. Do you know what routine maintenance must be done to your network?** I know that the very idea of learning about and keeping track of all the servers, workstations, and peripherals on your network probably gives you a major headache, but it is important information to maintain. If your in-house expert leaves, who will take over? Although it isn't rocket science, it is very important to know what maintenance is required and when. Learn about and understand backups, database maintenance, system updates, security patches, virus updates, system resets, and more.

**6. 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. As a client of **AFL Computer Consulting**, I can make sure all of the employee's access is disabled the moment you find out that he or she no longer works for you.

**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.



"What a relief! Daddy thought you might bring your flying monkeys with you, grandma."

## Quick Computer Tip: **How To Add A Shortcut To Your Desktop**

Do you have a document, folder, or application that you frequently access? If so, you might want to add a shortcut to your desktop to give yourself "one click" access to it without having to navigate the path to the actual location of the file. Here's how:

1. Right-click anywhere on your desktop and a pop-up menu will appear.
2. Select "New," then "Shortcut," and a "Create Shortcut" window will open.
3. Use the "Browse" button to find the path to the application or program.
4. Click on the icon of the program or file that you want, and then click "OK". Click "Next" and then enter a name for the shortcut.
5. Enter the name for your shortcut and click "Finish." The new shortcut will appear on your desktop. Drag the shortcut icon to any place on your desktop.



### Coming Soon:

## **Managed Services**

The new product that you are going to be hearing a lot about in the next year is a product called **MANAGED SERVICES**. Managed services is where your network hardware (computers, networks, printers, etc.) are monitored and managed remotely. This will allow the ability to change from fixing issues with your system reactively to proactively. I will be able to see errors that show up, low hard drive space, that

anti-virus definitions are getting updated and much more. This is referred to as remote monitoring. There is also a feature called patch management where I can update your system with patches (updates) from Microsoft and other companies when they need to be performed. But, not before I am sure the patches won't bring the computer down. Some of these products will also allow for remote access to your system to perform system maintenance and updates, such as disk defragmenting, virus/spyware scanning, etc. Other features available are asset management and software deployment. This is where I can track what programs are installed on the computer and see when programs are added or removed along with installing programs on any or all of your computers without having to step foot in your office or kick people off the computers. If you would like to learn more about these services or sign up for them, give me a call. I will be contacting you shortly regarding this service.



2872 West Bloomfield Oaks Drive  
Suite 110  
West Bloomfield, MI 48324

Phone: 248-425-0009  
Fax: 248-363-5948  
jeff.lipshaw@aflcc.com  
www.aflcc.com

### **The Small Businesses 'IT' Department**

### **Services We Offer:**

- Managed Services
- Hardware
- Custom and Packaged Software
- Virus Protection & Removal
- Spam Filtering and Removal
- General Network Repair and Troubleshooting
- Network Design & Implementation
- Disaster Recovery
- Network Security
- E-mail & Internet Solutions
- Wireless and Wired Networking

*Continued From Page 1: Are Your Children In Danger Online*

- ♦ I will tell my parents right away if I see a web site, e-mail, or message that makes me feel uncomfortable.
- ♦ I will never send my picture to anyone online or upload my picture to any web site without my parent's knowledge and permission.
- ♦ I will never agree to meet someone face-to-face who I met online without my parents' knowledge and permission.
- ♦ I will not respond to any messages that are mean or that make me feel uncomfortable in any way. If I get a message like that, I will tell my parents right away so that they can contact the online service.
- ♦ I will never give my parents' financial information to anyone, especially their credit card information, bank account information, or social security number.

If you want more information on how to keep your children safe online or to report illegal, violent, or explicit acts towards children, go to [www.cybertipline.com](http://www.cybertipline.com). This site is run by the National Center for Missing & Exploited Children and is a great resource for parents, teachers, and guardians.

### **I'd Love To Hear From YOU!**

Is there an article you would like to comment on? Is there a topic you want me to research? Have a funny story or a resource you want to share with the other subscribers? Then send it to me! I am always looking for new and useful content to add to Bits-N-Bytes.

**Jeffrey Lipshaw**  
248-425-0009  
jeff.lipshaw@aflcc.com  
www.aflcc.com

*Know Someone Who Could Use My Help?*

## **Refer A New Client To Me In September And I'll Send You A FREE iPod!**

I love getting referrals from my loyal clients and I'm not afraid to show it! Refer a new client to me during September and I'll give you a FREE iPod and your referral 2 FREE HOURS of computer support with no strings attached.

### **Everybody Wins!**

You get a cool new iPod to play your favorite music, and the person you refer gets to "try before they buy" with 2 free hours of computer support (they also get introduced to an honest, reliable technician who is dedicated to solving their computer problems). Just tell your friends to mention your name when they call so I can reward your loyalty and make sure they get their 2 free hours of support.

### **How To Legally Acquire Stolen Goods**

If all those cops-and-robbers shows make you want play too, try logging on to [stealitback.com](http://stealitback.com). This site auctions off goods collected by hundreds of police departments across the country including evidence from trials, expensive stuff confiscated from criminals, and shoplifted items that can't be returned to stores.

Stealitback.com was founded by a former Long Island cop in 1999. He says police auctions are not new, but by posting the items online, they reach a much larger audience. And the auctions relieve police of the burden of storing and selling the articles.