BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 2 February 2012 25th Year of People Helping People!

In this Issue

Protection from identity	Cont.	2
What are Sniffers		3
What are Sniffers	Cont.	4
What are Sniffers	Cont.	5
Lost Cell phone		6
More about Internet threats		7
More about Internet threats		8
Some things to look into		9
The lighter side		10

Don’t forget to visit our club’s site at: http://gtbpcug.org

As well Don Miller’s and Darrell Manns’ :

http://www.dmanns.org/dmiller/

Ten Ways to Protect Yourself From Identity Theft

http://askbobrankin.com/

Identity theft is one of the most traumatic non-violent crimes to which one can fall victim. When a crook uses your good name to commit fraud or robbery, the impact on your reputation, employability, and credit is severe and can last for years. You may even find yourself arrested for crimes you did not commit. So it's important to protect yourself against identity thieves.

The telltale signs that your identity has been stolen can be subtle and go unnoticed for months, even years. Inexplicable charges on your credit card bill may be chalked up to clerical errors. Letters from creditors you've never heard of and certainly never did business with may be ignored. But eventually, an enormous credit card bill, legal papers or police show up at your door. You are denied a mortgage or a job. Then the real nightmare of proving "I didn't do it" begins.

It can be maddeningly difficult to clear your name, costing hundreds of hours and thousands of dollars. That's why it's important to take steps NOW to make it as difficult as possible for a scammer to victimize you. Take action on these ten tips as soon as possible, and you'll tips the scales in your favor:

Check your credit report on a regular basis, to see if there is any incorrect information, or accounts you don't recognize.
My article Free Credit Reports Online explains how U.S. citizens can get three free credit reports per year.

Shred your sensitive personal documents before throwing them away. A battery-powered cross-cut shredder can render your banking and credit card information unreadable and costs less than $30. "Dumpster diving" is a favorite, low-tech way by which ID thieves collect bank statements, credit card numbers, Social Security Numbers, and other bits of your identity from your trash.

Be wary of telephone solicitors asking for personal or financial information to "verify your identity." Common scams involve someone who claims to be from your bank or credit card company, claiming that there is a problem with your account. If you did not initiate the call, hang up and call the toll-free number on your statement, then ask for the security department.

Continued on the next page

Keep important documents, such as tax returns, birth certificates, social security cards, passports, life insurance policies and financial statements secure in your home. A fireproof safe is a good idea, but remember to bolt it to the floor or hide it well.

Make sure no one is looking over your shoulder when you enter your debit card's PIN at an ATM or point-of-sale terminal. I recommend the "two finger method" where you point two fingers at the ATM keypad, but only press with one. This makes it nearly impossible for someone nearby to discern your PIN while you're entering it.

Memorize PINs, account numbers, and passwords; do not write them down. And for heaven's sake, do not put such data on scraps of paper kept in your wallet, purse, or laptop case!

Get blank checks delivered to your bank branch, not to your home mailbox from which they may be stolen. On a similar note, eliminate junk mail which may contain "convenience checks" and credit card offers that can also be intercepted from your mailbox.

Visit the Privacy Rights Clearinghouse and OptOut Prescreen for help eliminating these dangerous nuisances.

When you order a new credit or debit card, mark the calendar and follow up promptly if it does not arrive within 10 business days. Ask the card issuer if a change of address request was filed, and if you didn't do it, hit the panic button.

Don't give your Social Security Number to any business just because they need a "unique identifier" for you. Instead, ask if you can provide alternate proofs of identity, such as your driver's license or birth certificate.

Consider placing Fraud Alerts with the major credit bureaus, so new accounts cannot be opened without your knowledge. Call Equifax (800-525-6285), and they will pass along the request to both Experian and Trans Union. Fraud alerts expire after 90 days, so you can repeat the process quarterly, or lock down your credit file with a Credit Freeze. A freeze is permanent and free (in most U.S. states) but it may interfere with loans applications, employment screening, signing up for utility or phone service, new insurance policies, and other transactions. You'll also need to contact each credit bureau (Equifax, Experian, and Trans Union) to request the credit freeze.

What About LifeLock?

You may be considering LifeLock or a similar identity theft protection service. Although this can be helpful, no company can guarantee that identity theft will never happen. These services monitor your bank account, and look for suspicious online activity done in your name. They'll alert you if they spot any red flags and promise to help you repair the damage. But because of lawsuits filed by the credit bureaus, Lifelock can no longer place fraud alerts on your behalf.

Also, all identity protection services are barred from offering Identity theft insurance coverage to residents of New York. Since you'd have to manage fraud alerts or a credit freeze on your own, and because there is so much you can do on your own to protect against identity theft, I don't see much value in these services.

Do you have other tips for avoiding identity theft? Post your comment or question below...

Read more: http://askbobrankin.com/ten_identity_theft_protection_tips.html#ixzz1hebdnlXy

Read more: http://askbobrankin.com/ten_identity_theft_protection_tips.html#ixzz1hebX6wXh

Read more: http://askbobrankin.com/ten_identity_theft_protection_tips.html#ixzz1hebQ6T4I

What is a sniffer?

http://komando.com

Q. I'm doing research for a mystery novel. In the novel, someone discovers a "sniffer" on my character's computer. I need to know what a sniffer actually is. Is it something my character can discover and physically disconnect? Can it be held in your hand and turned over to law enforcement? Or would law enforcement have to confiscate the entire computer? Thanks for any help on this. It's a small thing, but it's holding up my plot.

A. First of all, let me just say that you have a great author's name. It's catchy and memorable. Plus, it will look good on a book cover or movie screen. As a rule I don't give out full names in tips, so everyone else will have to trust me on this.

I'm glad that you wrote. You have no idea how laughable I find many "high-tech" scenes in TV shows and movies. I cringe whenever crime shows "enhance" surveillance video. It always comes out crystal clear so they can catch the bad guys. Try that in real life, and you'll get a blocky mess!

Another favorite is when hackers break into government servers seemingly by magic. Sure it's possible, but it takes a lot of time and effort. Plus, hackers would use a phishing attack instead of tackling a government firewall directly.
How tech is depicted in movies is the subject of one my most recent Kim's Reports. Watch it now and see if you can spot the Hollywood computer myths.

Now, about those sniffers. . . First, it does not mean you have a cold.
Sniffers are readily available on the Internet. In fact, the most popular ones are free. Think of a sniffer as a secret spy. He patiently sits and waits. When something juicy like an account password crosses his path, he snatches it up without anyone the wiser.

One of my family members told me a story recently. He was visiting a friend's house. While there, he installed a sniffer on his laptop. His friend signed into her Facebook account. Using the sniffer, he grabbed her password. Then, he logged into Facebook as his friend.

Every time she updated her Facebook account, he deleted her status update. It drove her crazy. She cursed Facebook. She called her ISP. She said she needed to buy a new laptop. This went on for about 30 minutes until he couldn't hold his laughter and told her what was really going on.

The term sniffer actually has a specific meaning in tech circles. It's a nickname for a packet analyzer, also known as a network analyzer. Basically, a sniffer monitors traffic on a network.

All network communication is broken into bursts of information called packets. The sniffer reads these packets to see what data they contain. It then reports back to its administrator.

Sniffers come in both hardware and software varieties. Hardware sniffers are usually just highly specialized computers. Only high-volume networks require these.

Most sniffers are software programs. Network administrators install sniffer programs on a regular network computer. They can track certain elements of the network traffic. In fact, I have a sniffer-type program on my site.

Continued on the next page

There are a lot of legitimate uses for sniffers. Companies can find network problems, improve security and monitor bandwidth use. A sniffer can also detect and filter out restricted content.

The Internet is essentially one big network. Internet service providers use sniffers to make sure their part of it is running smoothly. It helps them monitor bandwidth and optimize traffic flow. Sniffers also detect pirated content people might be downloading.

It probably goes without saying that hackers use packet sniffing as well. All a hacker needs to do is get on your network. The hacker can then use sniffing to intercept and record user account passwords. They can also read unencrypted text, like email.

That's one reason using public Wi-Fi is dangerous. You might be using the same network as a hacker with a sniffer. Learn how to stay safe when using public Wi-Fi.

That's also why so many online services are enabling encrypted communication. Facebook, for example, has encryption turned on by default now. This keeps sniffers from reading packet contents going to and from that site.

Now, hackers can get around encryption. However, it takes a lot of time, effort and expertise. The odds of a hacker breaking your encrypted communication are very low.

Now that we have a basic understanding of sniffers, let's talk about your scenario, C.C. I would say a hardware sniffer probably wouldn't work in a home environment. Your character would probably notice a new computer in the house.

Most likely the sniffer would be of a software variety. However, I wouldn't go with that either. Sniffers aren't very good spy tools in that kind of situation. They aren't designed for stealth or remote access.

Your character would probably see the sniffer running fairly quickly. Once a sniffer is found, it's easy to uninstall. Plus, as I said, a lot of online services are moving to full encryption. A sniffer wouldn't give its owner much compromising information.

The bottom line is that a sniffer probably isn't the best threat for your character. However, I do have a better suggestion. That would be a keylogger.
A keylogger is probably what you meant anyway. This is a favorite tool of hackers and jealous significant others. Keyloggers steal a computer user's important information while remaining totally hidden.

A keylogger records every keyboard stroke. Many keyloggers can also take screenshots. Everything you do on your computer is recorded and sent to the keylogger's owner.

A keylogger can do things sniffers can't. For example, a keylogger can steal encrypted passwords and information. That's because the keylogger reads the information before it's encrypted.

The most common keyloggers are of the software variety. These are the ones that parents and companies buy to monitor children and employees. Hackers also build keyloggers into viruses.
Most security software will stop a software keylogger from installing. Whoever installs the keylogger usually needs access to the computer. They can tell the security software to ignore it.

Continued on the next page

Once a keylogger is installed, it is invisible. However, you can use specialized software to detect and remove it. So, it will work for the scenario you've set up.

With a software keylogger, the entire computer would have to go to a forensic lab. There's nothing to physically remove. If you want something physical, a hardware keylogger is a better bet.

Hardware keyloggers are easy to find online. They cost anywhere from $100 to $300. It depends on the amount of keystrokes the keylogger holds and level of data encryption.

Hardware keyloggers aren't as sophisticated as software keyloggers. They can record keystrokes, and that's it. They don't capture screenshots or mouse movement.

The amount of data they can store is somewhat limited. Some can record as little as 200,000 keystrokes. However, more expensive models can record millions.
Hardware keyloggers can't send the recorded data remotely. The keylogger's owner has to manually get the data off the gadget. That means visiting the computer regularly in person.

However, the hardware variety has some advantages, depending on how you look at it. First, you can't detect a hardware keylogger with software. It won't trip security systems or betray itself in any way.

Secondly, it's very easy to install. Unplug the computer's keyboard and stick the keylogger into the keyboard's port. Then plug the keyboard into the keylogger. You're done.

Thirdly, hardware keyloggers are very hard to spot. They're very small. When they're attached to the keyboard, it looks like a slightly long keyboard connector. Plus, the keyboard usually plugs in at the back of the computer. Who looks there?

With a hardware keylogger, you can physically remove it. That means you can turn it over to the police. You won't have to turn over your entire computer.

There are even trickier hardware varieties, as well. Some hardware keyloggers work on laptop keyboards, for example. Others can hide inside other USB gadgets. Image a keylogger hidden in your mouse or keyboard. How would you know it was there?

Fortunately, the hidden variety isn't readily available. Most often they're created by security researchers for testing purposes. However, the basic concept is certainly possible for any proficient hacker and plausible for your plot.

Hopefully that information gives you some good ideas for the book. For everyone else, you can keep on your guard against these threats. It never hurts to be informed. Writing a book can be a lot of fun. However, at some point you probably want to share it. You might even want to try selling it.

Help, I Lost My Phone!

http://askbobrankin.com

Losing a mobile phone can be a very big deal. Your phone probably contains all of your contacts, sensitive personal information, and perhaps work-related confidential data. Not to mention that smartphones can cost several hundred dollars. While there is no sure-fire way to recover a lost or stolen phone, here are a few tricks you can try.

Several carriers offer subscription services that will display the location of your phone(s) on a map. You have to sign up for these services before you lose a phone, because the activation process involves changing some settings or responding to a text message on the phone (s) you wish to enroll. Prices range from $5 to $10, allowing you to track two to five phones. Verizon calls it Mobile Recovery, AT&T offers Family Map, and Sprint has the Family Locator service.

Lost Phone Recovery Apps

If you have an Apple iPhone, you can access the "Find My iPhone" app via a Web browser.
Find My iPhone will display the current location of your iPhone on a Google Map, if the phone is turned on. If you can't find the iPhone, you can use Find My iPhone to disable it remotely the next time the phone connects to the cellular network. Find My iPhone was originally part of Apple's paid MobileMe service, but it's now part of the free iCloud service.

Another alternative is the $3.99/year iHound locator service. The iOS version works with iPhones, iPads, iPods, and iPod Touches. It tracks your device's location. You can push a command to a device that sounds a siren alarm. There's also an Android version that costs the same and does even more. You can send commands to disable the Android phone, and even wipe all of your data from the phone remotely.

Blackberry users can subscribe to the Berry Locator service for $6.95 per month.
It will send a message to your missing Blackberry and show you its location on a Web-based map.

Gadget Trak Mobile Security is a $19.95/year service for Android, Blackberry, and iOS devices.
It does tracking; sounds an alarm on a stolen phone; backs up phone data to a remote server;
and wipes a phone upon receipt of a special SMS message.

Pintail is a free app for Android phones that can help to find a lost or stolen phone. Once the app is installed, you can borrow a friend's phone and send your phone a text message with a PIN code. Pintail will use GPS services to locate the lost phone, and then send a text reply containing the phone's physical location and a link to Google Maps. Pintail can be downloaded from the Android market.

Even if you don't have any locator apps or services pre-installed on your phone, you can still try some old-school tricks to recover a lost or stolen phone.

Call the phone right away, using another phone. If you're lucky, your phone will ring and you will hear it under the sofa cushion. Or some good Samaritan may answer and agree to return your phone, especially if you promise a nice reward. Texting a plea for the phone's return, along with a financial incentive, is another tactic you can try. If all attempts to find a lost or stolen phone are fruitless, ask your carrier to disable the device, so you won't be liable for any misuse.

Read more: http://askbobrankin.com/how_to_find_a_lost_or_stolen_cell_phone.html#ixzz1gd5LmCmZ

Is Your Internet Security up to Date?

Antivirus up to date?

Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

http://gtbpcug.org/protect/

More about Internet Threats

How do I keep malware from reaching my machine in the first place?

by Leo A. Notenboom, © 2011

Q. Is there any way of keeping Adware from getting ON the computer in the first place? I already have several programs that take it OFF, but that still gives it the opportunity to clog up my connection (which it does!). How can I keep it from getting ON the PC in the first place?

A. I'm going to expand this from just "Adware" to all forms of malicious software or "malware" because the concepts and principles are the same. Even though many forms of adware (advertising software) are not strictly malicious, they can be annoying, as you're currently experiencing.

The answer depends on the specific malicious software or adware that you're having trouble with, but it typically falls into one of three categories.

You are the best defense

A lot of malware - I'll guess perhaps even as much as half these days - is malware that you've explicitly invited onto your computer.

In other words, you may well be doing it to yourself.

"I know it's not intentional - perhaps it's accidental or simply not realizing that this might be happening..." How?

Returning to sites that repeatedly install the software with which you're having problems.
Downloading and installing software that includes the malware.
Opening email attachments that turn out to include the malware.

Continued on the next page

There are probably even more ways that simply boil down to your allowing, or even asking, that the malicious software to be installed on your machine. I know it's not intentional - perhaps it's accidental, or simply not realizing that this might be happening - but it's frighteningly common.

That's why I say that **you** are the best defense.

The next time that you've cleaned something off of your machine and you expect it to return, take care to watch specifically what you're doing that might end up inadvertently inviting malware onto your own machine.

Removal tools are often prevention tools

Many of the tools that we'd consider malware removal tools are actually malware prevention tools as well.
Anti-virus and anti-spyware tools sometimes have options to monitor your computer for incoming malware and stop it in its tracks if they're configured properly.

Firewalls prevent malicious software from entering your machine over the network.

Keeping your machine's software - both OS and applications - up-to-date removes the software vulnerabilities that malicious software often exploits to infect your machine.
Tools like WinPatrol can also alert you to suspicious activity so you can choose to block it should you want to.

The take-away here is to perhaps take an inventory of how you have your machine protected and make sure that it includes all of the basic steps for internet security.

Sometimes, stuff happens

Even with the best of plans and tools, stuff can still happen. It shouldn't be often, and it needn't repeat, but as I've often pointed out, detecting and preventing malware is actually a race. Malware authors are always attempting to exploit unpatched vulnerabilities and devise new ways of avoiding detection. On the other side of the battle, software vendors are patching discovered vulnerabilities and anti-malware tools vendors are devising new techniques to detect all the new ways that malware can be hidden. In the middle is a window where even a fully protected machine can still remain vulnerable to the latest malicious software.

I'll also remind you that backups are for more than hardware failures - restoring to a full backup taken prior to a malware infection is often the most effective approach to ensure that malware has indeed been completely removed.

Some things to look into…

http://www.komando.com/toolbox.aspx?mode=print&id=11805

Filtering e-books also seems necessary these days. This link tells you all about it.

http://store.pugetsoundsoftware.com/maintaining_windows_xp_-_a_practical_guide.php

Windows XP isn't dead yet. Here you find out how to preserve it and continue to enjoy it.

http://tinyurl.com/7c7wb5q

Goodbye, desktop PCs--hello, flexible cell phone screens and living rooms with endless entertainment and gaming possibilities!

http://support.microsoft.com/default.aspx?scid=KB;en-us;306214&

How to create and use a password reset disk for a computer in a domain in Windows XP.

_____ _____ _____ _____ _____ _____

Tips:

http://softwarespot.wordpress.com/software/proeject/

ProEject is an easy to use application which allows you to safely dismount a removable drive by closing running applications and open windows, as well as clearing the registry and folders of any trace that the USB drive might have left behind. By placing ProEject on the same drive you want to eject and running, will automatically eject the drive with little fuss.

http://askthecomputerlady.com

Dear Computer Lady,
Is there a way to get Outlook Express dbx files that I had in XP to work now that I have Outlook, which does not open dbx files, in Windows 7?
Thanks for all your tips in your newsletters. You have saved me so many times while learning to use my computer.

Thanks! Mary

Dear Mary,

Outlook does not open DBX files from Outlook Express, but it will import the messages from the files. The easiest way, is to import your messages from the dbx files into Windows Mail, then use the following steps to import the messages from Windows Mail into Outlook.
Just open Outlook, click on the "File" tab, click on, "Open" and then click on "Import".
The "Import and Export Wizard" window will open. Click on "Import from another program or file" and click the "Next" button. In the next window, click on "Outlook Express 4.x, 5.x, 6.x or Windows Mail" and click the "Next" button.
Outlook will automatically import the messages from Windows Mail.

The lighter side

The Comfort Zone

I used to have a Comfort Zone,
but no one did I tell,
the same four walls of busy work
were really like a jail.

I longed so much to do the things
I'd never done before,
but I stayed inside my Comfort Zone
and paced the same old floor.

I said it didn't matter
that I wasn't doing much,
I said I didn't care for things
like diamonds, furs and such.

I claimed to be so busy
with things inside my zone,
but deep inside I longed for
something special of my own.

I couldn't let my life go by
just watching others win,
I held my breath and stepped outside
to let the change begin.

I took a step and with new strength
I never felt before,
I kissed my Comfort Zone "Good Bye"
and closed and locked the door.

If you are in a Comfort Zone
afraid to venture out,
remember that all winners were
at one time filled with doubt.

A step or two and words of praise
can make your dreams come true
and greet your future with a smile
success is there for you.

Author unknown

Some material appearing in this Newsletter was sent to the editor by other members. Thank you.

The group also welcomes two new members. Fred Buss and Brad Ward. Welcome!

Legal Notice

Bay Bytes, Copyright © 2012, is the official newsletter of the Greater Tampa Bay PC User Group, Inc.(GTBPCUG). The information in this newsletter is intended to help our members. It has come from many sources and cannot always be verified. It is recommended that you obtain professional advice from software and hard ware distributors, manufacturers, salesmen, or other professionals dealing with the subjects that appear in this newsletter. Unless specifically stated otherwise, the opinions expressed in Bay Bytes articles and columns are those of the individual authors and do not represent an official position of, or endorsement by GTBPCUG.GTBPCUG is not affiliated with any company, vendor or equipment manufacturer. Permission for reproduction of Bay Bytes in whole or in part is hereby granted to other APCUG user groups for internal, non-profit use, provided credit is given to the author, GTBPCUG Bay Bytes along with the copyright notice. Other reproductions require the prior permission of the editor. When published, please send a copy of your newsletter to

editor@gtbpcug.org or mail to P.O.Box 501, Brandon, FL, 33509-0501.