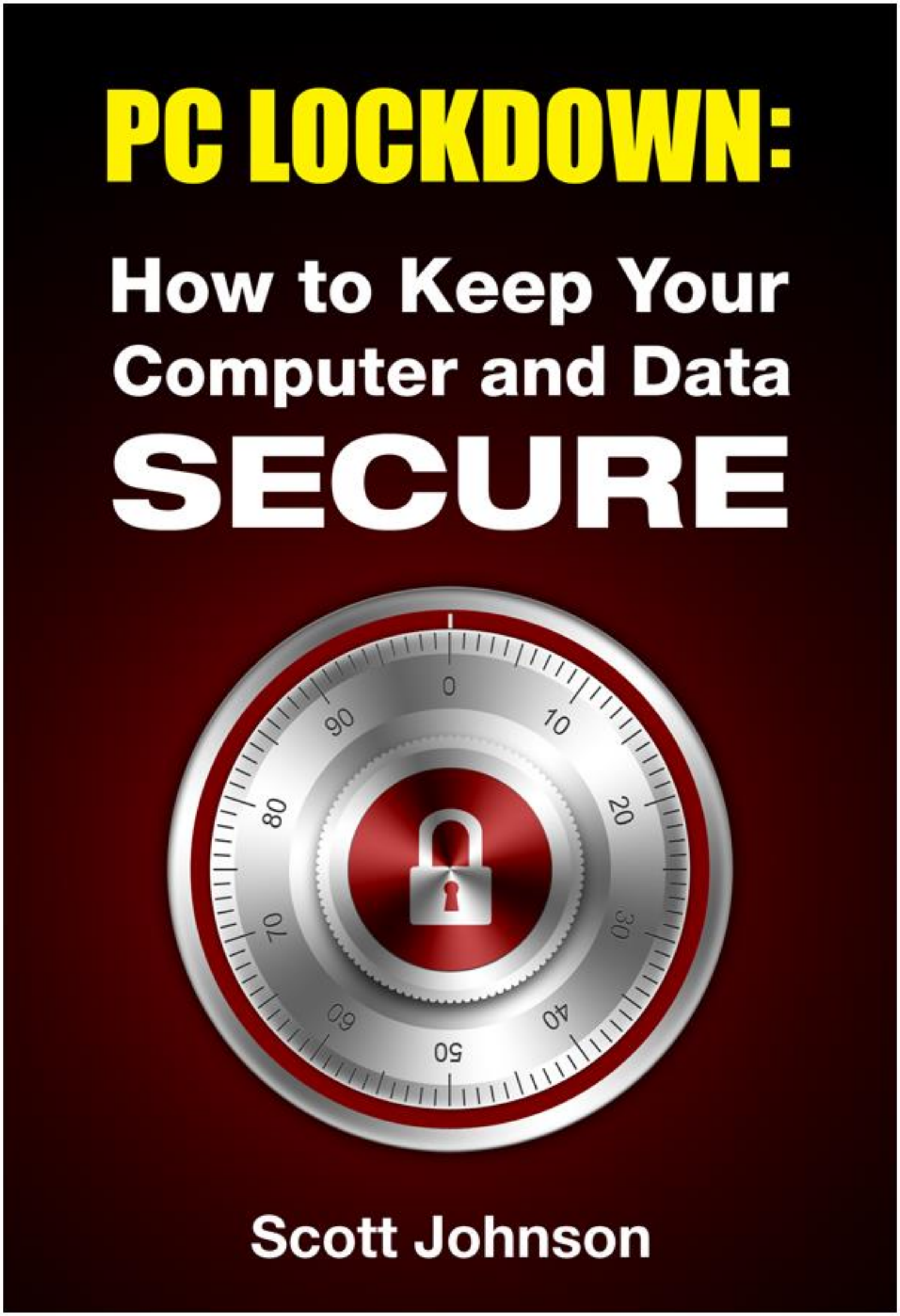


PC Lockdown: How to Keep Your Computer and Data Secure

Disclaimer:

The information presented in this guide is intended as a guideline for computer security. If you have data on your computer that is critical to your life or your business, you should consult directly with a computer professional to insure that your data is safe and secure. The author of this guide assumes no responsibility, legal or otherwise, for the actions that you take with your computer or your data. The internet and the world of computing changes rapidly; you alone are responsible for how your data is handled and what steps you need to take in order to secure it.

Rights:

This guide is protected under copyright laws. You may not sell it. You may not alter the contents. However, **you may give it away** as long as nothing is changed from the original.

Table of Contents

Introduction

Your antivirus/antimalware protection

How to create a GOOD password

Email – where security is inconvenient but necessary

Surf the web safely

Don’t get FOOLED on FACEBOOK

Hide your private information

Craigslist – lots of bargains, lots of scammers

Secure your data with an automated backup

A Final Word

Introduction

I have been working with computers – my own, and those of my clients – for quite a few years. My experience has taught me a few things.

First, hard drives will die. It is not a matter of "if", but rather "when". The hard drive in your computer is where all of the data is stored – all of your pictures, your videos, your collection of iTunes music, your tax returns, your email (if you use an email program such as Outlook or Windows Live Mail), your contacts list and more. For many people, that information is critical, and they would be in a very bad situation if it were all to suddenly disappear.

But, there is a certain type of phone call I get on a regular basis. It goes something like this:

> *"HELP! I went to turn on my computer this morning, and it's not working! I just get this message on the black screen that says HARD DISK NOT FOUND. What does that mean? Is all of my stuff gone? My whole life is on there! HELP!"*

In many cases, I am able to recover the data. In some cases, it is gone permanently. That's sad. I want to keep you from being that person.

Second, things are not always what they seem. That email you just got from Grandma, that says she found this great website and here's the link to check it out? It might not be a website you want to go to (the email might not even be from Grandma). Or the email from your bank, saying they need to confirm some information in order to protect your account – it's a scam. Some of them are pretty clever, too. I want to keep you from falling for these things by helping you recognize them.

Third, protecting your computer and your data from crashes and predators is not really difficult. The problem is, a lot of people just don't know what needs to be protected, or what steps to take to make sure their data is secure. If they knew how to do it, they would do it. I want to make sure you know how to do it.

I will cover a variety of areas in this guide, but keep in mind that the internet and computer security is a rapidly evolving area. The things I point out are great, but you need to be kept up to date regularly. One of the best ways to do that is to get my email newsletter. It is free. I will send you a tip each Monday, and whenever something important comes up that you should be aware of. You can sign up for it at my website, http://www.ComputerTutorFlorida.com.

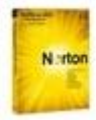
Stay safe,

Scott Johnson
The Computer Tutor

Your antivirus/antimalware protection

At the risk of stating the obvious, your computer needs to have an antivirus program. It should be obvious, but as I write this I recall a visit just yesterday with a client who was having computer troubles. As I did my analysis I wanted to see what antivirus program she was using. There was **no** antivirus program installed. There was one previously (although she didn't know which one) but now it was gone. Fortunately the situation was salvageable with no data lost. She now has an antivirus app installed.

The antivirus is one of your first lines of defense in protecting your computer from attracting or acquiring malicious software. You have a bunch of options:



Norton

AVG

Kaspersky

Vipre

Nod 32

Avira

Trend Micro

McAfee

MSE

These are just a few of the common ones. Some are free, some you pay for. I've tried most of these, and in general the free ones aren't as good as the paid ones, but there are exceptions to that.

I won't go into a history of what programs I have recommended in the past (you can read about that on my blog if you want – it's *really* exciting, believe me).

What I recommend you use to protect your computer from any virus, malware, junkware, spyware, whatever you want to call it – is my **Managed Service Plan** (MSP). This includes:

- Managed antivirus/antimalware software powered by Vipre (award winning program)
- Unlimited virus removal for 6 months or 12 months
- Automated software updates for programs such as Java, Adobe Flash, and dozens of others – so you never have to wonder if that "update" you're being asked to click on is legitimate. It's all done for you behind the scenes.
- Continuous "mini-tuneups" each day to keep your computer running fast
- Hard drive health and available space are monitored

You can get full details on the MSP and pricing at **http://ComputerTutorFlorida.com/msp**

How to create a GOOD password

A while back, one of the computer magazines published a list of the 10 most commonly used passwords. Here they are:

1. Password
2. 123456
3. Qwerty
4. Abc123
5. Letmein
6. Monkey
7. Myspace1
8. Password1
9. Link182
10. (your first name)

For a lot of people, creating a password is just an inconvenience that they have to work around. So they make the password as easy as possible to remember – which means it is very easy for someone else to guess, which means you are no longer protected. If a program or a website is requiring you to create a password, there is a reason for it. Do it the right way!

Even if you just picked a random word and followed it with a random number, that would be a huge improvement over choosing your dog's name or your child's birthday.

Here's a trick to choosing a good password, then being able to remember it: think of a sentence. Let's say you think of this sentence:

My wife and I are proud parents of 4 children

You could actually even write that down if you think you might forget it. But it is easier to remember a sentence than a set of random letters and numbers. So the password you just created is: **MwaIappo4c**

My **w**ife **a**nd **I** **a**re **p**roud **p**arents **o**f **4** **c**hildren

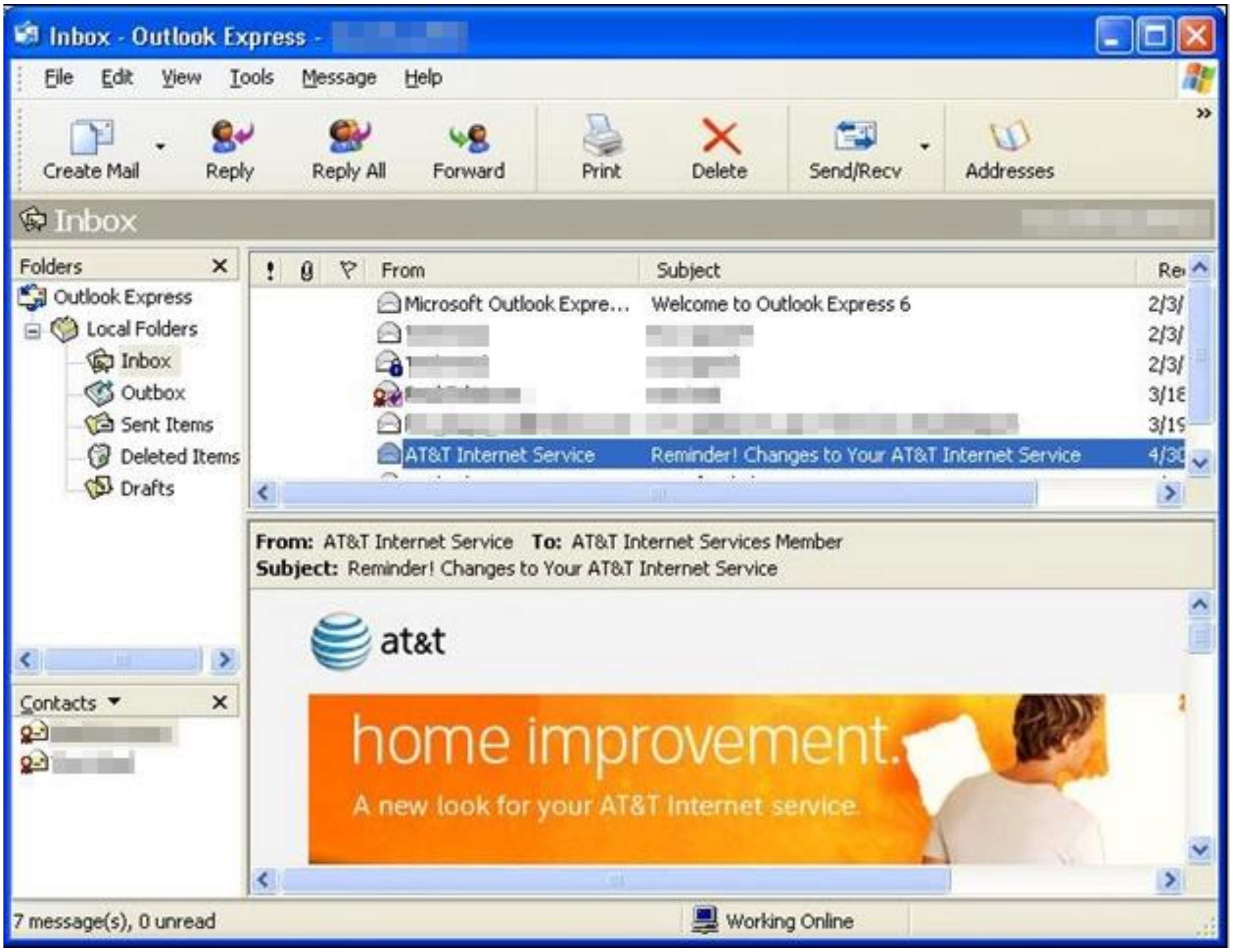
Look at that! You just created a password that has both numbers and letters, and upper and lower case, and it is not even a word that anyone would ever guess!

I shouldn't even have to say this, but a strong password is absolutely vital for anything related to financial matters – your online banking, your Paypal account, your eBay account, etc. But you really need to use a good password no matter what it is used for – it just makes sense, and it can save you a lot of troubles down the road.

Email – where security is inconvenient but necessary

There are a lot of ways to compromise the security of your computer, and several of them have to do with using email.

If you use Outlook, Outlook Express, Thunderbird, Windows Mail, or most other email programs, there is an option in the email settings to show the Preview Pane. This just means the window is divided in half, and one part displays the individual email "From" and "Subject" and the date, and when you click once on one of them, that email is displayed in the other half of the window. Here it is in Outlook Express:



From	Subject	Re
Microsoft Outlook Expre...	Welcome to Outlook Express 6	2/3/
[redacted]	[redacted]	2/3/
[redacted]	[redacted]	2/3/
[redacted]	[redacted]	3/18
[redacted]	[redacted]	3/19
AT&T Internet Service	Reminder! Changes to Your AT&T Internet Service	4/30

From: AT&T Internet Service **To:** AT&T Internet Services Member
Subject: Reminder! Changes to Your AT&T Internet Service

Can you imagine why this might not be a safe idea? It's because some emails contain malicious software that can be activated just by opening the email – you don't even have to open an attachment. Of course, if you have gone through all of your email settings for your particular email program and configured it properly, the likelyhood of that happening is slim – but have you configured your program accurately to prevent that? If you haven't, or if you don't know, you are better off turning off the Preview Pane in your email.

Another good policy is to not open attachments. Probably more viruses have been spread through email attachments than any other method. And it continues to happen, even though everyone knows that opening an attachment is a prime way to get a virus into your computer.   You're not going to let that happen to you, right?

Do you have a friend or relative that just loves to forward emails to everyone in their address book? You know what I mean – it's the person that sends you the emails that you don't even bother opening any more, you just delete them. Whatever is in the email, whether it's a joke, a picture of a cute kitten, or the latest "virus warning", these people feel that everyone needs this information. My advice is to get off that person's email list. Yes, you might cause a bit of hurt feelings, but it's only temporary. I am not on any list like that because most people know I don't want to see that junk filling up my inbox. Whenever someone sends me a forwarded email, I always send back this reply:

"Thanks for thinking of me,
but I really prefer to not receive email forwards –
I get way too much email already."

It's polite, it gets the message across, and I usually don't get any more junk email forwards from that person.

What about when there is a legitimate reason to send an email to a large group of people? Maybe you have an announcement that needs to go to 20 email recipients. If that is the case, you need to do it in a way that doesn't compromise the security of their email accounts.

The way to do that is not to copy and paste all 20 email addresses into the "To:" field. That just exposes everyone's email to everyone else, and it also makes the message look unprofessional because there is this huge list of emails at the top.

Instead, send the message "To:" your own email address. Then put everyone else's email into the BCC field (look closely, you will see that option). So when people get your email, it will look like this:

From: your email
To: your email
Subject: your subject

They won't even see their OWN address, or anyone else's. If you have a very large list of email recipients, such as 50 or more, you really need to use something other than a standard email program – Outlook isn't designed to do mass emails very well. There are email services available that can do a great job of it though, if you need to send out a newsletter or some other messages on a regular basis.

A lot of crap can come in through spam emails as well. If you find your email inbox filled with junk (and it will only increase, not decrease), I have an easy solution. Switch your email to Google's email service, Gmail. They have a great spam filter so I hardly ever see any garbage in my inbox. And you can keep that email address for life – much better than changing email accounts every time you change internet providers, right?

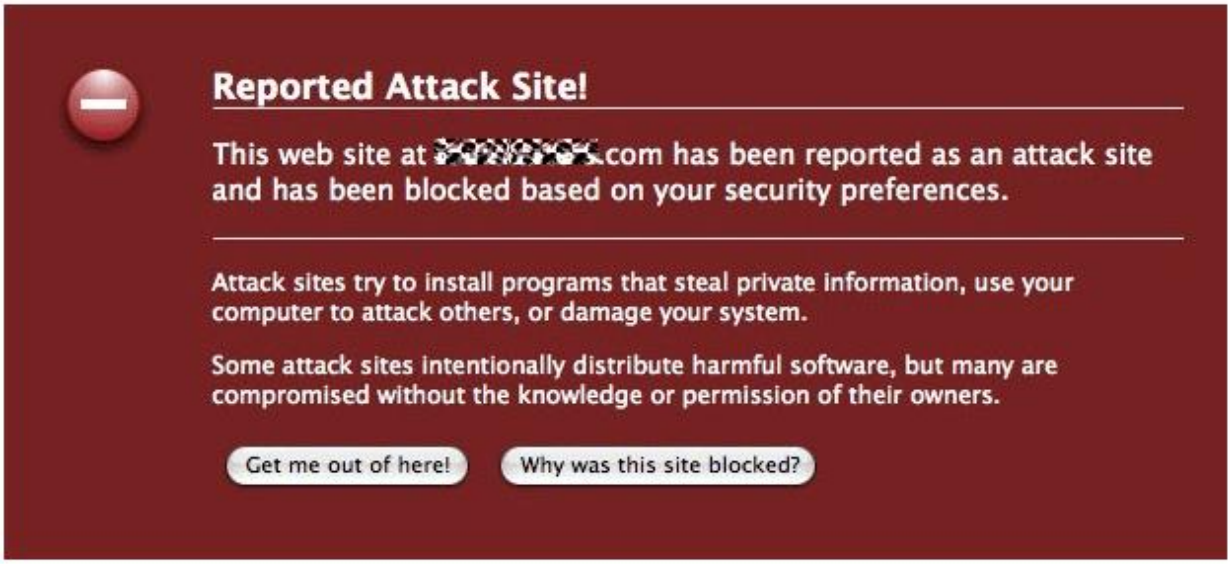
Surf the web safely

If you use your computer on any regular basis, you probably visit lots of different websites. There are a few people that just go to the same few websites all the time, but a lot of computer users like to “explore”. There’s nothing wrong with that, and the internet sure has a lot of interesting, entertaining and educational things to discover. But you have to be careful about how you do it.

There are some websites that are intentionally malicious. In other words, they will try to install bad software on your computer from the very first millisecond you are on that site. And sometimes you don’t even know that it is a bad site until you are already there.

So what is your defense? **Malwarebytes**, as listed earlier in this guide. The paid version of Malwarebytes has a great feature – when you click to visit a website that will try to harm your computer, Malwarebytes checks the site first and protects you by popping up a warning and not letting you get to that site (the free version of Malwarebytes does not have this feature). Of course, you can override the warning and go to the site anyway… but that would be kind of dumb, wouldn’t it? So that is one layer of protection right there.

Another security precaution you can take is to use Firefox as your web browser. If you are using Firefox and are about to go to a malicious website, you might very well see this warning pop up instead:



Reported Attack Site!

This web site at [redacted].com has been reported as an attack site and has been blocked based on your security preferences.

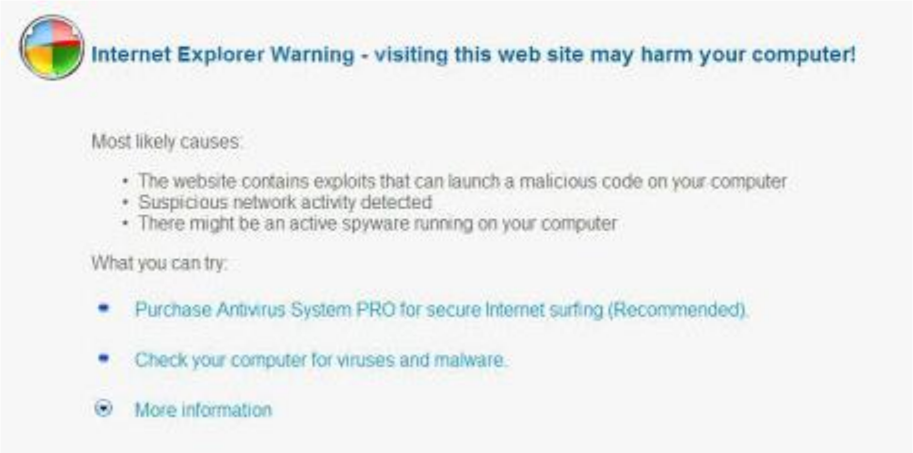
Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

If you see that, I highly recommend clicking the “Get me out of here” button and don’t go back. You do still have the option to visit the site, though (if you enjoy living dangerously). The image above does not show it, but in the bottom right corner there will be a small text link that says “Ignore this warning”. They make is small in the hopes that you won’t see it and click on it (but it’s your computer, so your option).

You can also choose to find out why this site comes up as a bad site – just click on “Why was this site blocked?”

If you use Internet Explorer, the most recent version, it should also pop up a warning to keep you from going somewhere you shouldn’t go. However, in the past Internet Explorer has been riddled with security issues and I just try to avoid using it whenever possible. Version 8 has made a lot of progress in that area, but Firefox has been safer than IE from the beginning so I usually use it anyway. Here is what the IE warning looks like:



Internet Explorer Warning - visiting this web site may harm your computer!

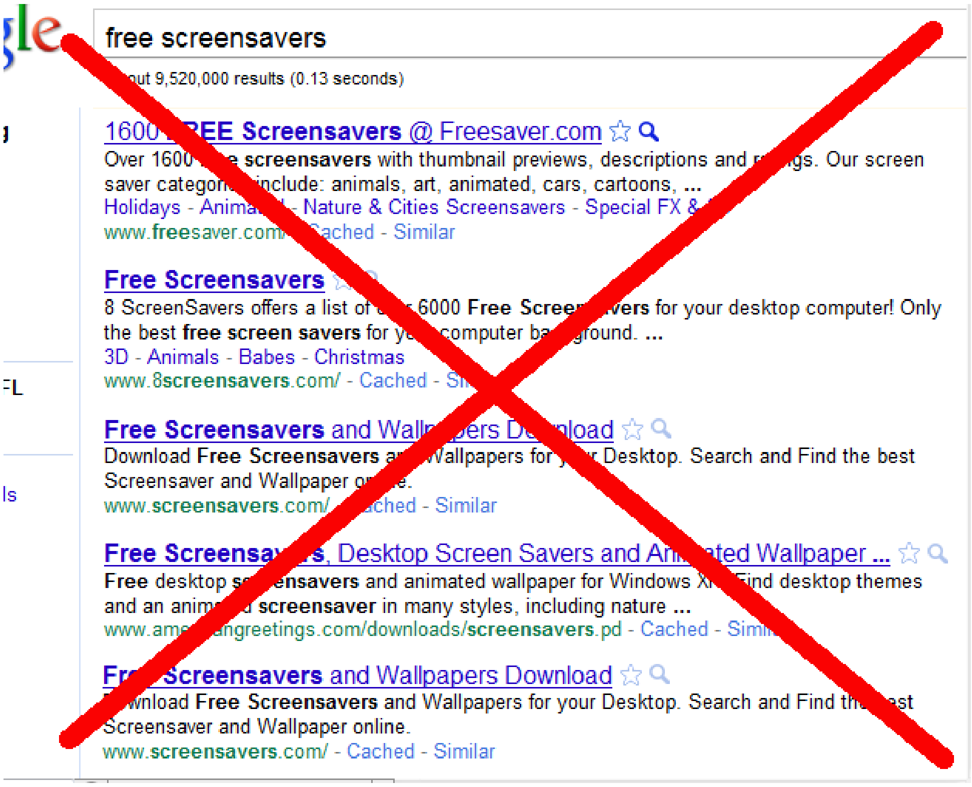
Most likely causes:

- The website contains exploits that can launch a malicious code on your computer
- Suspicious network activity detected
- There might be an active spyware running on your computer

What you can try:

- Purchase Antivirus System PRO for secure Internet surfing (Recommended).
- Check your computer for viruses and malware.
- More information

I will mention one other thing here about security when browsing the web. There is a seemingly innocent search that a lot of people do every day – people are looking for free screensavers. In fact, Google says that 246,000 people searched for "free screensavers" – and that was just last month! Like a professional pickpocket at an airport, spyware will be found wherever a lot of computer users go. That's why, if you do a Google search looking for free screensavers, most of the sites that come up in the results will be sites that are dangerous to your computer. They will try to install spyware, toolbars, and all kinds of other junk you don't want or need. That's why the screensavers are free! You pay for them in aggravation.



free screensavers

out 9,520,000 results (0.13 seconds)

1600 EE Screensavers @ Freesaver.com
Over 1600 e screensavers with thumbnail previews, descriptions and gs. Our screen saver categor include: animals, art, animated, cars, cartoons, ...
Holidays - Anima - Nature & Cities Screensavers - Special FX &
www.freesaver.com ached - Similar

Free Screensavers
8 ScreenSavers offers a list of 6000 Free Scree vers for your desktop computer! Only the best free screen savers for y computer ba ground. ...
3D - Animals - Babes - Christmas
www.8screensavers.com/ - Cached - Si

Free Screensavers and Wall ers D nload
Download Free Screensavers a Wallpapers for r Desktop. Search and Find the best Screensaver and Wallpaper o e.
www.screensavers.com/ ached - Similar

Free Screensa s, Desktop Screen Savers and An ted Wallpaper ...
Free desktop s ensavers and animated wallpaper for Windows X ind desktop themes and an anim screensaver in many styles, including nature ...
www.ame ngreetings.com/downloads/screensavers.pd - Cached - Sim

Fr Screensavers and Wallpapers Download
wnload Free Screensavers and Wallpapers for your Desktop. Search and Find th est Screensaver and Wallpaper online.
www.screensavers.com/ - Cached - Similar

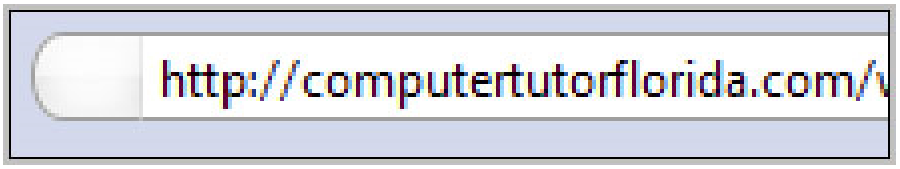
Here is something you need to know: **how to tell if a website is secure**.

It's a simple fact: some websites are secure, and some are not. There's no problem with that in itself; some sites do not **need** to be secure. My blog is not "secure", but that's fine because I am not asking you to enter any critical information.

But what if a website is selling something, and asking you to enter your credit card information? Before you input any information like that (credit card number, bank account number, social security number, etc.) you need to make sure that your data will be safe.

There is a quick and easy way to do that.

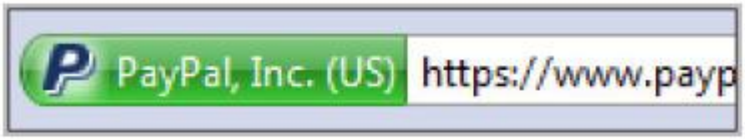
As an example, go to my site, and look up at the top of the page at the address bar:



http://computertutorflorida.com/v

See how the address for this site starts out with "http" – that means it is just a regular website, not one that you would want to enter your credit card into.

Now, if you go to my Remote Support Service (http://computertutorflorida.com/remote-support/) and click the Buy Now button, you will be taken to a site that does ask for a credit card:



PayPal, Inc. (US) https://www.payp

Notice the difference? This one starts with "https" – that extra "s" stands for **secure**. When you are making this purchase, you can either sign into your Paypal account, or just pay with a regular credit card if you don't have a Paypal account. Either way, the information that you enter will be secure.

This just means that the data you enter won't be "eavesdropped" into a third party computer while the transaction is taking place. Of course, the fact that a site is secure does not by itself mean that there are absolutely zero risks. But paying with a credit card is the safest way to purchase anything online, because you are protected against loss or fraud through your credit card company, or the merchant (or both).

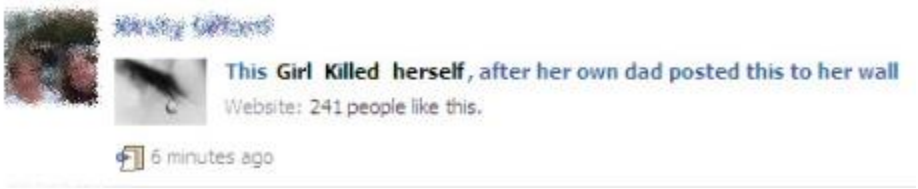
Don’t get FOOLED on FACEBOOK

First, let me say this – there’s nothing wrong with being on Facebook. Heck, I am on there all the time. Most people spend TOO much time on there, but that’s another issue. It really has become a great forum for finding old friends, and keeping up with people that you don’t often have a chance to see in person.

But like most things internet-related, Facebook has some danger points to watch out for when you are trying to protect your computer and your private information. You have to always be on guard for the unexpected.

First rule of Facebook – **don’t click any link if you don’t know where it will lead you**.

Here’s what happens. One of your Facebook friends gets a computer virus and doesn’t know it. He stays logged into Facebook all the time (even when away from his computer), so the virus now has full access to his Facebook account. One day this friend posts a message on your wall:



This Girl Killed herself, after her own dad posted this to her wall

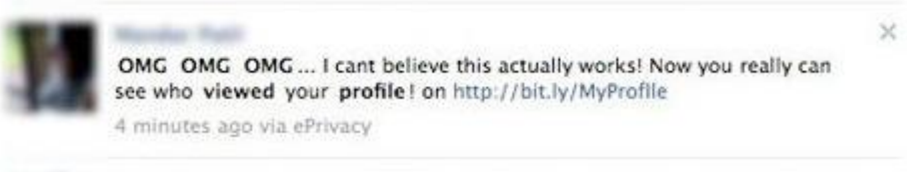
Website: 241 people like this.

6 minutes ago

As you probably already know that link will take you to a malware (malicious software) site that will try to infect your computer, then your own computer will start posting the garbage to other people’s walls, and it just spreads like wildfire.

I almost have to admire the creator of this one, because it so cleverly plays on people’s curiousity. I mean, wouldn’t you be just a little curious and want to click on that link to see the story and find out what happened? Don’t let your curiousity cause you some computer problems!

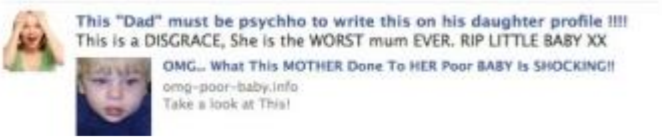
Another area of Facebook to stay away from are “hoax apps”. By this I mean Facebook apps that claim to be able to do something that they definitely don’t do. For example:



OMG OMG OMG ... I cant believe this actually works! Now you really can see who viewed your profile! on http://bit.ly/MyProfile

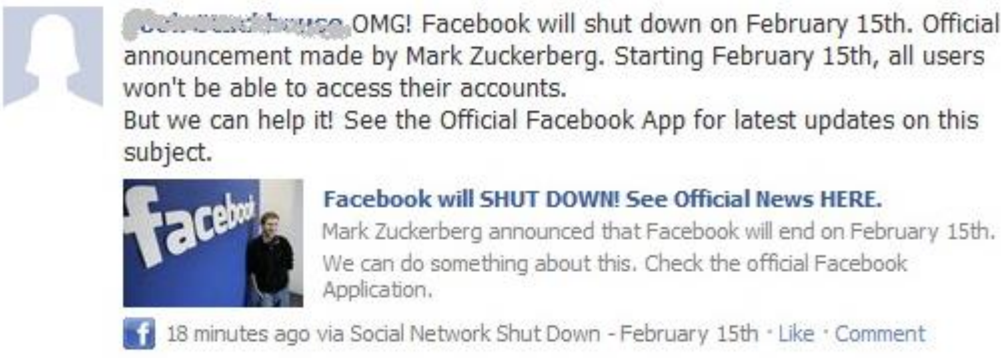
4 minutes ago via ePrivacy

Again, it plays on people’s emotions – wouldn’t you want to somehow know who has been viewing your profile page? But there is no app that would be able to track that. What actually happens is this: when you click to install that app, you are then giving the app permission to access your account and post to your wall. So of course it immediately posts a status just like the one you see above, so that all of your friends will see it and get the app too. Why would anyone do this? Traffic. They make money by having lots of visitors come to their app page, so the more this garbage spreads, the more money they make. In the meantime, you have spread this to all of your friends and then look foolish when you figure out that it was just a scam and you have to tell everyone to stop spreading it. Here are some others to avoid:



This "Dad" must be psychho to write this on his daughter profile !!!!
This is a DISGRACE, She is the WORST mum EVER. RIP LITTLE BABY XX

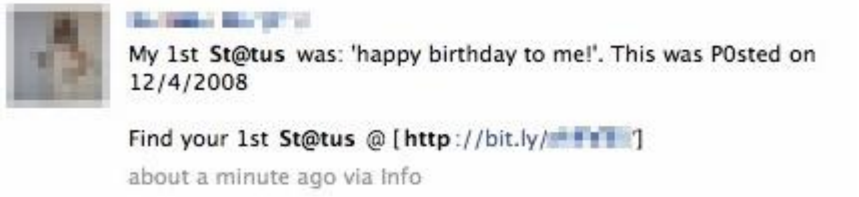
OMG.. What This MOTHER Done To HER Poor BABY Is SHOCKING!!
omg-poor-baby.info
Take a look at This!



[redacted] OMG! Facebook will shut down on February 15th. Official announcement made by Mark Zuckerberg. Starting February 15th, all users won't be able to access their accounts.
But we can help it! See the Official Facebook App for latest updates on this subject.

Facebook will SHUT DOWN! See Official News HERE.
Mark Zuckerberg announced that Facebook will end on February 15th. We can do something about this. Check the official Facebook Application.

18 minutes ago via Social Network Shut Down - February 15th · Like · Comment



[redacted]
My 1st St@tus was: 'happy birthday to me!'. This was P0sted on 12/4/2008

Find your 1st St@tus @ [http://bit.ly/[redacted]]
about a minute ago via Info

There are lots more, but you get the idea. If your friends start posting something that is different from what you normally see them posting, it's probably a hoax. When I see this on a friend's wall, I usually add a comment just to tell them it is a hoax, and to warn their other friends to not get suckered into clicking on it.

The interesting thing about this type of stuff is that no antivirus or antispyware program can protect against it. These fake Facebook apps don't usually install software on your computer, so there is nothing "suspicious" going on for your antivirus program to catch and stop. When you click on a hoax link, you are taken to the Facebook app page, and you have to grant it permission to access your account. If you do that, you are losing control over your account and giving it to this stupid little app that only wants to scam you and your friends.

Here is something else that people don't always consider when using Facebook: posting your vacation status. Tell everyone about your vacation, post pictures, post videos – but do it after you get back home. Think about it – when you go on vacation, would you put this sign in your front yard:

AWAY ON VACATION – HOUSE WILL NOT BE OCCUPIED FOR THE NEXT 10 DAYS

Of course not. But when you post your status that you will be out of the country (or even out of town) until some particular date, you are announcing that exact thing. This one is really just common sense, but believe me, I see it all the time on Facebook. Don't ask for trouble.

Ahhh! Sun, Sand, Beach.... Having an AWESOME Time on our vacation! OMG!!!

facebook
Search
News Feed
Top News · Most Recent 6
Everyone
Attach:
Share
thanks for the status update!!!

Now we need to talk about your **Facebook settings**. This is where you control **who** sees **what** on your Facebook profile, status updates, photos, etc.

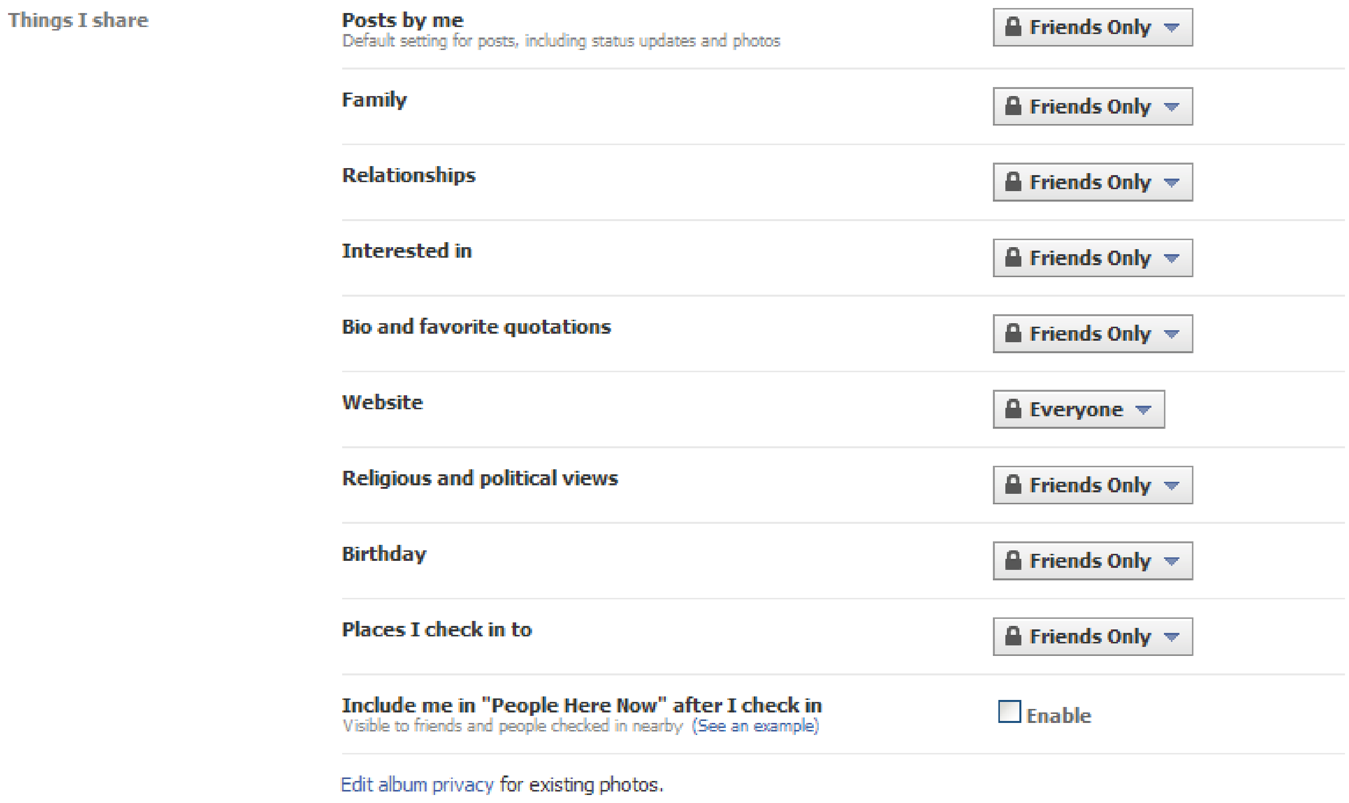
In the rest of this chapter, I am going to go over some specific steps you need to take to protect yourself and your computer while on Facebook. However, keep in mind that Facebook changes their layout and their policies on a fairly regular basis. By the time you read this, the pages shown may not look exactly like they do here. But the principal behind each recommendation would still apply.

Step 1: Privatize your information

You can control who sees your status updates, your birthday, your pictures, and lots of other stuff. There are essentially 3 groups of people that we are talking about giving access to your information:

friends, friends of friends, and everyone. You need to decide which of these groups can see the various components of your profile. I recommend making your details only visible to friends. Here is how to do that:

1. Click on Account – Privacy settings
2. Look for the link on the page that says “Customize settings” and click on it
3. On each of the items, choose “Friends only” in the drop down menu. In the “Things I share” section it will look like this:



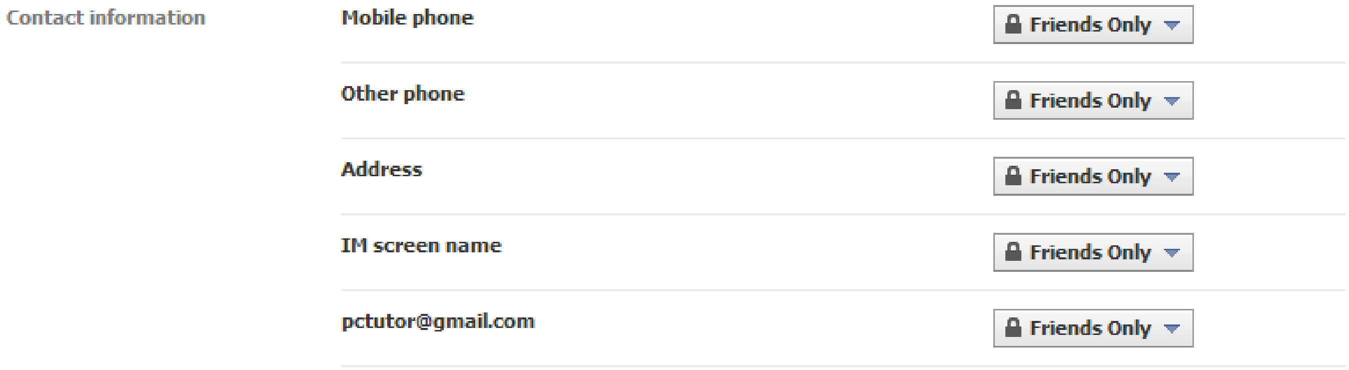
Things I share	Posts by me Default setting for posts, including status updates and photos	Friends Only
	Family	Friends Only
	Relationships	Friends Only
	Interested in	Friends Only
	Bio and favorite quotations	Friends Only
	Website	Everyone
	Religious and political views	Friends Only
	Birthday	Friends Only
	Places I check in to	Friends Only
	Include me in "People Here Now" after I check in Visible to friends and people checked in nearby (See an example)	□ Enable

Edit album privacy for existing photos.

(On my example above, I left my website visible to everyone because I want anyone to be able to see the site from a marketing standpoint.)

There is a section called “Things others share”, which can include items like when you get tagged in someone else’s photo or video. We’ll cover that in a few minutes.

At the bottom, there is a section called Contact Information. Here again, I would share this information only with those people that are your friends on Facebook. It’s fine for your best friend to know your phone number or address, but why should his or her co-workes or relatives need to know that? They don’t. So set this section to “Friends only” just like you did the other section. It will look like this:



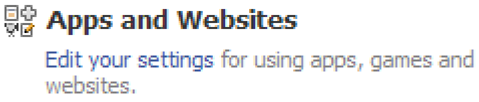
Contact information	Mobile phone	Friends Only
	Other phone	Friends Only
	Address	Friends Only
	IM screen name	Friends Only
	pctutor@gmail.com	Friends Only

Step 2: Privatize your information from Google

Now that your information can only be seen on Facebook by those people whom you have chosen to be your friends, we need to block Google from snooping around and displaying your info in search results. Otherwise, people could do a Google search on your name (and/or other identifying factors) and find the information in Google.

1. Click on Account – Privacy Settings

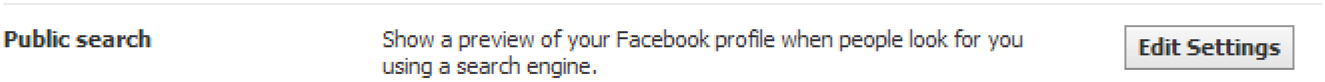
2. Look in the lower left corner for the Apps and Websites area, and click on "Edit your settings"



Apps and Websites

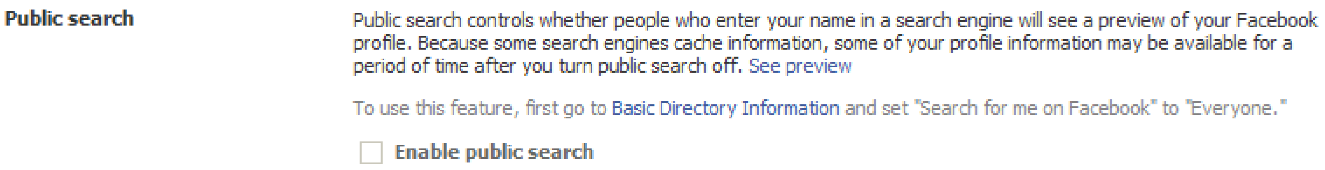
Edit your settings for using apps, games and websites.

3. Find the section called Public Search and click on "Edit Settings"



Public search — Show a preview of your Facebook profile when people look for you using a search engine.

4. Now find the checkbox for "Enable public search" and make sure it is UNchecked:



Public search

Public search controls whether people who enter your name in a search engine will see a preview of your Facebook profile. Because some search engines cache information, some of your profile information may be available for a period of time after you turn public search off. See preview

To use this feature, first go to Basic Directory Information and set "Search for me on Facebook" to "Everyone."

□ Enable public search

To check this, you can log out of Facebook and then do a Google search on your name, or your name plus your city, or your name plus your school, or any combination. Keep in mind it might take a little while for Google to get your info out of its index (a few hours up to a few days).

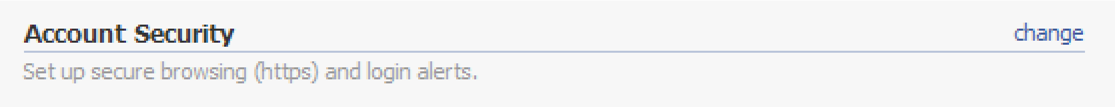
Step 3: Make your Facebook connection SECURE

It's pretty safe to say that anyone reading this has had their own Facebook account hijacked, or at least knows someone who has had this happen. We've all seen the status updates like this:

> *"Sorry everyone – if you got an message from me*
> *saying to click on a link, don't click it!*
> *I didn't send it! My Facebook account got hijacked."*

There is a simple way to prevent that from happening – just make your connection secure. Here's how:

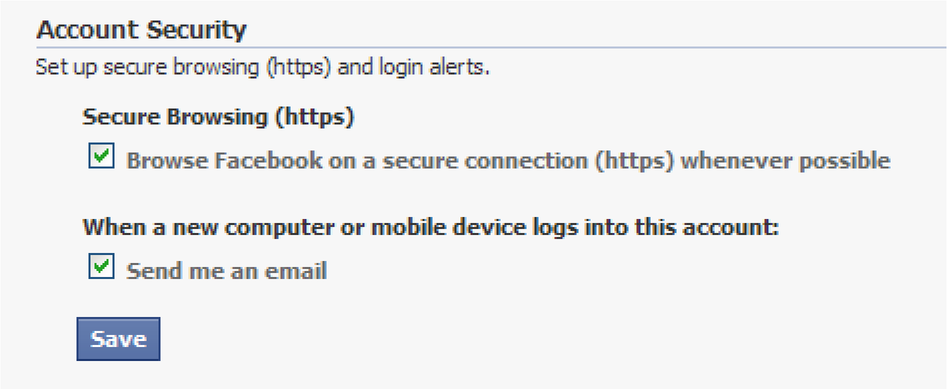
1. Go to Account – Account settings
2. Find the section called "Account Security" and click on "Change"



Account Security

Set up secure browsing (https) and login alerts.

3. Check the two boxes shown there and click Save:



Account Security

Set up secure browsing (https) and login alerts.

Secure Browsing (https)

☑ Browse Facebook on a secure connection (https) whenever possible

When a new computer or mobile device logs into this account:

☑ Send me an email

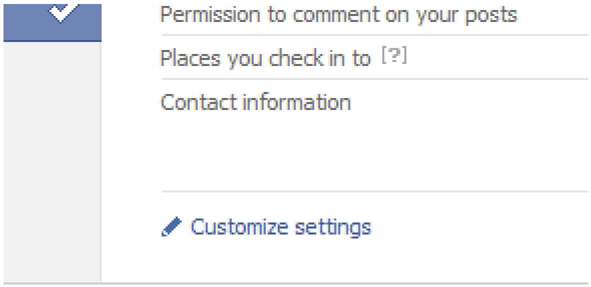
Now, you will only be browsing Facebook from a secure connection. And if someone else logs into your account, you will immediately be sent an email to advise you of that. Test it out yourself if you want – click Save, then go log into your Facebook account from a friend's computer and see what happens.

Step 4: Don't allow everyone to view your pictures

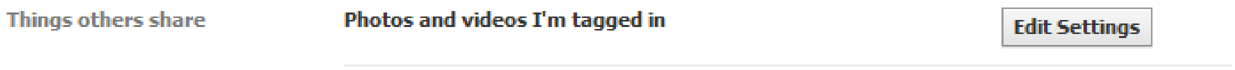
Without a doubt, there are pictures of you in other people's Facebook photo albums. It could be relatives, friends, co-workers – these days there are pictures being taken all the time and many of them get uploaded to Facebook.

The problem arises when people start "tagging" you in those pictures. When your image gets tagged, those pictures are immediately associated with you. They even show up on YOUR Facebook photo albums whenever someone visits your page and looks at your pictures. Why should friends of your friends be able to browse through all of your pictures? You should control who is able to see your pictures (or videos).

1. Go to Account – Privacy Settings and click on "Customize settings"

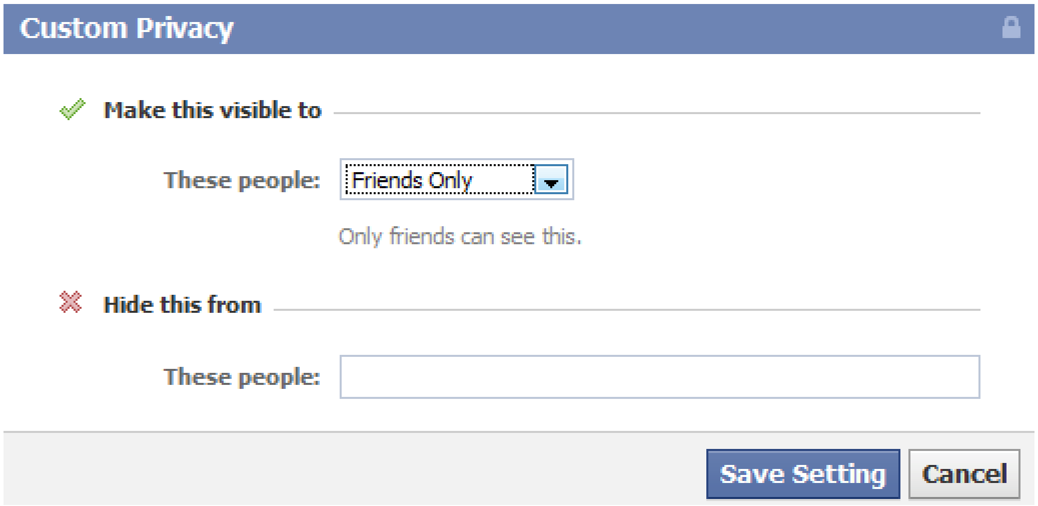

Permission to comment on your posts
Places you check in to [?]
Contact information
Customize settings

2. Scroll down to "Things others share" and find "Photos and videos I'm tagged in", then click the "Edit Settings" button



3. In the new window, click the dropdown menu and choose "Customize"

4. In the "Custom Privacy" Window, you can choose to allow your photos and videos to be viewed by friends, friends of friends, certain people, or only you. You can even specify certain people to hide your photos from:



These people: Friends Only

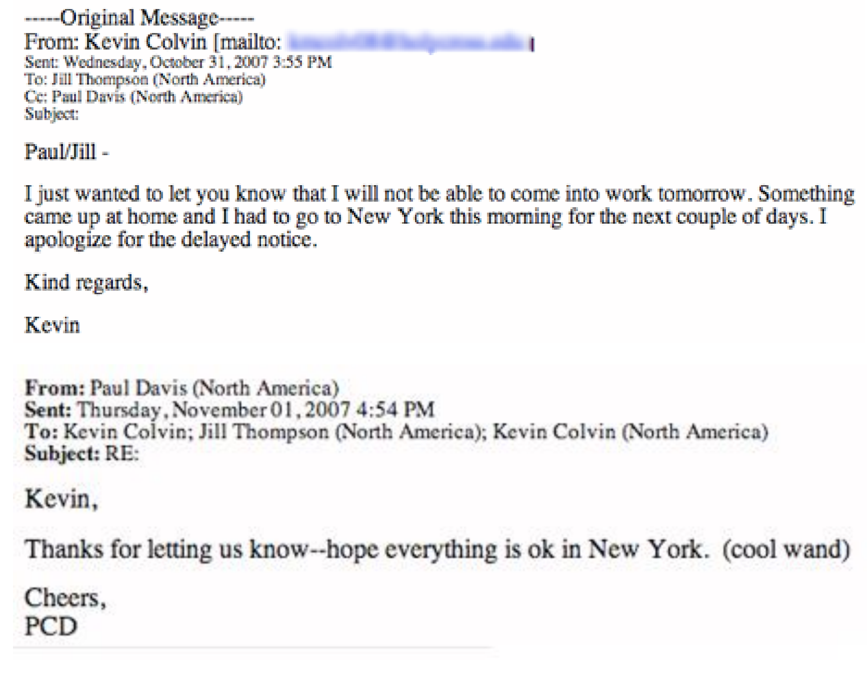
Only friends can see this.

These people:

The absolute safest plan is to hide your photos from everyone, so that only you can see them. But really, that kind of defeats the purpose of Facebook. Why even be on there, if you don't want to share some photos with your friends? You might want to block your boss from looking at your photos if they are incriminating or embarassing enough to potentially jeopardize your employment.

That reminds me of a story that directly relates to this issue. There was this bank intern named Kevin who sent his boss, Paul Davis, an email saying that he couldn't make it in to work the next day due to something that "came up at home". In reality, Kevin was planning to attend a Halloween party that would go late into the night, and he knew he would be in no shape to come to work after that.

Unfortunately for Kevin, there were cameras and Facebook users at the party, and Kevin was tagged in a few of the photos. Kevin's boss is on Facebook, and he was able to pretty easily stumble across the photos. He replied to Kevin's "can't come to work email" and attached a photo – and CC'd the rest of the office on the reply:



-----Original Message-----
From: Kevin Colvin [mailto: [redacted]]
Sent: Wednesday, October 31, 2007 3:55 PM
To: Jill Thompson (North America)
Cc: Paul Davis (North America)
Subject:

Paul/Jill -

I just wanted to let you know that I will not be able to come into work tomorrow. Something came up at home and I had to go to New York this morning for the next couple of days. I apologize for the delayed notice.

Kind regards,

Kevin

From: Paul Davis (North America)
Sent: Thursday, November 01, 2007 4:54 PM
To: Kevin Colvin; Jill Thompson (North America); Kevin Colvin (North America)
Subject: RE:

Kevin,

Thanks for letting us know--hope everything is ok in New York. (cool wand)

Cheers,
PCD

Step 5: Limit information available to applications

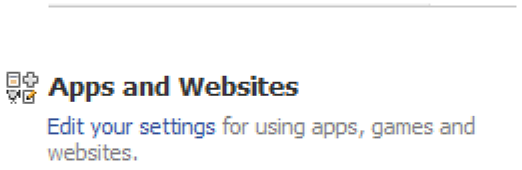
This is a big one, and one that a lot of people are not aware of.

You know all of those games that are so addictive to so many Facebook users? Farmville, Farmtown, FarmoMania, Mafia Wars, etc. – I just don't get why people would sit around and play those mindless time-wasting games in the first place. But they do – millions of them. People even pay money – REAL money – to buy items in the game, such as wood to build their pretend "barn" or ammunition to defend their pretend "Mafia" family. If you are one of the people that really gets into those things, don't take offense – how you ~~waste~~ spend your time is up to you. It's just not for me.

But wait, it gets worse. The goal of these games is to access information – your personal information. And the real kicker is, the games can get access to your private data **even if you never sign up for a single mind-numbing one of them**! How? Through your friends. That's right – if your friend plays

Aquarium Town, that game could get access to your data just because of your connection to your friend. That is, unless you block it – which you should:

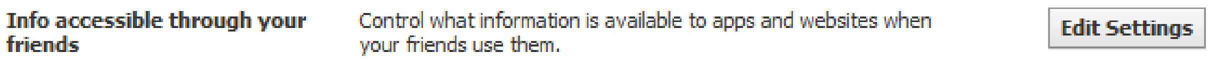
1. Go to Account – Privacy Settings. Find "Apps and Websites" and click on "Edit your settings"



Apps and Websites

Edit your settings for using apps, games and websites.

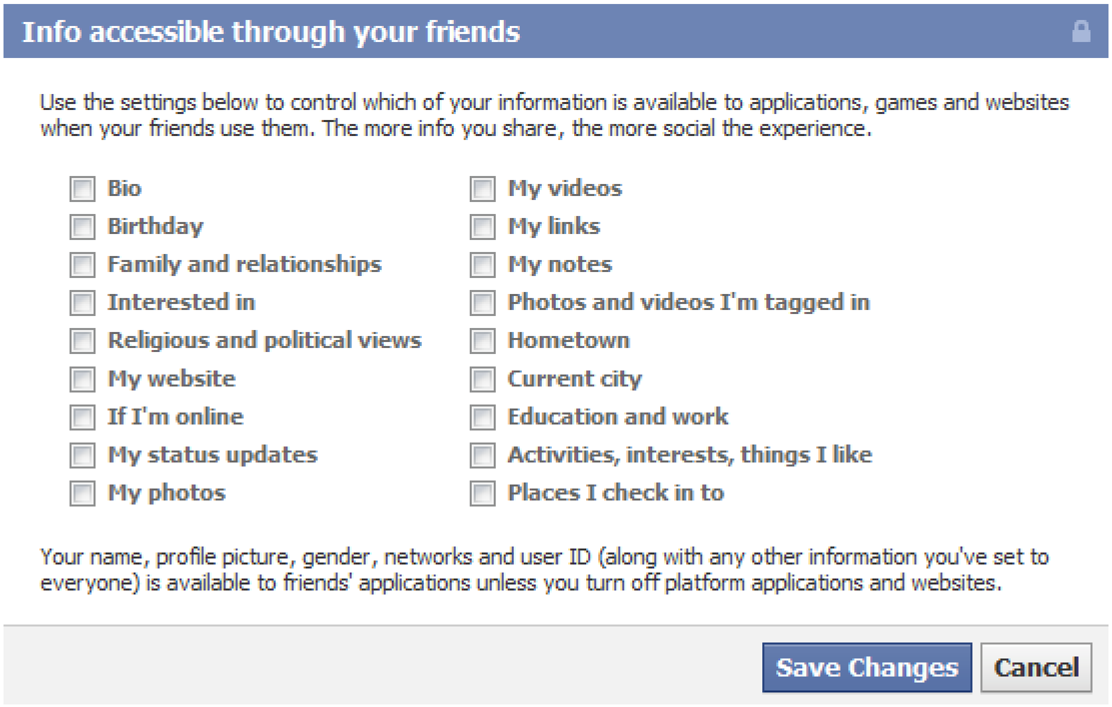
2. Find "Info accessible through your friends" and click the "Edit Settings" button:



Info accessible through your friends

Control what information is available to apps and websites when your friends use them.

3. Now UNcheck every single box and click Save Changes



Info accessible through your friends

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

☐ Bio
☐ Birthday
☐ Family and relationships
☐ Interested in
☐ Religious and political views
☐ My website
☐ If I'm online
☐ My status updates
☐ My photos
☐ My videos
☐ My links
☐ My notes
☐ Photos and videos I'm tagged in
☐ Hometown
☐ Current city
☐ Education and work
☐ Activities, interests, things I like
☐ Places I check in to

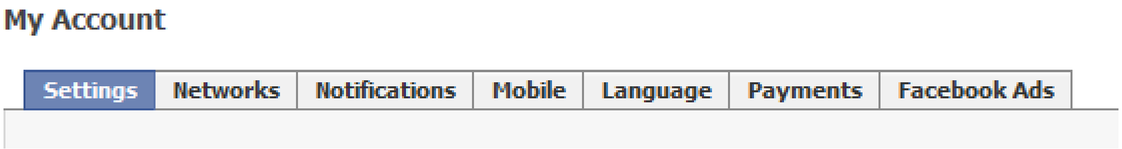
Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.

Step 6: Don't allow Facebook to use your pictures in their ads

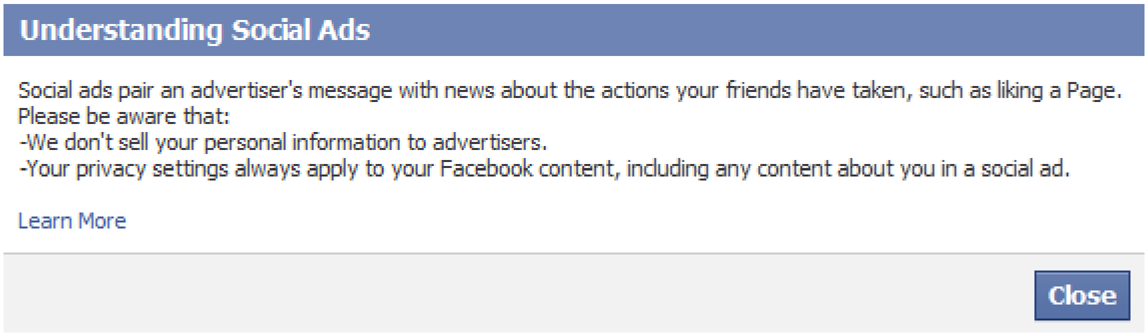
This one is really another no-brainer. Think about all the pictures stored on Facebook right now. That is a huge business asset for them, and at some point they are going to want to use those pictures to help them make money. They are planning to use people's personal pictures in the Facebook ads that show up on the right-hand side of the screen.

Imagine some day seeing a Facebook ad for a cure for constipation – and there's your face in the ad! Well, we're going to nip that one right now:

1. Go to Account – Account Settings and click on the tab that says "Facebook ads"



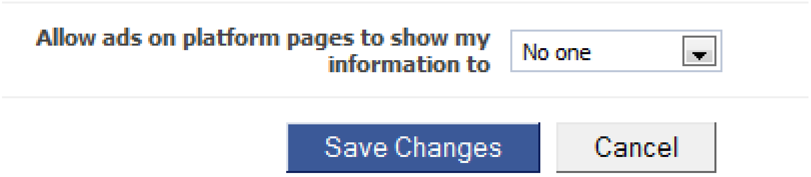
2. They will pop up a pathetic "here's why it's not bad" message. Just close it.



Understanding Social Ads

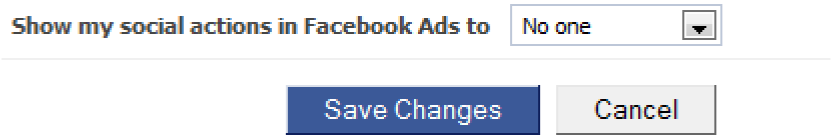
Social ads pair an advertiser's message with news about the actions your friends have taken, such as liking a Page.
Please be aware that:
-We don't sell your personal information to advertisers.
-Your privacy settings always apply to your Facebook content, including any content about you in a social ad.

3. In the first drop-down menu at the top, choose "No one" and Save Changes:



Allow ads on platform pages to show my information to: No one

4. Scroll to the bottom and choose "No one" in that menu also:



Show my social actions in Facebook Ads to: No one

There may be other areas of Facebook privacy where you want to take action to protect your information. It is a good idea to explore all the possibilities in the "Privacy" and "Account Settings" sections just to see what could be lurking in there to compromise your security.

Hide your private information

Do I really need to say that? Yes. Yes I do. I know this from personal experience.

When I do personal computer instruction, I sometimes will visit the client’s home or office. It’s better to learn on your own computer; that’s why I prefer to either come to you or connect remotely.

There is something that I have seen many, many times when working at one of my client’s personal or work computer (more often when we are at the house, using the personal or family computer). It looks sort of like this:

So I am sitting there working on various things on the computer, and I can see all of these post-it notes – the login information for the client’s online bank account, email password, Facebook password, you name it.

As you read this, take a quick look around the edge of your monitor. Any stickies with information that you wouldn’t want other people to have access to? If so, take it off the monitor and keep it hidden.

Craigslist – lots of bargains, lots of scammers

Craigslist is a great resource if you use it carefully. I have bought and sold a lot of items using Craigslist. Some of my computer customers have found me through Craigslist.

craigslist

On the other hand, Craigslist is crawling with scammers that want to steal your money. Most of them are outside the US, so if you do send money to them, it's gone with virtually no chance of getting it back.

I am not going to go into all the details of what Craigslist is – most of you have probably already used it and have a fairly good idea. If you are not familiar with it, you can go check it out – http://craigslist.org. The reason scammers are attracted to Craigslist is because they find lots of inexperienced internet users there, many of whom have money in hand ready to buy when they see a bargain.

And these scammers sure know how to sell a bargain!

Not long ago I was shopping for a car for my daughter, and I checked Craigslist regularly. There are lots of cars for sale on there. I found a Honda that seemed like a fantastic deal – in fact, too good to be true. I knew it was a scam from the start, so I strung the scammer along for a while and posted the whole story on my blog. It is one of my most popular blog posts, and people still find it every day. You can read the entire episode here:
http://computertutorflorida.com/2010/08/craigslist-scam-selling-non-existent-cars/

Craigslist rule #1: Don't buy anything from someone who wants you to use Western Union to pay

Scammers love, love, love Western Union. When you send money through Western Union (or Moneygram, or any other money-wiring service), it's like blindfolding yourself and walking through a bad neighborhood, while holding out your hand full of cash. Someone will definitely take it, and there is ZERO chance of you recovering it.

Craigslist rule #2: Only deal with a local buyer or seller

A scammer will very rarely want to meet with you in person. In fact, they won't be able to because you are in one country and they are somewhere else in the world – Nigeria is pretty likely, but it could be anywhere. They are sitting in an internet café along with a dozen other people, each one of them throwing out their bait through the internet to see which sucker is next to take the bait.

Craigslist rule #3: Don't deposit any check mailed to you from a Craigslist "buyer"

There are people sitting in jail or prison right now who never thought this would happen to them. In fact, they might be just like you – posting an ad on Craigslist to sell something, hoping to find a willing buyer. But then they got a little greedy and their common sense was shoved aside.

Here's how this scam works:

Let's say you have a car for sale, and you advertise it on Craigslist.

You get an email from someone who is very interested, and wants to buy the car (note that the email does not contain any contact information other than an email address). The "buyer" is quite willing to pay your full asking price.

Unfortunately, as the story goes, the buyer is located in another state and cannot pick up the car personally. However, he is willing to make some other arrangements. He will mail you a cashier's check for the total amount PLUS the cost of shipping the car PLUS some extra money for your trouble.

So, if your asking price for the car is $5000, he will send you your $5000 plus $2000 for shipping the car, and another $2000 to make sure you're happy with the deal. Sounds like a good deal, right? All you have to do is deposit the cashier's check for $9000 that he sends you, then send the $2000 shipping charge by Western Union to his "assistant" who will handle all the shipping arrangements.

This is where the greed comes in, and for some people it is just too much to resist. You are now getting $7000 for a car that you probably would have sold for $4000, and the buyer is sending you a cashier's check so it must be good, right? **WRONG**. Fake cashier's checks are very easy to create, and they look quite authentic. Your bank will accept the deposit, no problem.

So you get the big check, deposit it, and use part of that money to wire the $2000 to the assistant. Now you just wait for the car to be picked up.

Except you won't ever hear from the scammer again.

The next call you will get will be from your bank, because the cashier's check for $9000 was returned. It is either completely fictitious, or was drawn on an account that was closed.

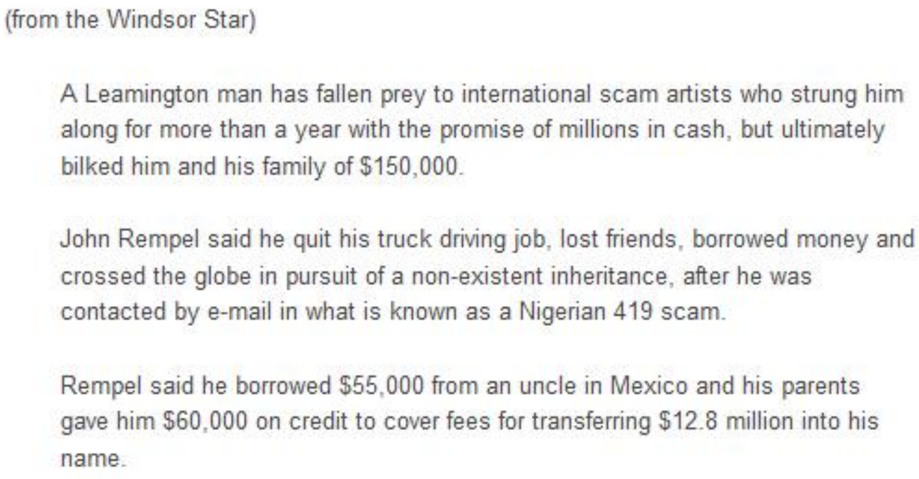
Here is your current situation: Your bank account has been charged back the $9000. You have also been charged a hefty fee by your bank, for depositing a no-good check. You are also out the $2000 that you wired. And you still have not sold your car.

What if you already spent the $9000 on a different car or something else, and you don't have the money to reimburse the bank? That's when the authorities are called in to investigate the situation. And all you can tell them is about "this guy on the internet sent it to me". You don't know his real name or anything about him – you don't even know what country he is really in. Somehow you need to come up with that $9000 or you are in serious trouble. Rule #3 helps you avoid this bad scene.

Another common Craigslist scam is for house rentals. The scammer just searches online for homes that have been foreclosed and are up for sale (thereby ensuring that no one is living there). They grab the pictures from the ad, and then they post the house as available for rental on Craigslist. They are an out-of-town owner, but they are willing to mail you the keys if you send them the first month's rent and a security deposit (by wire, of course). You know what happens – you send the money, and you never hear from them.

Really, the best advice for using Craigslist is to just use common sense. Don't assume you can trust someone you have never met. Don't get greedy and expect to get a lot more for something than it is worth. If your gut tells you something doesn't feel right, walk away from the deal.

Here's an interesting – but very sad – story about someone who fell for the Nigerian 419 scam (not through Craigslist, but it could just as well have been done through there). You can read the full story here: http://tinyurl.com/ydhtajz.



(from the Windsor Star)

> A Leamington man has fallen prey to international scam artists who strung him along for more than a year with the promise of millions in cash, but ultimately bilked him and his family of $150,000.
>
> John Rempel said he quit his truck driving job, lost friends, borrowed money and crossed the globe in pursuit of a non-existent inheritance, after he was contacted by e-mail in what is known as a Nigerian 419 scam.
>
> Rempel said he borrowed $55,000 from an uncle in Mexico and his parents gave him $60,000 on credit to cover fees for transferring $12.8 million into his name.

Secure your data with an automated backup

While this is the last chapter in this guide, it is certainly not the least important. In fact, if you talk to anyone that has lost important data because their hard drive crashed and they had no backup, they would tell you this is the MOST important thing in this guide.

In the introduction, I made a statement: hard drives will crash. It's a fact. And you don't know when your's will crash. It might be 5 minutes from now, it might be 5 years from now. If you have data on there that is important to you, you are risking losing it unless you have it backed up.

Most people don't realize how easy it is to protect your data with a backup. But it is only easy if the process is **automated**. In other words, it needs to work on its own, without your having to remember to do the backup. **If you have to remember it, you won't do it**. So a successful backup system needs to take out the "human" element and have it all happen on its own.

There are two options for backing up your important data: **offsite** or **local**.

Offsite backup

If your data is really important to you (such as documents, family pictures, etc.) then an offsite backup is probably the safest way to be secure. With all of your data safely backed up at another location, even if your computer was destroyed in a fire all of your data is still available to you.

Offsite backup is not expensive, and I have had a few clients who set it up and then had a hard drive crash, and they were SO glad they had the backup so they didn't lose any of their files or folders. This is something I set up for my clients all the time, and I don't even charge my time to do this. It only takes about 10 minutes to set up and I can do it remotely. All you pay is the fee that the backup company charges (for most people it's about $60 for the year for daily, automated backups). Contact me and let's get this set up for your computer ASAP.

Local backup

A local backup is good to have also, although it does require another piece of equipment – an external USB hard drive. You can get one of these for about $70 now. Once the external hard drive is connected to your computer, you can use a program called Second Copy (http://SecondCopy.com) to automatically backup all of your important data from your computer to the external drive on a set schedule. If you need help setting this up, I can take care of it completely for you through my Remote Support service.

A Final Word

So there you have it – a bunch of tips to keep your computer and your data secure. Is this a complete list of all possible security measures you can take? Of course not. You will need to use common sense and apply the principles in this guide, because there are a lot of situations that can compromise your security. The key is to always be aware and watching for them.

And now a shameless self-promotion:

If you need help with your computer, whether it's a security-related issue or something else, get in touch with me through my website: http://www.ComputerTutorFlorida.com. I can help take care of almost any problem, even if you are not local to me here in the Tampa Bay area of Florida.

I also recommend that you get on my email list, if you aren't already. You can do that from my website also. I send out emails that help you use your computer more easily and effectively, and I also update you on any breaking security concerns that require you to take action.

May your computer and your data always be safe!

Scott Johnson