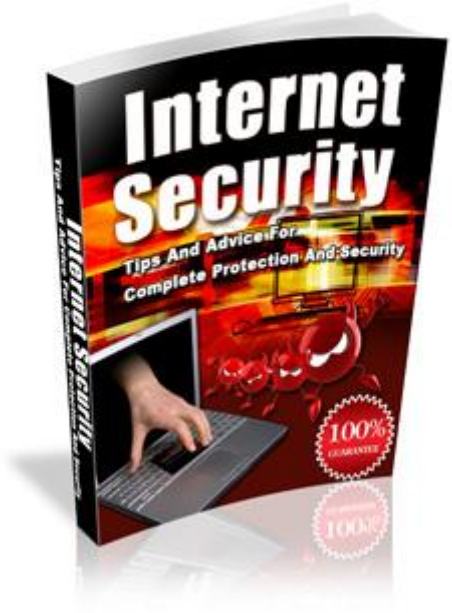
Internet Security Tips and Information



Contents

Internet Security- The Truth About Identify Theft 3
Internet Security for Teens- What You Need to Do 4
Internet Security-Downloading E-Mail Attachments 4
Internet Security- 5 Tips for Using Facebook 5
Internet Security- 8 Tips to Protect Yourself When Dating Online 6
Internet Security for Teens and Tweens- 10 Tips to Keep You Protected 7
Internet Security- Parental Control Software 8
Internet Security- Online Safety for Your Children 8
Cyber Bullying- Another Aspect of Breaking Internet Security 9
5 Tips to Ensure Internet Security 10
Internet Security- Downloading Music off the Internet 11
Internet Security- Popular Online Scams 12
Internet Security- Protect Your Wireless Connection 13
Internet Security- How to Deal with Spyware 13
Internet Security- Protecting Yourself When You Shop Online 14
Internet Security- Make Sure Your Passwords Protect You 15
Make Sure Your Emails Are Safe: Tips for Internet Security 16
Internet Security- Why Should You Use a Firewall? 17
Internet security-Signs That Your Child's Safety Might Be Compromised 18
Internet Security- Protect Your Business 18
Internet Security- Safety When Using Public Computers 19
4 Email Scams that Threaten Your Internet Security 20
Internet Security- Storing Your Password on Your Computer 21
Internet Security-What Does Your Large Business Require? 22
Internet Security-Using Social Utility Sites 22

Internet Security- The Truth About Identify Theft

You would hate to think that by ordering that new purse or buying that airline ticket for vacation might end up costing you your identity. While most websites are secure when it comes to transactions, your personal and financial information can be compromised. As a result, they can open credit cards, checking accounts, and even get an ID and purchase a new car with your personal information. As a result, you could end up owing thousands of dollars, as well as have to seek legal help which can cost even more money.

Identify theft can unfortunately happen to anyone. Here is some information that might be helpful in recognizing it and preventing it to maintain your internet security.

Signs that Your Personal Information Might Be Compromised

1. You receive something that you did not order.

2. Unexplained things pop up on your credit report. You might not even notice this until you try to purchase something and you are declined due to your poor credit rating.

3. Unexplained purchases show up in your checking account or on your credit cards.

4. You receive calls from bill collectors for accounts that you did not open.

Preventing Identity Theft

1. Always shred any unwanted credit card offers or mail that might contain personal information such as your account number, social security number, checking account number, etc.

2. Stay up to date on the latest scams. There are several websites devoted to this.

3. use anti spam ware and ensure that your e-mail account has a spam filter on it to deposit unwanted emails into.

4. Check the privacy policy on a website that asks for personal information. Don't submit anything if it doesn't have one.

5. Don't keep your personal or financial information on your computer. Likewise, don't store your passwords on your computer either.

6. Don't open an attachment if you receive an e-mail from someone that you don't know. Use an anti-virus program to scan the e-mail first to make sure that it doesn't contain any phishing or virus programs on it.

7. Keep your firewalls and anti-virus software up-to-date on all of your computers.

If you suspect that your security has been compromised, change all of your passwords, cancel your credit cards, close your bank account, and report it to the police. Also, report the activity at once to your financial institution and credit card company.

Internet Security for Teens- What You Need to Do

Everyday you hear about teens being attacked or compromised by people who take advantage of them by using the internet. For a parent, this can be a frightening concept. However, there are measures that you can take to protect your teens on the internet. The following is a list of tips to help ensure internet security for your teens.

1. Talk to your teen. First, make sure that you talk to your teens about internet security. Having good communication is always the most effective preventive measure. After all, you can put security features on your computer at home, but teens have access to computers almost everywhere they go. Make sure that your teen understands the dangers associated conversing with people they don't know on the internet, meeting people off of the internet, and using their financial information to purchase something online.

2. Be aware. There are thousands of chat rooms, message boards, and forums out there for teens. As a result, there are thousands of people out there who pretend to be teens in order to converse with them. This is a dangerous situation. When your teen is at home, monitor their internet use without being too overbearing. Know what chat rooms they use, what people they converse with on a daily basis, and ask to be able to access their facebook and myspace pages. Let them know that if they are going to have a computer in their room you have the right to look at their internet usage from time to time.

3. Report any suspicious behavior. If your teen tells you that someone on the internet wants to meet them, do some investigating yourself on this person. Likewise, if your teen tells you that they are troubled by someone who is contacting them on the internet then report this person to the police. It is better to be safe than sorry.

4. Don't let cyber bullying go unnoticed. Cyber bullying is a very real threat to internet security, as well as physical and emotional well-being to teens. If your teen is being cyber bullied then report the offenders to that website that it is occurring on and then let the school know as well. More and more organizations and websites are taking this seriously this days. On facebook, if you block someone now, it actually asks you if it was due to cyber bullying.

Internet Security-Downloading E-Mail Attachments

It is very important to remember to be careful when you receive an email that comes with an attachment. It is doubly important if that attachment is from someone that you don't know.

As a rule, it is a good idea to delete the email and not even worry about it if it's from someone that you don't know and weren't expecting. After all, an email with an attachment can equate to a virus and a virus can harm your system so much that it might be beyond compare. In addition, you can lose valuable information and even have someone hack into your personal and financial information and use it for their own purposes.

It seems silly that people would waste their time trying to come up with different ways to destroy other people's systems, but it happens on a daily basis. Sometimes, people do it just because they can and there isn't reason a valid reason behind their actions. This can be very frustrating for the victims of such an attack. You must learn to be cautious.

So how can you protect your internet security when it comes to downloading e-mail attachments?

- Anti-virus software. You should definitely invest in some anti-virus software. This will scan the e-mails and attachments for you and let you know if they are safe. This can be particularly important if you are using free email accounts.
- E-mail programs with built in sensors. If you pay for your e-mail account then chances are that it already has some sensors to detect harmful attachments. Sometimes, as soon as the e-mail itself comes in it is sent to the trash can or the harmful attachment itself is removed for safety precautions. This is ideal.
- Ignore the mail. A lot of times people who send harmful things to your e-mail account try to get away with it by pretending that they know you or are sending you something that you already requested. Well, if you know them then you should be able to identify the e-mail address. You should also recognize the name. Sometimes, they will use the name of a legitimate company to try to fool you. For example, it might say “Amazon” but when you look more closely at the e-mail address it might read amazon@hotmail.com. Now, would it really make sense for Amazon to use a free e-mail account?

Internet Security- 5 Tips for Using Facebook

You probably have a facebook account. If you don't, then chances are that your child does. Facebook can be an excellent way to interact with your friends and co-workers, as well as keep your family updated on what is going on in your life. You can post family vacation pictures, send emails, and “chat” with people that live far away. Better yet, you can do all of this for free! However, there are some risks associated with internet security when it comes to Facebook.

Luckily, Facebook is aware of these internet security risks. There are actually some things that you can do to help protect yourself. The following is a list of 5 tips that you can use to make sure that you are safe when using Facebok.

1. Make your profile private. You can do this in a number of ways. You can make it so that only your friends can see your information and photos, or you can make it so that people can see your name and information but not your photos or wall unless you add them as a friend. Check this out under your “privacy settings”tap on your account.

2. Block people that you don't want to see your information. There is a choice under their photograph that will allow you to block them. When you do this, you will not show up on a search that they do and they will not see anything having to do with your account. It will be as though you do not exist to this person. This is a good feature is someone specifically is bothering you.

3. Report cyber stalking or harassment. If you choose to block someone, a window will pop up asking you the reason. One of the choices is cyber stalking. Choose this option if it is true. It won't stop if people don't report it.

4. Only add people that you know. This will help your internet security tremendously. Having 300 or more friends just so that you can say you have a lot of them is not a good reason for continuing to add people.

5. Don't purchase anything via Facebook. Many applications cost money. Ignore these and use the multitude of free things that the site offers. You don't want your financial information to be compromised just because you send someone a picture of a birthday cake.

Internet Security- 8 Tips to Protect Yourself When Dating Online

A lot of people find great, healthy relationships through online dating communities. Most of the people who sign up for them are legitimately looking for love and relationships. However, there are always going to be people out there who will take advantage of others.

So what can you do to protect your internet security, and yourself, when using online dating websites?

1. If you do decide to meet someone in person, do it in a public place. Preferably, meet them in daylight hours and ask someone to go with you. If that doesn't work, then at least leave information with a trusted person which includes where you are going, how long you plan on staying,a s well as anything identifiable about the person that you are meeting.

2. Do not rely on a photograph. It might not even be the person that you are really talking to. Or, it could have been them 20 years before. People use different pictures or are dishonest about their appearance all the time.

3. Save all of your conversations in a file on your computer. Better yet, print them out. Keep them somewhere that is fairly easy to access.

4. Talking to someone online is not the same as talking to them in person. Don't rush the relationship and don't feel as though you have to meet them right away.

5. use a different e-mail account for your online dating than you do for your regular emails.

6. Do not ever give out any personal information at the beginning. In addition, keep your last name and anything personal, such as your address and directions to your house private, until you have met the person and have gotten to know them a little bit better. If you must give them your number, give them a cell phone number instead of your house phone.

7. Find a reputable online dating service. Don't just go to Google and search for singles chat rooms. An account that you have to pay for is generally more reputable than one that is free of charge.

8. Don't post any racy or revealing photographs of yourself. This is sure to draw the wrong kind of person-and not one that is looking for a relationship with anything serious in mind. In addition, try to choose a screen name that isn't too revealing either.

Internet Security for Teens and Tweens- 10 Tips to Keep You Protected

There are a lot of safety risks out there for teens and tweens who use the Internet. However, this doesn't mean that they have to stop using the 'Net. Instead, they should use good judgment and try to make wise decisions. The following article lists some helpful tips to keep your teen and tween's internet security protected.

1. Don' let your username say too much about you. For instance, don't make it your name and age, like Susan16. Instead, make it something that doesn't say much about your name, age, or sex. Keep it as neutral and vague as possible.

2. Don't ever post your social security number, driver's license number, phone number, home address or credit card information on the internet. If a friend asks you for your number on Myspace then either email them a private message or wait until you see them in person.

3. Don't add friends on the Internet that you don't know. People often misrepresent themselves and pretend to be something they are not. It happens all the time and they are very good about it. Don't think that you will know the difference.

4. Never agree to meet someone in person that you have met off of the Internet. If you are part of a group and someone wants to get together to discuss something that sounds legitimate, have a parent go with you and meet in a public place. Never substitute a friend for a parent.

5. If you have concerns about someone who is harassing you on the Internet, tell an adult. Cyber stalking is being controlled these days and awareness is growing.

6. Make your profile private so that only the people you know can see your information and photos.

7. Do some research on sites before you sign up for them. Don't just join them because everyone else is. Learn how they work before you post anything.

8. Don't store your passwords on your computer. It can make hacking easier.

9.If you purchase something with a credit card, ensure that you are using a secure server. This should be noticeable by a little emblem on the bottom right hand side of your screen.

10. consider not using your full name when you join a site. Not posting your last name is a great preventive measure when it comes to Internet security.

Internet Security- Parental Control Software

Keeping your child safe is one of the biggest challenges that parents face today. Good communication is an excellent tool and necessary when it comes to warning your children about dangers that they may face. However, sometimes it takes more than just good communication when it comes to protecting your child online.

Although you can go through the process of putting your family's computer in a common room, looking into the Facebook and Myspace accounts from time to time, and talking to your child about the risks of posting personal information, risks still arise.

The fact is that sometimes your child will be subjected to adult material, or material that is otherwise inappropriate for children, by mistake. There re some pornography websites whose addresses are very close to popular websites with the same name. Sometimes, the only difference is whether it is .net, .com. or even .gov.

One of the things that you can do to protect your child's internet security is to install parental control software. Although it might seem extreme, a parent will do whatever it necessary to protect their children.

So what can parental control software do?

- Create alerts. You can be notified at once through either text messages, phone calls, or e-mails when someone in your home visits an inappropriate website.
- Time controls. These are good because you can actually set a pre-determined amount of time that your child can spend on the Internet. Of course, when their time runs out, they can still access other features of the computer such as word programs which they might need for school purposes. A common complaint that parents have is that their child spends too much time on the Internet.
- Usage Logging. With this feature, you can produce and review logs of your child's internet activity. You can see what websites were visited, logs of Instant messaging chats, as well as the various programs that were used during the Internet session.
- Content controls. These allow you to choose what types of content, such as adult content, that you want your child to avoid access to.
- Program controls. Program controls control the access to certain programs such as downloading music files or other files that could be dangerous.

You can pick and choose which options you want and change them as needed. After all, you might not be facing all of these issues at once.

Internet Security- Online Safety for Your Children

Every parent wants to keep their child safe. Protecting your children when they are on the Internet is no exception to this. While you don't want to think about people harassing your child

or trying to bring harm to them, there are still those out there who might try. The following is an article that contains tips on how you can provide online safety for your children.

- You can purchase online tools for added internet security. These contain features that allow you to control your child's access to adult material. Some ISPs also contain parent-control options that block some types of material. In addition, you can purchase programs that block access to sites that is based on a list that your ISP makes.
- You can also purchase filtering programs that restrict personal information from being sent online. This is particularly helpful in protecting your financial and personal information.
- Install a program that lets you set a time limit on how long your child can stay online. This way, you can ensure that they are not spending a large amount of time on the internet. However, they will still be able to use office programs for school.
- If your child has a Myspace of Facebook account, get one as well and befriend them in order to monitor their use. Only intervene if there is a safety concern in order to give them more privacy.
- Don't let your child participate in chat rooms. Some ISPs offer programs that block chat rooms. Sometimes people enter chat rooms designed for children and teens and pretend to be one themselves.
- If you're aware of any child pornography contact the National Center for Missing and Exploited Children. If your child receives pornography, contact your local law enforcement office.
- Talk to your child about their screen name creation. A screen name should be neutral and should not reveal any of the child's personal information such as their name or age.
- Talk to your child about posting personal information like their address, age, and full name on social utility sites. When they create an account, have them make it private to ensure that only people they know can access it.
- Continuously monitor your credit cards and banking account in order to be aware of any unusual activity. Talk to your child if you become aware of something different on the account. Then, talk to your credit card company or bank.

Cyber Bullying- Another Aspect of Breaking Internet Security

When you think of Internet security, you are probably thinking of protecting your personal and financial information. However, there are other types of internet security breeches. One type is cyber bullying.

A phrase that is becoming more and more prevalent in the world wide web, cyber bullying can be very invasive and emotionally upsetting to children, teens, and even adults. It's difficult to control because in many cases the perpetrator is known but can not be proven. How? Because they will give just enough information to let their victim know who they are, but not enough information to actually be convicted of anything. They can do this by using pretend user names, fake pictures, and revealing very little information about themselves.

So what types of things happen with cyber bullying?

- Threats- a lot of times, a cyber bully will make threats. These can be thinly veiled or outright vicious.

- Harassment on victim's out website- another type of cyber bullying occurs when the bully posts negative material in abundance on the victim's own website. This can come in the form of negative comments, threats, and other types of general harassment.
- Slander- if the bully has their own site (like a blog or a facebook or myspace page) they might make slanderous comments about the victim. These can be falsities, such as claiming that the victim is cheating on their spouse/significant other, or they can be harmful truths that the general population doesn't need to need.
- Accusations- a rare form of cyber bullying, but equally dangerous, is when the bully actually accuses the victim of doing the same thing that the bully is doing. An example would be this: the bully sends negative e-mails to the victim. Then, the bully gets on their own blog or website and writes about ow upset they are due tot he fact that the victim is sending THEM negative emails. In such cases, the bully might even receive sympathy and the victim is then harassed even more by people who feel sorry for the victim.

So why do things like this happen?

It is very difficult to know why. Anger, resentment, lack of self-esteem, or sometimes plain boredom can lead to cyber bullying. In addition, the anonymity of the internet makes it easier than every to bully someone. Still, cyber bullying can be emotionally devastating and can threaten your own emotional security. If it is happening to you, don't sit back and let it continue.

5 Tips to Ensure Internet Security

Do you want to keep your computer and personal information safe? Of course you do. Here are 5 tips to help ensure your internet security.

1. Be careful of em-mail attachments

One of the most common ways to threaten your internet security is to open an e-mail attachment that contains a virus. Sometimes, just clicking on the attachment itself will unleash the virus. If you receive an email from someone that you don't know and it contains an attachment, don't open it just to be on the safe side. You can always send a message to that person to verify that the email is legitimate. It's best to invest in an anti virus software program that can scan the attachment before you open it. Some e-mail systems will scan emails for you. However, if you go through a free program (like hotmail) don't count on the system being as complete as an email account that you pay for.

2. Anti-virus software

You must invest in anti-virus software. It is one of the most important things for your computer. In addition to keeping you safe from viruses, it can also scan your hard drive and clear out unnecessary information, thus making your computer run more efficiently as well. Anti-virus software programs are everywhere but it helps to do some research before investing in one. With some of them, you have to update them and pay again every year.

3. Update security patches for your browser

On Windows, you can go to “Windows Update” under the “Start” menu it will update security patches for you. This is necessary because holes are formed on the Internet frequently and while you might be protected this week, that doesn't guarantee that you will be next week.

4. Protect your passwords

While it is easier to use your same password, or a variation of it, for all of your accounts, it is safer not to do so. When forming your password, it is better to use a combination of letters and numbers. Also, never give your password out to anyone and resist the urge to store them on your computer. From time to time, change your password on your important accounts that contain personal information or financial information for added internet security.

5. Install a firewall.

A firewall blocks unwanted access to your computer. Some systems, like Windows Vista, have firewalls built into them. You can also download others.

Internet Security- Downloading Music off the Internet

Today, most people have downloaded music off of the Internet. Not only is it convenient, but it is also fun and very inexpensive. In the past, if you liked a song you either had to wait until it came on the radio to record it or you had to go out and buy the entire album. Not only was this expensive, but it could be a hassle, too, if it was the only song off of the album that you wanted.

Downloading music, however, costs less than $1 per song in most cases. It also downloads quickly and you can burn it on a CD for your home or vehicle. However, downloading music off the internet comes with internet security risks as well.

When a peer to peer (P2P) site is used, each person's computer acts as a host for a song or download. After installing software, a person can decide if they want to only download from other people or let other people also get into their computer and download from them.

Obviously things like this can cause problems where internet security is concerned. By letting other people into your computer to download music, other things on your computer are also at risk from being taken as well. This is especially true if a good hacker gets in control of your computer. Files might be stolen, or deleted, or a virus can get into your computer and infect it, causing you to lose everything. Not really worth it for a couple of free songs.
There is another problem with downloading music in this way as well. Music is copyrighted. When you download it without the artist's consent, you are basically stealing. It is punishable by law. You have probably heard of pirated music or pirated movies before.

A common argument is that artists are already rich and downloading a couple of songs shouldn't matter. However, it does matter. Artists, by the way, don't really make that much money off of their CDs. For a $13 CD, some of the profit goes to the songwriter, some to the record company, some to the musicians that played on the album, some to the distribution, and

some to the record store that sold it. Unless the artist was also the songwriter, they are getting a very low profit, usually only a dollar or so.

If you are downloading music, have a good anti-virus software program available, as well as a strong firewall. This will protect your computer, but not your rights if you get sued.

Internet Security- Popular Online Scams

Nobody wants to get hooked into a scam, but some of them are so clever that you can get caught up in them without even realizing that you are doing something that threatens your internet security.

So what are some poplar internet scams?

1. Cashier's checks. This is a new scam that is becoming popular, especially on craigslist. Let's say that you post something for sale. A person writes you, without seeing the item, and says that they want to purchase it. They offer you a cashier's check that is sometimes even over the amount that the price is set for. They even tell you to deposit it and to that they will wait until the money shows up before they pick up the item. The money shows up in your account, they get the item, and then suddenly, the bank calls. Turns out the check wasn't good to start with. To avoid this, only deal with local people. Never accept a check that is more than the amount. If possible, have your bank check out the cashier's check with the bank account that it was drawn upon.

2. Online auctions. Although the sites might be legitimate, the products might not be. To protect yourself, always purchase from a seller with positive feedback, make sure that it is a reputable auction site (like Ebay), understand the payment terms, use a safe payment method, and don't accept cashier's checks for items.

3. Phishing. In this scam, someone writes you from a legitimate company, like a bank, and tells you that your information has been compromised. They then direct you to another site where you are asked to enter your personal information in order to protect everything. Don't fall for it. If it was for real, you would have received a phone call or something from the mail. To be on the safe side, call the company by looking up the number in the phone book.

4. Disaster scams. A disaster strikes and the next thing you know, someone is writing you asking for donations. Look them up on the internet before you write a check.

5. Work scams. These can come in the form of work at home scams or scams in which the person tells you that they found your resume online and want to offer you a job. Never do anything that requires you to pay money upfront or provide your social security number of bank account number.

Internet Security- Protect Your Wireless Connection

Using a wireless connection when it comes to your internet can be great. It's fast, it's easy, and you don't have to deal with cords. Plus, you can hook up at a lot of different places-from airports to McDonalds.

While wireless routers are great, they are not as secure as hooking up your computer to a wall in your home. Other people can use your routers and hook up to the internet. They can also access your own personal information and be privy to things such as your financial information and other things that you don't want other people to have access to.

Hackers are notorious for breaking into unsecured connections. Actually, you don't have to be very technologically advanced to do it, either. Even someone with limited technological skills can use your router for their own computer. This is especially true if you do not set a password or make your connection secure.

Sometimes, people just want to use your router to access the internet themselves. Other times, they want to steal information or send you viruses. Nobody wants to deal with that. A virus can crash your computer, sometimes to the point that it is not salvageable.

But how do you make sure that your internet security is good when you use wireless internet?

First, if you are not using your wireless router then you should turn it off. This is one of the best ways to protect your internet security.

You should also disable the router's DHCP service. What does this do? This basically gives the computer access to the wireless connection. However, when you disable it and figure it manually then you can give your network a distinct IP address and make it more secure.

It is also important to setting up a strong password in order to encrypt the server. Make sure that the password is something that is strong enough that it can't be figured out. It is always suggested that you do not use the same password over and over for all of your accounts and that you try to make it a combination of letters and numbers. Don't ever use your name, zip code, social security number, or even telephone number.

Setting up and then activating a firewall is an additional way to protect your internet security. This is important whether you are using a wireless router or not. A firewall can protect you from viruses.

Internet Security- How to Deal with Spyware

So what, exactly, is Spyware? Spyware is software that can collect your personal information, change your computer's configuration, and install advertising on your computer without you even knowing it. Spyware generally does this without your consent, which is what makes it threaten your internet security.

There are a host of problems associated with spyware, too, and some of these problems include trying to get rid of it.

Why do people use Spyware?

Spyware is typically used for marketing purposes. When a company makes spyware, they get contracts from other companies that pay them well. They can direct traffic to other websites that are similar. For this reason, they can be be good.

However, like most things, spyware can be abused, too. Sometimes, things pop up on your screen that are unwelcome, such as adult content. Or, sometimes hundreds of things pop up at once. This is annoying and can make you not want to return to that particular website.

What kinds of spyware is out there?

Most spyware is adware. Adware captures data for advertising that is targeted. Malware, on the other hand, causes problems with your computer. Malware can be a virus that harms your computer, for example, or hijack your computer's information. This can then be used for identity theft purposes. Your personal information can be sold to other people who can then use it to open accounts and purchase things in your name.

What else can spyware do?
It can cause you to lose control of your computer. It can also cause error messages and make your computer run slower, which is a big annoyance in and of itself. Your computer can even be used to send out emails that contain viruses or for illegal purposes if the right hacker gets into it.

How can you get rid of it?

Of course, now you want to know how you can get rid of it. Well, resist the urge to use the “uninstallation” part of the program. While it might appear to take the spyware off of your computer, it generally doesn't. In fact, it might even set off a trigger that installs more. Instead, spend the money and invest in a reputable cleaner or spyware detection program. These sometimes have to be updated every year which might require a new subscription but it's worth it to get your computer cleaned. It's better to spend money on that than trying to recover your identity later.

Internet Security- Protecting Yourself When You Shop Online

The internet can be a great place to go shopping! You can do it right from your home with little to effort. However, there are horror stories from people who have had their credit card and even entire identities stolen. So what can you do to protect yourself from this happening to you?

- Keep in mind that a lot of credit card companies have provisions for challenging fraudulent charges. If you see something that doesn't look right on your bill, give them a call. Also, print out a copy of every receipt of what you buy.
- Only shop at sites that contain a physical address and a telephone number. If you feel

leery about them, either trust your gut or give them a call or email. See how quickly they return your message. If you call them, don't just talk to a machine, talk to a person. Remember who you spoke to. Ordering from a trusted site might be better than one you have never heard of. For example,. Ordering straight from Old Navy is probably more secure than ordering from a random woman online who sells Old Navy.

- Don't ever provide personal or unnecessary information like your social security number or checking account information in order to process credit card transactions. All they need to know is your billing address, telephone number, credit card number and type of credit car, and the security number on the back. Never give out your social security number. It is not necessary.
- Look for sellers who have secure servers. Some companies that are considered safe are Equifax, SecureSite eBusiness, Thwate, and Verisign. The encryption technology is always changing and while it already makes shopping pretty safe, it keeps adding additional features for the security and protection of shoppers like yourself. There should be a little emblem in the bottom right hand corner of protected sites to watch for.
- When you are on a secure page, right click with your mouse on any blank space and you should get the options box. Scroll to the bottom of the box and click on “Properties.” A table that is the security certificate should appear. You can check this out to help put yourself at east.
- If it give you an option to store any information, just say no. If you return, you can enter it all again.

Internet Security- Make Sure Your Passwords Protect You

In this day and age, protecting our internet security is very important. We store important information on the internet such as our personal information as well as out financial information. Identities are stolen everyday and getting yours back and clearing up the damage that it can cause is expensive and time-consuming.

One of the most important things you can do is to protect the passwords that you use for your various accounts. Why is this important? Because if someone gets a hold of your password, they can have all sorts of information about you.

Most people use their same password, or a variation of it, for all of their accounts. Needless to say, this is not a good idea. After all, if someone gets that password they can tap into almost any internet account you have and thus breech your internet security.

So what can you do?

First, don't use your same password for everything! And adding “1” after the password in instances when you need a number does not make the password different.

Secondly, don't store your password on your computer. Yes, it can be a pain to type it in every time, but if someone broke into your house they would be privy to all of your accounts.

Also, don't store your passwords on a notepad right there by your computer, or in a document on your computer called “internet passwords.” They should be a little harder to locate than that.

You can also use Microsoft's Password Strength Tester. This program lets you enter in a password to see what its strength is. If you give it something that doesn't test very strongly then you need to change it in order to make it more secure.

One thing that you can do is to make your password a combination of letters and numbers. This is more difficult to figure out. Also, don't ever use your social security number, driver license number, or zip code. You shouldn't be storing your social security number on the internet to begin with like that and your zip code is too easy to figure out.

In addition, don't use your child's name, your partner's name, or your own name as a password. Again, these are quite simple to figure out.

By following these tips when it comes to your password, you should be able to strengthen your internet security. While it is a hassle to come up with several different passwords and to remember them, it is more of a hassle to straighten out the mess that can result from not doing it.

Make Sure Your Emails Are Safe: Tips for Internet Security

The last thing you want to do is to have an unwanted e-mail wreck havoc on your computer. However, this happens everyday. At the best, it can make your computer run slower. At the worst, your personal and financial information can be stolen, or your entire computer can crash and everything could get lost due to a virus.

The following article includes some tips for internet security when it comes to your e-mail.

- Don't open attachments from people you don't know. This should go without saying. However, people do it all the time. Usually, the subject lines of these unwanted e-mails either make it look as though they are sending you something that you requested (“here's the information you asked for”) or they make it appear as if they know you (“Hey, it's me, John”). However, if you weren't expecting any email with an attachment and you don't recognize the sender's address don't open it. It could contain a virus.
- Don't give out any information. On the other hand, sometimes your internet security can be threatened from senders who pretend to know you and try to get you to give them information. For instance, if you are applying for jobs on various search sites, someone might contact you and say that they found your resume. They could then send you to another site and ask for your personal information, like your social security number, by pretending to have you fill out an application. Unless you are applying for a state or government job, or have already been through the interview process and they need to run a background check on you, you should never give out your social security number.
- Don't use the same passwords. Never use the same passwords for your email account as you do for your expedia account, online banking account , or any other website that stores financial information. It is fairly easy to figure out email passwords and once a hacker has it, they can get into your other accounts as well and your information can be used.
- Change your passwords. Also, remember to change your passwords from time to time. Try including numbers, as well as letters, in your passwords. It makes it harder to figure

them out.

- Don't let other people access your email account. Never give someone else your password when it comes to your email accounts. It's difficult enough for you to keep tabs on your internet security, much less trusting other people to keep it safe.

Internet Security- Why Should You Use a Firewall?

What is a firewall and how it will protect your internet security?

A firewall is usually part of the internet router and basically works by passing traffic between secure and insecure areas.

There are to kinds of firewalls: proxy servers and packet filters. Proxies are generally more expensive than packet filters.

Computers are identified by IP numbers a firewall can tell if a source is legitimate by comparing it to a set of rules that it employs. With a packet filter, the firewall won't let in sources that do not pass the rules. It more or less stands guard over your computer and won't let things pass through that do not adhere to its standards.

While firewalls are meant to keep things coming in, in some rare cases it can actually prevent users from getting out as well. This can be frustrating when you are trying to visit a site that you know is secure but for some reason your firewall has a problem with it and won't let you access it.

If this becomes a major hindrance, you can reconfigure your firewall settings. Of course, if you are part of an Intranet, such as at a place of business, there is little that you can do unless you, yourself, have access to the main computer and passwords. If you do have access, however, you can always add the site that you are trying to access as a 'safe site" so that the firewall will let you in in the future.

You can purchase internet security programs that contain firewalls. It is best to do some research on them first to get a good feel of what you are purchasing. Some are created superior to others. If you get a good program, it should also come with some adware and spyware blockers as well, and perhaps an anti-virus program. Of course, most good anti-virus programs also come with firewalls.

Although people often bemoan firewalls and the fact that they try to keep people out of sites that are sometimes legitimate, they can be a great way to protect your computer from harmful attacks. If you own and operate a business and have employees accessing the internet they can be especially helpful, too. It can be difficult to protect your internet security when you are dealing with multiple internet users. It's hard enough being safe yourself!

Internet security-Signs That Your Child's Safety Might Be Compromised

Although you do everything you can to protect your child, sometimes things get past parents and your child's internet security protection is compromised nonetheless. So how will you know if there is something going on with your child? The following is a list of signs to watch for that might indicate your child is suffering from internet related concerns.

1. Your child turns off the computer the minute you walk into the room. They might have been catting with their crush or significant other, or been been chatting with their best friend about something that they thought should be private. Or, they could have been looking at an inappropriate website. For this reason, you might want to invest in a tracking tool that creates logs of your child's internet activity that you can review.

2. Your child receives standard mail or packages from people you don't know. It is possible that they ordered something online. Ask them and then check your bank account or credit cards. However, sometimes predators do get online and pretend to be something that they are not. In some cases, they send their victims gifts in order to get them to become beholden to them. Open any packages that you weren't expecting. In some cases, it is better to ask for forgiveness than permission.

3. You find pornography on your child's computer. While it was true that growing up you might have sneaked a look at Playboy or something similar, Internet pornography can be difficult to get a grasp on. It is rampant and much of it is fairly different than the almost chaste images seen in Playboy. Some of it is also “deviant” pornography that includes bestiality and even child pornography. Therefore, the content should be monitored and communication should exist.

4. Your child becomes withdrawn. Sex offenders and other people who prey on children do their best to upset family interactions. If your child tells them a problem that they are having at home, the person will often try to make that problem appear larger in order to make the child more upset at the parent or sibling in an attempt to drive a wedge through the family itself. This is to gain more control of the child.

5. Your child spends a lot of time on the computer, especially at night. Invest in a time control device that limits the amount of time they can spend on the internet at once.

Internet Security- Protect Your Business

Although you often want to protect your children from harmful things on the web that can threaten their internet security, you might also be concerned about your business. There are several types of software that be purchased in order to help protect your business.

So what can these various types of software programs offer in terms of protection?

- You can use a filtering program that in some cases can block dozens of categories at once. You can also customize your filtering in order to choose what types of content you

want to be inaccessible to your employees.
- You can create an entire list of specific websites to block as well. That way, if you don't want your employees on Facebook while they are in the office, they will be blocked from entering the site. This is generally in addition to the filtering program that the software, or hardware, will offer.
- You can create a list of keywords that can't be used in search engines. This will also limit access to content and sites that are inappropriate for the workplace.
- Use the software to block Instant Messaging. This can be a problem in many offices where the employees want to chat with their friends, and sometimes even co-workers, when they are on the job.
- Create logs. Create and review logs of internet activity to see that everyone has been up to. These can show you what websites were accessed and the amount of time spent on the websites. It can also keep track of what people were searching for in the search engines.
- Prevent files from being downloaded, thus making it more difficult to get a virus, or download applications such as music downloading programs. This can protect your internet security from harmful bugs, spyware, adware, and viruses.

So does some of this sound like an invasion of privacy? Perhaps. Just remember that your employees are on the job and that you should be able to protect work computers from viruses and other harmful programs that can access your computers. You might want to make your employees aware that these things programs exist, especially the logs, so that they will not be blindsided. It is also recommended that you have a good computer policy in your employee handbook for the employee to read when they are hired. Make sure that you update it when necessary.

Internet Security- Safety When Using Public Computers

Many times, you might find yourself having to use a public computer. Perhaps the internet is down at your home or you have moved and it hasn't been set up yet. Or, you might be traveling and need to use an internet cafe or a internet site in the airport. These are generally okay to use, but you must use caution when you are accessing sites that ask you to use your password.

The following article will give you some information safety measures when using public computers.

First of all, when you are at home and you are accessing Expedia or Amazon or even your bank account, you might have your password already stored on your computer so that you can enter the site with a click of the mouse. And why not? It's a lot easier to do it that way. You don't have to remember your password and you're at home so you feel safe.

However, while this is a not a good idea even in the first place, it's an even worse idea to do it while you're using a public computer. More often than not, when you enter a site on a public computer and it asks you for your password it will ask you if you want the site to remember it or not. Always answer no.

Some public computers will actually reset everything once you have logged off. Your browsing history and any information you entered while you were using it will be erased. However, this isn't the case with every public computer. So, to protect your internet security you are better off ensuring that nothing personal is left behind.

Have you ever entered your pin number at the store or at an ATM machine and had someone standing right behind you? Were you afraid that they might read your number and use it themselves? You should use the same caution when using public computers. The person sitting down after you, or standing behind you, might easily find out your passwords and use them to their advantage.

This is not to say that you should be paranoid. When you are finished, it helps to erase all of your browsing history, as well as any cookies that you might have used. Check under “internet tools” at the top to see if any passwords were remembered. It is better to be safe than sorry at any rate.

4 Email Scams that Threaten Your Internet Security

Do you trust your e-mails? It's hard to believe, but there are people out there who have nothing better to do then to think of ways of conning other people out of business. It actually is their business to scam. Don't let your internet security be threatened by these scammers.

The difficult thing is that while some of the scams sound outlandish, many of them also appear legitimate, too. Intelligent people have been scammed and had their internet security threatened when the emails appeared real.

To help keep you and your information safe, the following is a list of 4 email scams that can threaten your internet security.

1. The bank scam. This is one of the more realistic sounding scams. A supposed bank will contact you and tell you that they have had a security breech and that you're information has been violated. They will then direct you to an outside website where you are then supposed to enter your personal and banking information to “protect it.” First of all, you wouldn't receive an email from your bank if this happened. Secondly, never enter your banking information like this. If you feel like it could be true, call your own local bank branch and ask them.

2. The fake job scam. In this scam, a person e-mails you and tells you that they found your resume and are interested in hiring you. They then direct you to a website where you are asked to enter a bunch of information such as your social security number and driver's license number. A legitimate business would ask you to call them to set up an interview.

3. The lottery scam. Here, a person will write you and tell you that you have won the lottery. Again, you will be directed to a site where you will be asked your banking information so that the money can be deposited. Don't fall for it. This is not the way the lottery works.

4. The foreign money scam. This is a great one as well. A person will write you and tell you that they live in a foreign country and came into a lot of money. They will ask you to deposit it for them in your account and as a result they will give you a chunk of it. Just say no. They want your account information to take your money.

Internet Security- Storing Your Password on Your Computer

One of the most common things that you do might be threatening your internet security. It's a mistake that nearly everyone is guilty of making. What is it? Storing your password on your computer.

When you create a new account, or sign into your account, your computer generally asks you if you would like to have the password saved. It makes more sense to answer “yes” due to the fact that it makes life a little simpler to not have to re-type your password time and time again. However, doing this can compromise your security and your personal information.

Aside from the fact that if someone comes into your home and gets on your computer, they can easily have access to your accounts, saving your password also allows hackers easier access to your accounts as well.

Think about the accounts that you might have saved your password on. Expedia, for example. Even within Expedia you save your credit card number, billing information, and other pertinent financial information. In fact, you might have more than one credit card number entered in it.

Another account that you probably have personal information stored in is Amazon. Again, with this type of account you store your credit card information. Although Amazon itself is a secure site, someone with access to your information can use it against you to make purchases, open new credit cards in your name, and generally ruin your credit.

Your bank account is one of the most important things that you need to protect. With online banking being very popular these days more and more people are using it instead of traditional banking. However, is your information gets into the wrong hands then someone can transfer money from your bank account or even use your information to open an account in your name.

Job search sites can also be a problem. In some cases, you have to enter your social security number or driver's license number in order for them to run a security check on you. These are two things that you do not want people to have access to.

If you have trouble remembering your passwords, write them down on a piece of paper and store them close to your computer, but not in an obvious place. Many people actually create a file on their computer but then they name it something like “computer passwords” which isn't very secure at all.

Internet Security-What Does Your Large Business Require?

Why is internet security important for a large business? There are several reasons.

One of the most important reasons is due to the fact that a breech of internet security can threaten the very livelihood of the company itself, including vital information such as financial formation. For that reason, one system should be able to keep track of recording and monitoring all internet activity across the board when it comes to the business itself.

There are a couple of different ways that you can go about doing this. To begin with, you can monitor your employees using restricted access and by not allowing access to certain websites. (A lot of companies block facebook and myspace, for example, much to the chagrin of the employees).

It is important to do this because many large businesses are threatened by hackers who get onto the internet and hack into the business's system and threaten secure information. They do this by either gathering the information to use for various reasons, or by sending out viruses that can harm the integrity of the system itself. By restricting access and monitoring your employees, you can help stave off some of these attacks.

A good security protection system within each computer is also recommended. This can be in the form of a firewall or anti-virus program-preferably both. By installing these, you can try to ward off some of the most common attacks. Programs that block adware and spyware is also suggested and should be included as part of a good anti-virus program, too. In addition, it should be noted that updating your web browser from time to time can be advantageous as well. (Windows Vista does it for you automatically.)

Some companies have started having internet training sessions for their employees as well. In these sessions, employees are taught the dangers of opening attachments from people they don't know, changing their passwords frequently, and staying away from sites that are not secure.

Ensure that the email system that your employees use has a virus system included as well. A good system will read and scan the attachments quickly to ensure that there are no viruses included. Some of them even do this right as the emails come in, making it go a little bit faster.

Lastly, make sure that you always back up your important fields and documents and make certain that your employees know to do this as well. Invest in flash drives for everyone.

Internet Security-Using Social Utility Sites

If you don't have a Facebook, Myspace, or Twitter account then you are among the few. Social utility sites are some of the most common websites on the Internet today. Children as young as ten years old can build their own websites and upload music, photographs, and videos on them. They can be a great way to keep in touch with family and friends, promote your business, or even meet new people. However, do they threaten your internet security?

In some cases, they can. They can also threaten your personal security if you don't make wise decisions about how you use them.

Like in “real life” you should use caution in your “virtual life.” You wouldn't give someone on the street a photograph of your child, your phone number, or your address, right? Well, believe it or not millions of people do that on the internet everyday.

On Facebook, it gives you a place to enter your employment information, your address, your telephone number, and your work history. If you choose to make your profile public, that means that anyone who looks at your profile can read all of that.

Facebook also has applications that require you to pay for certain things. (Usually things like “gifts” that you can send to people on your friend's list.) However, if someone hacks into your account they can steal your credit card information. This is particularly easy if you store your password on your computer.

In addition, sometime people hack into social utility sites, use a person's profile, and send out viruses to the people on their friend's list. When this happens, the victim's friends open the e-mail thinking that it is from someone that they know, only to be hit with a virus that could crash their entire system.

To avoid this, make sure that you change your password on a regular basis and that you keep diligent watch of your activity. If you decide not to use your account anymore, have it deleted.

Always ask permission before you include a photograph of someone on your site. Many people do not want their picture posted for various reasons.

Don't add someone if you do not know them. It I very easy to pretend to be something that you're not when it comes to the internet.

Lastly, make your profile private so that only the people on your friend's list can see it. This will stop unwanted people from lurking on your site.