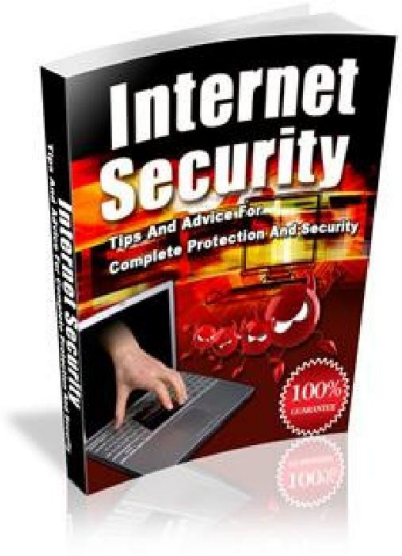
Internet Security Tips and Information

By Joe Black, Courtesy of WindowsRepairTool.com



Contents

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.

Parental Control Software Lets face it life keeps us to busy to be able to monitor our children's internet activity completely. And as much as we would like to believe our children our being honest with us it's highly likely they are not. The harsh reality is our children know more about technology then we do and can easily hide their activity from us. If you want the piece of mind of knowing your children our safe invest in Parental Control Software. There are many great products available. To save you some time I have provided a link to the software I use personally. Click here

Handling Email

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?

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?

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.

ParetoLogic Anti-Virus PLUS is a **Microsoft Certified Anti-virus and Internet Security Suite** that is surprisingly affordable. These days we are all on a strict budget.
I recommend this software because it is every bit as good as Norton and MacAfee but at a fraction of the cost. This product is an all in one solution. It includes malware, spyware as well as Anti-Virus protection and elimination. Click here to learn more.

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 are 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 control**s. Program controls control the access to certain programs such as downloading music files or other files that could be dangerous.
- **All in one solution**. Look for an advance piece of software that has all its bases covered. Email recording, Content filtering, and Keystroke logging are among the most important.

There are many great products available. To save you some time I have provided a link to the software I use personally. Click here

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