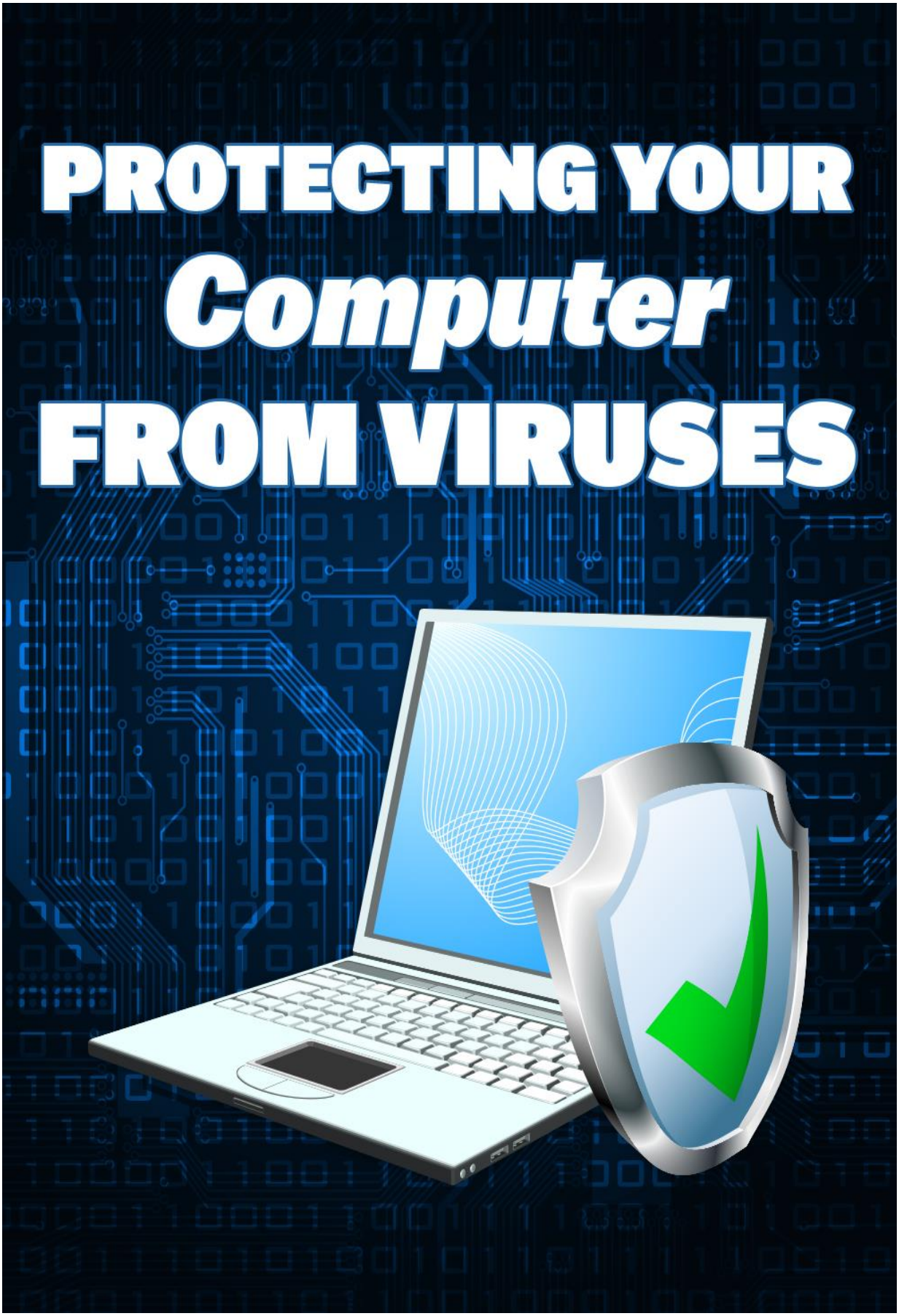
PROTECTING YOUR *Computer* FROM VIRUSES



Anyone with a home computer knows better than to leave his/her computer unprotected against viruses, Trojans, and other assorted malware. They make your computer run slowly, they corrupt your files, they flood your inbox with spam, and so on and so on. For as long as there have been home computers, there have been computer viruses.

If you've been keeping up with Apple, you may remember some years ago when Steve Jobs was selling Macs on the basis that Mac users don't ever need to worry about viruses. Great sales pitch, to be sure, but more recently, Steve Jobs has sheepishly admitted that "Mac users may want to invest in some anti-virus software, after all."

So, no matter your operating system, your computer is not safe from viruses. Even a computer sold on the strength of being immune to viruses is not, in fact, immune.

The fact is that the people who program these computer viruses are just as capable of keeping up with the technology as the people who program anti-virus software. There is a constant evolution on both sides. As the anti-virus software gets stronger, the virus makers have to get stronger to keep infecting computers, and as the viruses get stronger, the anti-virus must be made stronger in order to fight off virus infections.

In all likelihood, this sort of constant one-upmanship between virus and anti-virus will probably continue for as long as the modern home computer is a part of our daily lives.

In the interest of giving the reader a full understanding of computer viruses and how to keep one’s computer safe from them, we'll start off with...

THE DEFINITION OF A VIRUS

The term "virus" is actually a broad label that is applied to a number of categories of malicious software. An actual "computer virus" in the strictest sense of the term is defined as a program that can make a copy of itself and infect a user's computer without that user's knowledge or consent.

The word "virus" is also applied to malware that doesn't quite fall into this category, like spybots, adware, worms, and so on. These programs are not technically "viruses," but using the term “virus” as shorthand for all malware gets the point across quickly.

Although they may be able to infect your computer without your knowledge, many spybots and adware bots are not actually capable of self-replication, and thus, are not technically viruses.

A Trojan may contain a virus, but a Trojan is actually something that you download onto your computer with your own consent. It is, as the name suggests, a file that promises to be one thing, but is in fact another, such as an application that displays pop-up ads on your computer every time you start an Internet browser, or even spybots, capable of stealing vital information to be sent to remote users.

A worm is a program that will download itself to your computer without your consent. It's interesting to note that worms are not inherently necessarily malevolent.

There was a software company in Japan that was working on "benevolent worms." These were worm programs that would find routes around your computer's security and patch them up. While these programmers were working with the best of intentions, the project was a failure simply because these benevolent worms were nonetheless eating up valuable bandwidth, which is the primary reason that worms are such a nasty thing to deal with in the first place.

Spyware is used, as the name suggests, to literally spy on users. While you are using your computer, a remote user can actually observe from, perhaps, thousands of miles away, writing down your email passwords and credit card numbers as you work. Other spybots may not show your work in progress to other users, but may record certain details and send them to a hacker at a later date.

Adware and Spamware are exactly what you think they are. They find websites that you visit frequently, they mark your email address and your Internet proxy address, and they flood you with tons of spam and pop-ups.

It's worth knowing the definitions of all of these different types of viruses simply so you'll know what you're looking for when shopping for anti-virus programs. Most of us are happy to simply keep calling them all "viruses." but a program that boasts of its capability to search for and destroy viruses may actually not be able to do the same for adware, spambots, spyware, worms, trojans, and so on.

In other words, either make sure that your security program can check for all of the above or use a combination of various programs to make certain that you are fully protected.

A BRIEF HISTORY OF THE COMPUTER VIRUS

The very first computer virus was a viral worm known as THE CREEPER. This bizarre virus was created in 1971 as an experiment by Bob Thomas, a programmer with BBN Technologies Research and Development. Thomas simply wanted to explore the possibilities of a self-replicating

program, and hence, the first virus was born.

The Creeper would infect DEC PDP-10 computers running on the TENEX operating system and display the message, "I'M THE CREEPER, CATCH ME IF YOU CAN."

The program was made as simply an experiment, but when these computers were plugged into ARPANET, the predecessor to the modern Internet, THE CREEPER found its way onto a number of remote computers outside of the lab.

The virus spread faster than Thomas had ever intended or hoped for, and some time later, a program known as The Reaper was released. The Reaper was the very first anti-virus program ever designed, created specifically to clear computers of THE CREEPER virus.

It is unknown who wrote The Reaper, but there are some theories that it was Bob Thomas, the same programmer who wrote THE CREEPER. Some suspect that Thomas perhaps released the virus on purpose, knowing he could sell the anti-virus, but it is more likely that he simply wanted to reverse any damage he had done through his research and development experiment with BBN.

The first virus to actually go "into the wild," as in “outside” of that early network of computer labs, was the Elk Cloner virus. The Elk Cloner virus was written by a high school student, Richard Skrenta, in 1981.

The Elk Cloner virus was literally written as a practical joke. It would make its way onto Apple DOS 3.3 systems via floppy disk and display a short poem, beginning with the line "Elk Cloner: The Program with a Personality."

If you used a floppy disk infected with the virus, then every floppy disk on which you copied a file would then become infected with the virus, and as such, the virus would then spread to anyone you would loan the disk to, and so on and so on.

Skrenta had no idea how far the virus would go when he first wrote it onto a computer game disk, assuming it would maybe surprise a few of his friends, get a laugh out of them, and that would be the end of it. However, 1981 was an era where the home computer was first starting to make its humble debut, and by so many degrees of separation, the Elk Cloner virus slowly made its way onto hundreds or thousands of computers.

Today, Skrenta has actually grown from his origins as a computer prankster to become a very successful programmer and game designer in his own right, having developed one of the earliest online multiplayer games throughout the early nineties, Olympia, so while Skrenta may be blamed for having created the first home computer virus, he can also be thanked for having created a precursor to modern online gaming.

While these early viruses were made as experiments or as practical jokes, it wouldn't be long before criminals had found a new tool to commit more crimes. The viruses we're dealing with today are not merely designed to get a laugh out of their targets or to explore the possibilities of modern technology. They are, by and large, designed only to exploit.

The first piece of actual malware (as in a virus specifically intended to harm the user's computer) ever written was the (c)Brain virus, written by the Farooq Alvi Brothers, a software design team operating out of Pakistan. The program would infect DOS systems by rendering 7kb of space into unusable bad sectors. 7kb doesn't sound like much today, but this was back in 1986, when seven kilobytes were actually quite precious.

The virus would slow a computer down, but would do no actual irreparable damage. Booting up would display the following messages...

"Welcome to the Dungeon © 1986 Brain & Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!"

"Welcome to the Dungeon © 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination..."

The virus actually included the phone numbers and names of its makers. This is because the virus was actually created for a very good reason. The Farooq Alvi Brothers specialized in making software for hospitals, and a program they had written for heart monitoring machines was being pirated. Pirated versions often wound up becoming corrupted, and this could easily lead to accidental deaths.

The (c)Brain virus is easily justified from an ethical standpoint, but, unfortunately, the virus wound up spreading not only through the pirating networks, but onto innocent home computers as well.

This practice of using a virus to deter would-be pirates is still in use today, though it is illegal. Thanks to the advent of file sharing programs like Napster, and later, Bear Share and Limewire, many music and film distributors have taken to releasing Trojans and viruses onto these file-sharing networks disguised as popular songs and movies. The issue of right and wrong here is debatable, but it does remain illegal.

Today, the Farooq Alvi Brothers still make a living as programmers, being amongst the leading Internet providers in Pakistan.

Throughout the 1980s when people started using home computers more and more, we saw the first real wave of computer viruses. This was, of course, before the Internet, but viruses still managed to proliferate thanks to interchangeable media.

While it was a much slower process than it is today, viruses could still reach hundreds, thousands, or even hundreds of thousands of home computers through the sharing of interchangeable media like floppy disks, as well as the early protoplasmic material that would eventually become the Internet: Dial-up modems and BBS boards.

These boards were full of people looking to download new software either for cheap or for free (meaning, of course, pirated), and these users proved to be very easy targets for anyone hoping to infect home computers with viruses.

The first Trojans appeared on the Bulletin Board Systems. When a user came on a board asking for free software, another user might oblige, providing them with the software, but with a virus attached. This was not necessarily the intention of the file sharers, but rather, they may have been handed the file with a virus unknowingly, or it may have worked its way into the file in question simply by association with their infected computer, meaning that, perhaps, every file being sent from their system was infected.

Even at this stage, virus programmers were really just hobbyists, and while their work may have spread quickly, it was still a relatively small phenomenon, and there was little fear of identity theft happening as a result (although the damaged and slow computers weren't exactly appreciated, nonetheless).

Starting around the 1990's, it became possible to embed a virus directly into an email, with or without a downloadable attachment, thanks to shared file programs like Microsoft Outlook.

We also saw viruses embedding themselves directly into websites, infecting any and all visitors, whether or not they've actually agreed to download something, viruses embedded in Instant Messages, and viruses that might simply worm their way onto your computer just because the virus maker happens to have your Internet proxy address handy.

It was during the big PC boom of the 90's that it became a possibility to take advantage of people with a computer virus, and not just to slow their computers down. Where previous viruses had been done as jokes or as experiments, now, with people filing their taxes online or using PayPal to purchase items on eBay, it became easy to use viruses to take credit card numbers, to commit fraud and identity theft, and to steal information to sell to spam marketers.

Likewise, at this point, it became clear that computer viruses were a serious problem, and more and more companies started putting out anti-virus software. And, of course, as the anti-virus companies started fighting back, the virus programmers had to step up their game in order to work around the software. As the viruses became more sophisticated, so, too, did the anti-virus software, and so on and so on. And this brings us to where we are today.

Why People Make Viruses

If you've never been a victim of identity theft, it may seem that the only reason viruses exist is to slow your computer down and to force you to send it in for repairs. As such, you may wonder who has the time to sit around coming up with ways to mess with people like that.

Well, the truth is that there's a lot of money in creating computer viruses. Again, today's virus makers are not just trying to be funny and they're not just experimenting. They want money.

The people who create viruses are not just hobbyists; they're professionals (or professional criminals, if you will). Viruses aren't just there to slow your computer down; they are there to steal information from you. They will either take your financial information and steal your money directly or they will steal your personal information, sell it to spam companies, and make some money that way.

Virus programmers are dedicated and skilled at what they do, and they don't do it for free. They want money, yours or someone else's, and most of them make a good living doing it.

True, there are some practical-joker virus makers out there, but the vast majority of the thousands upon thousands of viruses, worms, Trojans, and malware bots we have today are designed only to take information from you.

That viruses are bad for your computer, that they slow your PC to a snail's crawl, is merely a side effect. In fact, they are even being designed these days to take up less of your computer's RAM, so you may even be infected without any slowdown whatsoever.

The benefit this offers the virus makers is that you might never know you're infected in the first place, and if you don't know that you're infected, then you will be less likely to do something about it.

So, again, most of the people out there programming viruses are not doing it as a hobby, but as a career.

They take to it with all of the seriousness and misguided work ethic as you would take to your own career. The difference is that their chosen line of work is illegal and malevolent.

They want to take advantage of you, they want your information, and if they can get it, they want your money, and that is the only reason there are so many viruses out there.

It should be understood that merely getting rid of viruses when they infect your computer... isn't really the best way of going about protecting yourself from virus infection.

Of course, you want to run a scan regularly to make sure that you're clean, but more importantly, you need to make sure you're actually protected in the first place. If you only scan your computer when it starts slowing down, then you're only dealing with the problem after it happens.

When the home computer market really started to take off in the mid-1990s, many users actually wound up replacing their computers when they started to slow down thanks to virus infections. This was before these new PC users really knew what viruses were, as they just assumed that a two-year-old computer running at a snail's crawl was just "showing its age." Really, this is comparable to trading your car in when all it needed was an oil change.

Carrying this analogy a little further, installing a full security system onto your computer is comparable to carrying full insurance on your car... as opposed to waiting until you're in an accident and then worrying about how you're going to pay for the damage.

In other words, it's simply not the sort of thing you can afford to neglect.

At this very moment, there are viruses trying to get into your computer, whether it's through websites, through e-mail, through IM messages, or through an open Wi-Fi connection. If you are connected to the Internet, then you are literally under assault day and night from the virus makers.

It is not even a matter of "you will probably get infected if you don't protect yourself." Rather, you *will* become infected if you don't protect yourself. In fact, there may be some viruses on your computer right now, depending on the last time you ran a scan.

So, get some security software and scan your computer regularly, at least once a week, with a "search and destroy" anti-virus program.

WHAT YOU SHOULD LOOK FOR IN COMPUTER SECURITY SOFTWARE

Ideally, you should try to get your hands on a full security package, as opposed to just an anti-virus program, an e-mail spam filter, and so on

and so on that are all separate programs. There are quite a few of these full security package programs available. McAfee Security Center comes highly recommended, as it is a full package covering anti-virus, spam filtering, pop-up blocking, spyware, adware and malware filtering, worm and trojan filtering, and so on.

However, a full package like McAfee does cost somewhere in the area of forty to sixty dollars, depending on the retailer. A full package like this is the only security you'll ever need for your computer, but, that said, if you're strapped for cash, then you're strapped for cash, and you need to make sure you're protected right now, not "when you get around to doing something about it."

If your computer is unprotected, then stop reading this right here and go download a free virus protection program NOW.

The free virus protection programs are not the best protection you can get, but they will work as a temporary band-aid until you can find some full security software that you can be happy with.

Whatever you settle on, the number one, first and foremost, most important aspect of the software is that it absolutely has to be up to date. You can't simply unpack the anti-virus software that came with your PC three years ago and install it. Rather, you need to make sure that whatever software you're using receives regular updates.

The best in this category will update about once a day. Some actually update more than once every day.

The fact is that hundreds of new viruses enter the world every day. If your anti-virus software can't keep up with these new viruses, then it's not really worth it.

PUBLIC COMPUTER SECURITY

These wireless Internet hotspots are certainly a welcome new development. There’s really nothing like getting some work done while enjoying a cup of coffee at your favorite café.

Simply put, wireless Internet has made life easier. Using a Wi-Fi enabled modem, for one, cuts down on all of those obnoxious wires you have to drag around your house and allows you to sit down with your laptop on the couch in perfect comfort and to do whatever you like.

Being able to look up directions on MapQuest or Google Earth while in the passenger seat of the car is a great bonus too and has certainly helped more than a few lost husbands get out of stopping to ask for directions.

However, as great as these connections are for us, they're also great for hackers.

The fact is that most Wi-Fi hotspots these days are using unprotected connections. In fact, a recent study conducted by a computer security group found that airports in particular are a popular place for hackers to do their business. They have thousands of people moving in and out all day, many of them using laptops, iPhones, and Blackberries, to be sure, so all a hacker has to do is to sit there with his/her own laptop hacking right into people's personal files.

So far, airports have done very little to counter this. Simply put, it's not very high up on their list of priorities.

If you're wondering how hard this is for a hacker to accomplish… it's not hard at all. The actual programming knowledge required to hack through somebody's security setup on an open Wi-Fi connection is the sort of thing that you can learn in a few hours at the local community college.

What you need to do when using free Wi-Fi is to simply not rely on the Wi-Fi provider to give you any degree of security with your connection. Take this into your own hands and provide your own Wi-Fi security.

All you really have to do is, whenever possible, use WPA encryption on your Wi-Fi firewall. Just find the security settings, and you should see the option there.

It's really not that complicated, though with a public Wi-Fi access point, it may not always be an option.

When this is not an option, just use your own judgement. For someone to hack your Wi-Fi connection in a hotspot, they would have to be within that hotspot. In a crowded area, we'd advise against it.

Before closing this subject, we should take a moment to remind you that some crooks still do it the old-fashioned way.

And by this, we mean that… say your security system is top-notch, regularly updated, and your Wi-Fi security encryption is set to WPA, now… how is that going to protect your identity when some looky-loo takes a peek over your shoulder and gets a glance at your Social Security Number?

All of this computer security software does a great job at protecting from hackers, but in the end, it's just software. It's not going to scare peeping Toms and laptop thieves away, nor can you use the software to track your laptop on a GPS unit.

Consider not only cyber security for your laptop, but practical security.

We can boil this down to a few basic tips:

1. NEVER LEAVE YOUR LAPTOP UNATTENDED.

Chances are, when you ask a stranger to "watch my laptop while I use the restroom," that that's exactly what they're going to do. They're going to watch the display as they take notes on any personal information you may have left onscreen.

Basically, if you're in a public place, never let your laptop out of your sight, even if that means taking it to the restroom with you.

2. USE A SECURITY SCREEN

A security screen is basically just a shaded piece of film you snap onto your laptop. It blocks light in such a way that you can easily see the display if you're sitting a couple of feet directly in front of the laptop, but as such that you cannot see the monitor at all from a few inches to the left or right. In other words, only the actual user can make out what's onscreen, and anyone who likes reading over people's shoulders will have to go find someone else to bother.

Many laptops these days have a security filter built right in, but if not, you can probably buy a security screen for the money you have in your pocket right now. As an added bonus, security screens also work to reduce the glare from the sun or from bright indoor lighting.

3. DISCOURAGE THEFT

There are a bunch of little tricks you can use to discourage theft of a laptop. Even if you watch your laptop like a hawk, a shiny new MacBook is a great way to lure thieves out of hiding. Remember, if your laptop is stolen, so too is all of the information it contains.

Try carrying your laptop in a regular book bag or messenger bag, as opposed to one of those beautiful laptop cases. Lock it in the trunk when you leave it in the car; don't just drop it on the front seat. You could also take a note from guitarists. Have you ever known a guitarist who didn't put a bunch of stickers all over his guitar case? If a thief sees a shiny new guitar next to one covered with stickers, he'll take the shiny new one.

STAY UP TO DATE

The sad fact is that much of what you've read above may be somewhat out of date by the time you read this. The viruses are getting smarter, and so is the anti-virus software. There will always be some new development in computer viruses and how to combat them, so just make sure to stay up to date and know from what you're protecting yourself.