TECH EXPERTS

ExpertsUpdate

October 2007

Brought to you by:
Technology Experts Corporation • 980 South Telegraph Road • Monroe, Michigan 48161 • (734) 457-5000 • info@expertsmi.com

Top Mistakes That Make You A Prime Target For Identity Theft

The numbers are staggering: according to the 2007 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 employer's 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.

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.

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.

Do You Make These Mistakes When Sending E-mail?

A Quick Lesson In E-mail Etiquette

In this day and age, it is amazing how many businesses and professionals still violate basic e-mail etiquette rules. Almost everyone uses e-mail to communicate with their clients and friends yet very few give any thought to the importance of those communications.

If you want to make sure you are not offending your clients and friends when sending e-mail, here are 6 basic rules to live by:

1. Never send e-mails to people who have not requested to receive them. This is also known as spamming and federal laws are getting much tougher in the rules and penalties for sending unwanted e-mail messages. Many businesses make the mistake of thinking that they are free and clear to send e-mail promotions to their clients, even if the client has not specifically requested to get those promotions. When in doubt, it's always smarter to err on the side of caution and NOT include them in your broadcast; doing so could cause you to lose favor with your clients, or worse yet, lose their business altogether.

2. Don't attach files unless you've gotten permission to from the recipient. With the looming threat of viruses, it's considered bad net-etiquette to send file attachments.

3. DO NOT USE ALL CAPS. Using all caps in an e-mail is the online equivalent of screaming at the top of your lungs. Unless that is what you intended to do, make sure you use lowercase letters.

4. When sending to a large list of people, use the BCC (blind carbon copy) feature. Otherwise, you are exposing every recipient's e-mail address to everyone else on the list. Since most people like to keep their personal e-mail addresses private, exposing your entire list will cause you to lose quite a few brownie points.

Here's another point to consider: I wish I had a nickel for every sales person that sent out a broadcast e-mail to all their clients and prospects and accidentally copied everyone on the list. This is an EASY way for your competition to get their hands on one of your most precious assets.

TIP: Make sure employees know what they can and cannot send through company e-mail accounts.

5. Never send information you wouldn't want the entire world to know about. E-mails can quickly spread around the Internet. Never send confidential information, off-color jokes, political opinions, pictures, or gossip that you wouldn't want made public. This goes double if you are using a business e-mail address. And if you are a business owner, you want to make sure your employees know that it is against company policy to send this type of information through your company e-mail. Even a well-meaning joke can land you in a lot of hot water if taken the wrong way. Always take a minute to think before you hit the "send" button.

6. Avoid fancy formatting, background graphics, and other "cute" pictures and fonts. What looks great on your monitor may be impossible to read on someone else's; it also may annoy the reader who has to weed through the fluff to find the content.

FREE Report: 12 Surefire Signs Your Business Is Ready For A Server

Is your business limping along using outdated computers or a peer-to-peer network that is constantly giving you problems?

Are you planning on adding employees, opening a remote location or adding an additional office?

Are you just sick and tired of dealing with conflicts, error messages, and expensive breakdowns and down time?

If so, you might consider upgrading your network to a file-server network for greater security, functionality, and file-sharing capabilities.

At one time, servers only made sense for larger organizations because of their high cost and complexity. But thanks to major advancements in technology, client-server networks are very affordable and easy-to-implement.

To learn more, call our office at 734-457-5000 and ask for Carol.

You can also send us an e-mail to request this report. Just send your request to serverreport@expertsmi.com.

Important Security Alert For Anyone Using Instant Messaging In The Workplace

According to the Radicati Group, 85% of businesses—both large and small— are now using instant messaging (IM) as a communication tool.

Unfortunately, hackers are rapidly developing ways to use IM to spread viruses and gain access to computers and networks.

Instant-messaging security vendors FaceTime Communications and IMlogic Inc. have both reported an exceptionally high spike in attacks over recent months.

IM attacks work similar to e-mail viruses; the sender tries to get the user to click on a link that takes them to a website where they'll be infected with a virus, or it tries to get the user to download a file.

Many of these attacks appear to be from legitimate sources or people on a "buddy" list.

Just recently, FaceTime discovered a threat on AOL's instant messenger system. They quickly contacted AOL but tens of thousands of computers had already been infected with a peer-to-peer file sharing program called BitTorrent.

Hackers then used this program to upload movies to the victim's hard drive and use their computer as a vehicle for sharing it with others.

These attacks are also getting more complex. Savvy IM users will often reply to an IM and ask their buddy if the link or file sent was safe.

However, hackers have now developed an intelligent bot that will actually automatically respond to the message confirming the file or link is safe. One bot actually had 6 different responses depending on the question that was asked by the user.

Just like viruses, worms, and other security threats, businesses need to put measures in place to protect themselves from these new threats.

The first step is educating your employees about these threats through your employee's acceptable user policy. However, since there is always a chance someone will click on a link or download a file, education is not enough.

If you currently use IM, we urge you to contact our office at (734) 457-5000 so we can discuss installing the proper software and security measures to make sure you don't fall victim to these growing attacks.

Now is the time for your fall computer check up!

As fall approaches, take time to remove the dust and debris that accumulate inside your computers. It can act just like insulation, making them run much hotter than they should. This can cause lockups, freezing and costly downtime.

Our 15 point system inspection is designed to keep your computer equipment running smoothly, and pinpoint potential problem areas before they turn into **expensive** repairs.

Fall System Checkup
Just $39 per computer!

Volume pricing available for 5 or more systems.
Limited time offer.

Tech Experts
Information Technology Professionals

Call us for all of your computer and networking needs!
(734) 457-5000 · (866) 99-EXPERTS
980 South Telegraph Road · Monroe

Excel 2007 Has A "Small" Problem Multiplying

We all learned how to multiply with pencil and paper, even great big numbers and decimals. But when it comes to something important like a blueprint or a scientific formula we reach for a calculator - or a spreadsheet.

That's much more reliable, right? Well, not if the spreadsheet is Excel 2007. Technicians have revealed that Excel 2007 thinks that 850*77.1 is 100,000.

What's the correct answer? It should be 65,535. Other sites have verified that the error carries over into some (but not all) calculations based on the incorrect result.

If it were just 850*77.1 that gave a wrong answer, we could probably work around that. But there are tons of other problem numbers. Set up a spreadsheet to divide 65,535 by every number from 1 to 65,535 itself, then multiply the number by that result.

So, for example, the spreadsheet divided 65,535 by 26 to get 2,520.577. Then it multiplied 26 by 2,520.577 to get... 100,000?! Over ten thousand of these simple calculations gave the wrong answer.

We won't know just why the problem comes up until Microsoft speaks out, but there is one thing about 65535 - it's the very largest 16-bit number.

In hexadecimal (the programmer's friend) it's FFFF. But converting the "problem" results to hexadecimal in Excel yields FFFE. That's a clue.

Meanwhile, if you have any spreadsheets where some results hit the range around 65535, it might be a good idea to double-check with your trusty calculator... or a pencil.

GOOD NEWS: The Excel team has dissected the problem in detail and is working feverishly to swat this Excel bug.

And finally, two weeks after the scary announcement, Microsoft has fixed the bug. Get the hotfix now, or just wait for it to show up in Automatic Updates.

The Best Laptop You Shouldn't Own

For about $200 you'll soon be able to buy a laptop that comes with a web browser, a word processor, camera, built-in wireless, flash memory, open source operating system, and more.

But this laptop, called the XO, wasn't made for you, no matter how small your business is. It was "designed for the poorest and most remote children in the world," by the non-profit group, One Laptop Per Child (OLPC).

Its 433Mhz energy-efficient AMD processor is slow. It has no hard drive, CD, or DVD drive. Your hands are too big for the child-size keyboard. You'd go nuts trying to run a business using this machine and its puny 7.5" screen.

But you can and should consider making a purchase. The XO will be available to buyers in the U.S. for a two-week period, from November 12 - 26.

Under a program called "Give 1 Get 1," buyers can purchase two laptops for $399. One would be shipped to a child in a developing nation, and the other to the buyer. If you have the budget, buy them - just have both units shipped overseas, to kids who can really use them.

On the web: http://www.laptop.org.

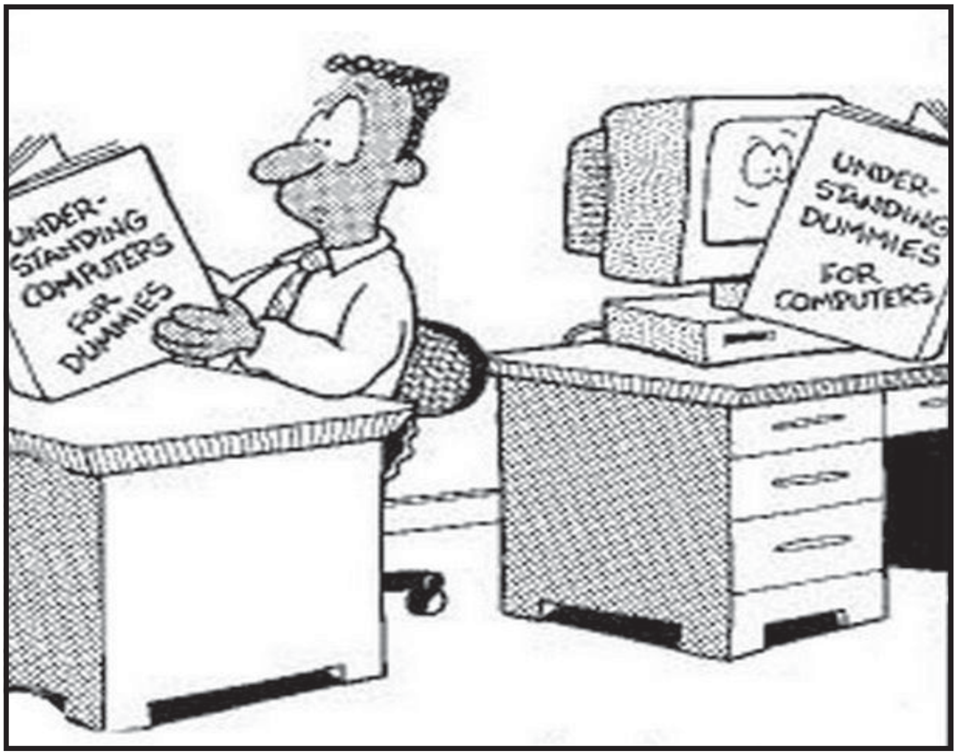
Take advantage of our client portal! Log on at:
https://connect.expertsmi.com/support

CONTACT INFORMATION

24 Hour Computer Emergency Hotline
(734) 240-0200
•
General Support
(734) 457-5000 • (866) 993-9737
support@expertsmi.com
•
Sales Inquiries
(734) 457-5000 • (866) 993-9737
sales@expertsmi.com

Tech Experts
Information Technology Professionals

980 South Telegraph Road
Monroe, Michigan 48161
(734) 457-5000 ◆ Fax (734) 457-4332
info@expertsmi.com


UNDER-STANDING COMPUTERS FOR DUMMIES
UNDER-STANDING DUMMIES FOR COMPUTERS