How to Protect Yourself Online From Hackers, Cyberstalkers and Identity Theft

Hacking, spam, malware, viruses and identity theft are of concern to anyone who spends any significant amount of time online. This describes many millions of people, most likely including you, if you're reading this!

Identity theft is just one of the security concerns that face internet users today. Hacking, spam, phishing and malware are some others. These can overlap, of course -for example, some phishing attacks are done with intent to steal your identity.

Today's Internet -What are the Risks?

There are many risks involved with being online today, but you have to keep things in perspective. You want to be safe and vigilant, but not paranoid. The fact is, most of the time, you can safely surf the internet.

Furthermore, most spamming and cyberattacks are more annoying than dangerous. However, you also have to be aware that there are some serious scammers and criminals who target online users.

This doesn't mean you should be constantly worried about this. It does mean, however, that you should be alert and take the proper precautions!

Let's take a brief look at the different types of dangers and attacks that can occur online.

Spamming

This is the most common and -usually- least dangerous

type of online nuisance. Most spammers are out to sell you cheap and often fake merchandise or services. We've all gotten emails on topics such as dating sites, cheap pharmaceuticals, get rich quick, and countless other topics.

Spam is essentially any unsolicited email from someone you don't know. As a rule, you should never respond to spam in any way, except to report it. If it comes in your regular inbox rather than spam folder, all you have to do is mark it as spam.

That way, the sender's address will be blacklisted. Of course, in reality, spammers change email addresses constantly, so you will probably get more spam from them in the future anyway. But it's still a good idea to report it, as it makes things at least a little more difficult for them.

The most important thing to know about spam is to never open an attachment that comes with it. This is where spam can lead to bigger problems than an everyday nuisance. Attachments may contain viruses, malware or some type of scam you really don't want to get mixed up with.

Some of the most notorious types of spam emails include those send by financial scammers. these include:

- Nigerian email scams (though they often come from many other places as well)
- Various "notifications" of large deposits into your bank account
- Official looking notices from your bank, Paypal, eBay or some other site that involves financial transactions

- Notification that you've won the lottery -usually the UK or some European lottery that you've never even played

Some spammers are clever and they send emails that look legitimate. If you get an authentic looking email from anywhere and you want to be sure that it's real, there's a simple way to verify it-

Simply close the email and log onto the site itself. If your bank, Paypal, eBay, etc. has an important notification for you, you can be sure it will appear when you log on. In most cases, though, such emails are spam if you weren't expecting anything.

More clues include the presence of an attachment or a demand for you to provide your password or other personal details.

Manage Your Email

Many people do things that encourage the pileup of unwanted emails. A lot of this isn't spam, at least not technically.

If you voluntarily sign up for an email list or agree to receive email from a person or company, they have a right to send it to you. If you want to stop receiving it, there should be a box or form where you can opt out.

Before you sign up for anything, remember that some companies will email you frequently if you give them permission -sometimes multiple times per day! So if you want to cut back on such emails, be careful what you send for or agree to.

Computer Viruses

Just like the type of virus that makes people sick, a computer virus is designed to make your computer "sick." These are usually created by malicious hackers who mostly do it for their own entertainment.

Occasionally, there is a political or economic motive behind them, but that's more when large companies are attacked. Hackers who target random websites are just getting a thrill out of seeing how much damage they can do.

There are a few things you can do to minimize the risk of getting computer viruses.

- *Keep all of your programs and applications up to date*
- *Use virus protection software*
- *Be careful and don't download attachments from anyone you don't know or trust*

Spyware and Malware

In everyday use, spyware and malware mean roughly the same thing, although there are more technical definitions for each. In essence, these are software programs that are placed on your computer without your knowledge.

These programs do things that are malicious, for the benefit -or, in some cases, merely the amusement- of the sender.

Malware is often sent with a commercial intent. The program may capture your email address so the sender can spam you later on. Or the program may redirect you to sites that you would never have gone to on your own.

They can also cause annoying pop-ups to appear.

You may wonder how malware of this sort can be effective. After all, when you receive spam, you probably just delete it and/or report it. You probably shut down pop-ups or quickly leave sites you're not interested in.

However, the mentality of the spammer and malware creator is one of numbers. They know that if they blast out millions of these programs, a small minority of victims will take the bait. That's all they need to make it worthwhile for them. So make sure you're not one of these victims!

Some malware is even more malicious than just trying to get you to buy some bogus diet pills. Some malware is used in order to capture your personal information for the purposes of stealing your finanical data or your whole identity.

This is one of the tactics used by identity thieves. So you should do everything you can to avoid malware, as its consequences can range from annoying to catastrophic.

Identity Theft

The words "identity theft" probably strike more fear into the hearts of online users than any others. This is the ultimate nightmare -having your entire identity stolen, which can mean your bank accounts or credit cards raided.

In extreme instances, it can even cause legal problems, if someone commits crimes using your name, social security number or other data.

Identity theft can have extremely serious consequences to your finances. An identity thief can empty out your bank account or max out your credit cards in a day. They can also do lots of damage to your credit rating.

Identity theft can be accomplished in a number of ways. The internet is one of the main tools of identity thieves, but not their only one. They also steal cell phones and steal obtain people's personal data by spying on them at ATM machines.

Precautions to Take Online

Fortunately, you don't have to be an expert on computer programming or security measures to stay a lot safer online. Many of the most common security issues people face online can be dealt with by using common sense and taking some basic precautions. Many of these are free, while some may involve spending a few dollars.

Be Alert!

This is the most important piece of advice. Many people who fall for online scams, or who have their data stolen are guilty of making minor mistakes that they really should have known not to make. Sometimes this is due to ignorance. More often, however, it's a matter of carelessness.

Passwords

Passwords are one of your main weapons against cyberattacks of all kinds. They aren't infallible, but then nothing is. The fact is, though, that using strong passwords and changing them frequently will go a long way to protecting you online.

As cumbersome as it may be, use separate passwords for all of your major accounts. This is especially true for any sites that involve financial transactions. Yet, it should really be applied across the board. In other words, your Google, Yahoo, Paypal, eBay and Facebook passwords (or whatever sites you typically log onto) should all be completely different.

A surprising number of people, for the sake of convenience, use one -often easy to guess- password for all of their accounts. This is a dream come true for scammers and identity thieves. This means that all they need is one of your passwords and they have them all! Don't make it so easy for them.

Additionally, make your passwords difficult. You've probably heard this before, but many people use ridiculously easy passwords to guess -such as their names, birthdays or other significant dates.

Remember that so much information online today is available to anyone who knows how to use a keyboard and mouse. Finding out your date of birth is not very difficult, so if this is your secret password, don't be surprised if your identity is stolen one of these days!

It's also a good policy to change your passwords regularly. The reason for this is that hackers sometimes succeed at breaking into major websites and stealing passwords. You've probably heard about this at one time or another.

There's also always a possibility that your own computer, one of your websites or accounts has been hacked. So it's just common sense to change your passwords every couple of months, at least.

Keeping track of all these difficult, unique and changing passwords can be a hassle, to be sure. Yet it's a lot less of a hassle than having your identity stolen or having a nasty virus attack your computer!

CyberStalkers

Cyberstalking is term used to describe stalking someone on the internet. Whereas in the past, a stalker would have to follow someone in person or perhaps call them on the phone, now they don't even have to leave their damp basements or the cafes where they sit with their laptops -they can harass you remotely.

Unlike other forms of computer crimes and cyber attacks, cyberstalking is usually personal. For example, a rejected spouse or boyfriend or girlfriend might stalk his or her ex after a breakup. Or someone may have their eye on a co-worker or fellow student and begin harassing him or her online.

Of course, cyberstalkers sometimes go after people they've only found online. Perhaps they found a picture or profile that appealed to them, and not being very socially adept, sane or ethical, they decide it would be fun or satisfying to go after this person and follow them around online. Or they might begin to do this if you've rejected their attempts at becoming your friend.

The most serious and unfortunate type of cyberstalking is targeted against children. That's why parents must be very vigilant about safeguarding their kids who use the internet.

We will discuss some specific ways to minimize your vulnerability to cyberstalkers in the section on Safe Surfing and Social Networking.

Safe Surfing and Social Networking

Many problems occur when people surf the internet in a careless manner. There are also common issues involved with popular social networks that you should be aware of.

Shopping online has become a common practice, and it's usually safe. However, you should be aware of who you're dealing with before parting with your credit card or Paypal information.

It's best to only shop on trusted and reputable sites. These sites have a high level of security in place. You will see a padlock symbol on such sites to verify that they are secure.

Shopping on smaller or unknown sites is always a little risky. The person or company you're shopping with may be honest, but if their site isn't secure, it can easily be broken into.

The growth of social media sites, especially Facebook, has created a revolution in the way people interact online. It's also created lots of opportunities for hackers, cyberstalkers and identity thieves to gather personal information about people.

Watch What You Post on Social Sites!

The above is one of the most important statements in this whole report. Many people make it easy for unsavory characters to get sensitive information by simply posting it for all to see on Facebook or other social sites.

Be careful before you post

- *Photographs*
- *Your phone number (cell or landline)*
- *Your current or future location*
- *Information about relatives or children*

Facebook in particular encourages people to be very open about what they're doing and where they're going.

If you're active on social networks, consider how your privacy settings are set up. You may want to have it so only friends can see your details. And be careful about what details you reveal to anyone.

Identity thieves, hackers and cyberstalkers are often clever individuals who are good at piecing information together. They can Google you, check out your Facebook, Twitter, LinkedIn, etc. profiles and so forth. If you put out too much information, they can easily use this to build their own profile on you.

Additional Tips to Protect Yourself Online

As we've seen, a great deal can be accomplished by staying alert and using common sense. Be careful what kind of information you post, downloading attachments and shopping online. Keep your software updated, and use quality anti-virus programs.

Aside from these recommendations, however, there are some additional steps you can take.

- *Keep Track of Your Credit Report -this keeps you up to date about what's going on with your credit, and if there's been any unusual activity. If something does happen, you want to know as soon as possible.*

- *Be careful about revealing your social security number -this is the primary way you are identified by the government, financial institutions AND identity thieves!*
- *Use a paper shredder to shred any old documents or paperwork with sensitive information.*
- *Use discretion offline as well as online -make sure you're not being watched when you use your ATM card or listened to when giving any important information over the phone.*

Conclusion -Staying Safe Online

When it comes to protecting yourself online, you have to understand that a certain amount of risk is unavoidable. This is true for everything in life, online or offline. However, you can greatly reduce the chances of many problems occurring by keeping the above tips in mind.

Hackers, identity thieves and cyberstalkers rely a great deal on people being careless or uninformed. Most of them aren't willing to go to too much trouble to go after you -if they were ambitious they would get real jobs!

They prefer to prey on those who are foolish enough to open strange attachments, use easy to guess passwords or reveal everything about themselves on Facebook. So make sure you don't make yourself such an easy victim.

The internet provides us with innumerable opportunities

to educate ourselves, to socialize and to have fun. Just make sure you enjoy these things safely!

To find out more, and learn how to protect yourself,

visit our partners by clicking here