



SmallBusinessIT

# TECHNOLOGY ADVISOR

*Tech Tips for Small Businesses*

## Top Mistakes That Make You A Prime Target For Identity Theft

### QUOTES ON NEW YEARS

“Youth is when you’re allowed to stay up on New Year’s Eve. Middle age is when you are forced to.” - *Bill Vaughn*

“Now there are more overweight people in America than average-weight people. So overweight people are now average. Which means you’ve met your New Year’s resolution.” - *Jay Leno*

“An optimist stays up until midnight to see the New Year in. A pessimist stays up to make sure the old year leaves.” - *Bill Vaughn*

The numbers are staggering: according to the 2006 Identity Fraud Report, identity theft cost consumers *and* businesses a whopping \$56.6 billion dollars. Identity theft occurs when someone steals your name, Social Security number (SSN), bank account number, or credit card to open accounts, make purchases, or commit other fraudulent crimes.

### The Methods They Use To Steal Your Identity

The methods identity thieves use include low tech strategies (like going through your trash can, also known as “dumpster diving”) to highly sophisticated phishing scams that include cloned PayPal or bank websites that trick you into giving your username, password, or account number. Other ways include:

- Stealing records from an employer or bribing an employee who has access to the records.
- Hacking into the company’s employee records.
- Stealing mail, such as bank account or credit card statements, tax documents, pre-approved credit cards, or new checks.
- Abusing their employer’s authorized access to credit reports.

### How Identity Theft Affects You

Once someone has stolen your identity, they can use your credit cards or bank account to purchase expensive consumer goods like computers and electronics that can easily be resold for cash. They can also open and charge up new credit cards, which can be a real mess to straighten out with vendors and credit reporting agencies. Other criminal activities include taking out auto loans in your name, opening a new

phone or wireless service in your name, or writing counterfeit checks to drain your bank account. Some have even used it to file for bankruptcy to avoid paying debts they’ve incurred, or to avoid eviction.

### How to Protect Yourself and Your Employees

Never give your personal information, Social Security number, credit card number, or bank account numbers over the phone or online unless you know for certain you are dealing with a legitimate company. Make sure your employees are given an AUP (acceptable use policy) that educates them on the dangers of phishing scams and spam e-mails designed to either trick you into giving your information or installing a virus that secretly steals the information stored on your PC without your knowledge.

You can recognize a secure website, as it has an https:// at the beginning of the web address (regular web sites only have http:// and no “s”) at the top of the page on which you are submitting your information. It also must have a picture of a lock in the bottom right corner of the page. If you don’t see both of these measures in place, do not submit your information.

And even if you DO see this, use a credit card instead of a debit card or pay by check option because you’ll get security protection from your card’s issuer. Visa, MasterCard and American Express all have a zero liability policy. If you notify the bank of unauthorized transactions, you pay nothing. And some credit card companies offer one-time use numbers to prevent someone from stealing your account number and using it for unauthorized charges.

*(continued on Page 4)*

## SHOULD YOU LEAVE YOUR COMPUTER ON AT NIGHT OR TURN IT OFF?

I've been asked by customers whether or not they should leave their computer on all the time or turn it off when they are not using it.

Several years ago I would have told my clients to turn their machines off to save power. But with the proliferation of viruses and threats over the last few years, I have changed my mind.

Today, anti-virus programs and anti-spyware applications need regular updating. These updates are often scheduled to run in the wee hours of the morning when you are not using your computer.

Windows also needs to be updated whenever a new security patch is released. This is usually not daily, but it may happen several times a month. It's important to update your operating system as soon as a patch becomes avail-

able because hackers move very quickly to reverse engineer Windows updates. As soon as an update is released, they create a virus specific to that vulnerability and start looking for unprotected machines to infect and invade.

In addition to the above, you should be backing up your data every day, and the best time to do this is at night when you are not using it.

So bottom line, leave your computer on all night and restart it two or three times a week to clear the memory.



## A QUICK LESSON IN E-MAIL ETIQUETTE...

Even seasoned e-mail users step over the lines of e-mail etiquette from time to time. If Dear Abby were around, here are 5 tips she would have for sending e-mails:

1. Don't send large attachments unless requested. Large attachments can cause e-mail problems for the recipient. Wherever possible try to zip or compress attachments.



2. Make sure your anti-virus software is up-to-date. Here's another problem with attachments: they are vehicles for viruses. You'll quickly lose friends and customers if you send them documents full of viruses!

3. Don't write in ALL CAPS. It's the online equivalent of yelling.
4. When sending an e-mail to a group, use the BCC (blind carbon copy) field instead of the To field. By copying everyone in the same e-mail, you are publicizing their e-mail address to everyone else on the list. In some cases, this might be appropriate, but many people are very private about their personal e-mail address and will be annoyed by your lack of discretion.
5. NEVER send personal or confidential information by e-mail. Once you hit "send," you lose all control over where that message ends up. This goes double for credit card numbers, bank accounts, and passwords to secure websites, as well as personal information about other people.

## BE CAREFUL OF WHAT YOU SAY IN AN INSTANT MESSAGE

If you think your words disappear forever when an instant messaging session is closed, think again.

Your IM is not a safe refuge for private chatter. Companies and government agencies can monitor and log instant-messaging conversations conducted on company computers. Google saves chat sessions automatically and they can be searched later. Users of Google Talk must disable the setting or choose "off the record" for sessions they don't want saved.



Instant-messaging services such as AOL's AIM, Yahoo's Yahoo Messenger, and Microsoft's Windows Live Messenger don't store con-

versations on their servers automatically, but they offer various tools for companies and individuals to log conversations.

Recent scandals demonstrate that in-

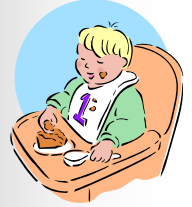
stant messaging is not private. Government-monitored IMs found inappropriate messages by a member of Congress, who then resigned. And IMs have figured in corporate scandals, as well. Instant-messaging services are offering a host of new products and tools for tracking IMs. AIM Pro, a free version for individuals and businesses, automatically archives conversations and saves them for 14 days. The feature can be extended or turned off.

Microsoft's Live Communications server allows a company's information technology department to log and search employee conversations, including those on IM services like Yahoo and AOL.

A study by the American Management Association and The ePolicy Institute shows that only 13 percent of companies now track and log instant messages. The crackdown, however, is starting to take effect. Two percent of employers have fired someone because of what they said, and about 26 percent of companies have fired someone for misuse of email.

### The Lighter Side: Things toddlers eat....

Panicking when his toddler swallowed a small magnet, George rushed him to the emergency room.



"He'll be fine," the doctor promised. "The magnet should pass through his system in a day or two." "How will I be sure?" he pressed.

"Well", the doctor suggested, "you could stick him on the refrigerator. When he falls off, you'll know."

### Grief and suffering

A dietitian was addressing a large audience in Chicago:

"The material we put into our stomachs is enough to have killed us. Red meat is awful. Soft drinks erode your stomach lining. Chinese food has MSG. And mayonnaise can be disastrous."

"But one thing is the most dangerous of all and we all have eaten it or will eat it. What food causes the most grief and suffering for years after eating it?"

A 75-year-old man in the front row stood up and said, "wedding cake."

**\$297  
Value!**

## FREE Data Security Audit During January!

**Don't risk losing your data! Our FREE data security audit will determine if you are at risk for losing your data to a backup or hardware failure, viruses, or other disasters! Call us before January 31st and it's absolutely FREE!**

\*This offer is valid only for qualified businesses with a minimum of 5 PCs. Other restrictions may apply.



SmallBusinessIT

# TECHNOLOGY ADVISOR

Tech Tips for Small Businesses

JANUARY 2007 VOLUME 2 ISSUE 1

## INSIDE THIS ISSUE:

- **FREE Data Security Audit!**
- **Top Mistakes That Make You A Prime Target For Identity Theft**
- **Should You Leave Your Computer On At Night**
- **Email Etiquette**
- **WARNING! Be Careful of What You Say In An Instant Message!**

402 Amherst Street, Suite 300  
Nashua, NH 03063  
866.324.8273  
[WWW.SCIINC.COM](http://WWW.SCIINC.COM)

(continued from page 1)

Shred all medical bills, financial statements, credit card applications, tax statements, or any other mail that contains confidential information about you before you throw them into the trash.

Never open e-mails or attachments from e-mail addresses you are unfamiliar with, and NEVER respond to e-mails that ask you to verify your account information because your account is being closed, suspended, or charged. If you want to verify this, call the bank or the company to see if it was a legitimate e-mail.

### Signs That You've Fallen Victim to Identity Theft

If you see any unexplained charges or withdrawals from your bank accounts, if you receive credit cards that you did not apply for, or if you start receiving bills or collection letters for items you have not purchased, someone may have stolen your identity.

Always follow up with the business or institution to find out exactly what is causing the situation as quickly as possible. The faster you act on identity theft, the easier it will be for you to clear your name.

## Services We Offer:

- SPAM Email Filtering Services
- Computer Virus & Spyware Removal & Protection
- 24x7 Remote Monitoring & Maintenance
- Complete network management and support
- Critical Patch and Service Pack Installations
- Computer Network Security
- Secure Wireless Networks
- Implement and Manage VPNs (Virtual Private Networks)
- Manage System Backups
- Recommend Data Storage Solutions
- Provide Disaster Recovery
- Troubleshooting and Problem Solving on all Networks and PCs
- Help desk - Phone and Remote Support
- Hardware Installation and Support
- Software Upgrades and Installations
- Server Installations and Upgrades
- Manage Software Licensing
- Act as a Vendor Liaison
- Monthly Reporting
- Quarterly Review and Planning Meeting
- Database Administration & Maintenance

...For More Information Visit

[www.sciinc.com](http://www.sciinc.com)