

## **Have fun, stay online & protect your teenage children**

Your teenage children probably love the internet as much as other people their age. As far as they're concerned, it's an extension of their life: they can meet friends in chat rooms, exchange views in forums, build communities that they actually identify with on social networking sites and so on. It's a great way of letting teenagers express themselves, share pictures, videos and the like. And from a parent's perspective, it may feel safer too. After all, your children are better off hanging around upstairs with online friends than being out in the park, aren't they? But there are risks on the internet too. Kids will be kids and they are always at risk of meeting rather dubious characters, and being lured into fun but dangerous activities. Fortunately, by keeping yourself informed about what your teenage children enjoy about the internet, by helping them to explore cyberspace safely, and by making sure that they know to come to you if they feel threatened or encounter any sort of problem online, you can greatly reduce the risks they face. The key, here, is communication with your children! It's a three-way exchange of information between the web, your children and you.

Here are a few tips to ensure that you remain fully aware of what your children are doing on the internet.

### ***Know what your teenagers are downloading and sharing***

Don't let them download unauthorized copies of copyrighted music from a file-sharing network, or let them share copyrighted music by using instant messaging (IM), email, or by handing out or uploading CDs. Be careful: even if you think your kids are "just downloading music", the way most peer-to-peer software programs work means that while you're downloading, you're also sharing the data you're downloading at the same time!

If you use a file-sharing program, make sure you only turn it on to update files. Set read/ write passwords for your shared folders to protect yourself from other computer users for whom an unprotected folder might be a convenient dumping ground for their files.

### ***Treat online stores like real stores***

Just because it's an online store doesn't mean your children should abandon all common sense! There are things they would never do in a real store — like leaving their wallet open on a jeans promotion shelf and then walking away — and they need to recognize when they behave carelessly online. Before submitting credit card numbers or other confidential information over the internet through an apparently secure connection, get them to check that the store's internet address is authentic (and teach them never to follow a link that someone else has sent them, e.g. in an email, but instead to type the address of their favorite stores into their browser themselves). They should also pay attention to estimated delivery dates. Sites that only offer delivery dates more than 20 days after payment involve more risk.

Installing a good internet security program with parental controls can help you to block inappropriate websites. Better still, you can set it up to filter data leaving your computer in order to prevent your teenage children from divulging personal information without your permission.

### ***Get online gaming under control***

Some games are played directly on the web. They require you to turn on ActiveX or JavaScript controls. These are programming languages that let developers to create programs capable of interacting with your web browser to a much greater degree. Although these codes can be very helpful when they are turned on, they can also prove very useful to hackers who want to gain entry to your computer. When your children have finished playing games online, make sure they turn off the ActiveX and JavaScript controls in your browser's configuration menu (usually requires a check box to be unchecked).

It might be a good idea to set up a separate user account for online gaming, with only a web browser installed on it. When they've had enough, your children can switch back to the full account. When playing an online game, it's more sensible to play it at the game site rather than at any one of the score of amateur websites also hosting it.

### ***Conclusion***

Help your teenagers to enjoy everything that the internet has to offer. By taking precautions and teaching them to stop and think before either downloading anything from the internet or divulging too much information, you can protect your identity, private documents, your computer, and most importantly, your children, from security threats. To reduce the risks, make sure your computer has security tools installed like Norton Internet Security and Norton Confidential — these can all help you to have fun and stay safe.

## How to Protect your Identity – Online and Offline

Many of us go online several times a day—we might email a friend, place an auction bid, or sell a few shares of stock online. And each time we log on, our identities are at risk. Sadly, there are people out there trying to gather enough of our personal information to create a virtual composite of who we are, which they can sell to others or use for themselves, perhaps even opening lines of credit in our names. That's why identity theft has become such a hot topic these days. Fortunately, there are many real-world and online precautions you can take to limit your exposure and protect your identity.

### ***Everyday Vigilance***

Most precautions are common sense. The challenge is in the details and execution. If you want to reduce your exposure to identity theft, incorporate these steps into your regular routine.

- Don't carry documents and cards you don't need. That includes your social security card, passport, and extra credit cards. When you're not using these items, lock them away in a safe place—along with other identifying documents, like your birth certificate and will.
- When you dispose of documents containing personal or financial information, shred them before tossing them in the trash or recycling bin. That way dumpster diving identity thieves will have to work extra hard to piece together those credit applications, convenience checks, and financial statements. The same policy applies to expired drivers licenses and credit cards. Be sure to cut up them up when you receive replacements.
- Take special care with your mail. Put a hold on it while you're on vacation, and arrange for sensitive packages (like new checks) to be picked up at the post office. You might even consider mailing your bills from the post office rather than placing them in your mail box where a thief could come by and snatch them.
- Memorize your PIN numbers, and if you've written them down somewhere, tear up those pieces of paper. Whatever you do, don't carry PIN numbers in your wallet or purse.
- Carefully review your banking, investment, and credit card statements each month. Make certain there hasn't been any unusual or unauthorized activity. And to make sure no one's using your identity to apply for credit, check your credit activity with one of the major credit bureaus at least once a year.

### ***Online precautions***

Even if you have your paper trail covered, the Internet presents a whole other arena for identity thieves to operate. And because the online landscape is ever-changing, you need to be extra vigilant as you use your computer. Here are some key ways to protect yourself online.

- Learn to spot phishing scams. Using fake emails and Web sites to pose as legitimate organisations, phishers trick people into divulging passwords, credit card numbers, and other sensitive information. These counterfeit emails and Web pages are almost indistinguishable from the real thing; so be extremely cautious with online requests for important information. And remember, legitimate organisations will NEVER ask you to verify personal information over the Internet.
- Never send your social security number over the Internet. If you get a request for it, verify the authenticity of the requestor and then provide it directly to that person.
- Be cautious with email. Many phishing scams use spam email as part of their deception; so get a good antispam program to reduce your exposure to misleading emails. And because email and IM aren't always secure, never use them to exchange sensitive information.
- Password-protect all your computers, laptops, and PDAs. Use unique user names and passwords, combining letters with numbers and special characters. Be sure to use especially strong password combinations on your guest accounts.
- Try to minimise the amount of personal or financial data on your computer. That way if your laptop or computer is stolen or hacked, you'll have less exposure to identity theft.

- Use a personal firewall. A good firewall program hides your computer from hackers, gives you control over all Internet traffic on your computer, and automatically blocks intruders who may try to get at sensitive data.
- Buy antivirus software and update it regularly. A good virus protection tool will protect your data from viruses, Trojan horses, and other malicious code.
- Never open an email or IM attachment unless you know who sent it and what's inside. And make sure your antivirus software scans both email and IM attachments.
- Install an antispyware program. While a lot of spyware programs simply monitor your Websurfing habits, some are used for malicious purposes, including keystroke logging and identity theft.
- If you sell or give away your computer, remove your data from the hard disk before delivering it to the new owner.

---

**Your identity is an irreplaceable possession, and if someone steals it, you may find yourself dealing with the ramifications for years. So be judicious with your personal information, keeping it private and safely locked away; because in the end, your own habits and a good set of security tools are your best defense against identity thieves.**

---

### ***Top Tips:***

1. Don't carry your Social Security card in your wallet or purse, and if you get a request for your Social Security Number, verify the authenticity of the request and the identity of the requestor. When you're satisfied, provide your number directly to that person—not over the Internet.
2. Learn to spot phishing scams. Phishers are among the most notorious online identity thieves. They use scare tactics and other deceptive practices to elicit personal information from unsuspecting Internet users.
3. Be cautious with email. Many phishing scams use spam email as part of their deception. So, get a good antispam program to reduce your exposure to misleading emails. And because email and IM aren't the safest ways to communicate, never use them to exchange sensitive information.
4. Use strong passwords—combining letters with numbers and special characters—to protect important files, folders, and all your computer accounts. Try to minimize the amount of personal information on your computer. And if you sell or give away your computer, remove all your data from the hard disk before delivering it to the new owner.
5. Use a personal firewall, antivirus software, and an antispyware tool to protect your sensitive personal data from hackers and malicious code.

## Take Control of Spyware and Adware

These days—whether we are checking the latest stock quotes, sending an email to an old high school friend, or instant messaging a relative in another country—there may be someone monitoring every move we make. This trend is more than a little disconcerting, striking at the heart of our sense of privacy and freedom. Unfortunately, spyware and adware have become an all too common annoyance and security risk.

But what exactly is spyware, and how is it different from adware? What sort of harm can these programs cause? And is it possible to control them? These are all good questions. And despite the confusion surrounding these technologies, each question has an equally good answer.

### ***Is it spyware, adware, or simply unwelcome?***

There is some debate—even among security experts—over the definition of spyware. However, if a program installs itself on your computer so it can capture private information without your knowledge, it's probably spyware. If the main purpose is presenting ads or routing you to a commercial site, it's adware. Of course, what you call the software doesn't really matter. The most important question is whether you want it on your computer. If it compromises privacy and security as you define it (or at a minimum, becomes an nuisance), then it falls squarely into the category of unwelcome software. And that means you need to learn how to deal with it.

### ***How harmful can it be?***

While a lot of spyware and adware programs are fairly harmless, some spyware puts your privacy, data, and identity at risk. These programs employ clever, highly sophisticated methods to get at your most private information. And while not all spyware is dangerous, that's not to say their more benign cousins aren't a serious problem. Programs that constantly launch pop-ups are maddening. And some spyware and adware, working busily in the background, can dominate your system's resources, sometimes bringing down your entire system.

### ***Where does it come from?***

So, how does this unwelcome software find its way onto your computer? It can happen in a number of ways. Spyware and adware often get installed along with free programs you download from the Internet. Or they can make their way onto your machine as you surf the Web, in many cases lurking behind an intriguing pop-up window or fake dialog box. And while some spyware programs sneak quietly through browser security holes, downloading unwelcome software typically requires some action (or inaction) on your part. And that's good news, because it means you retain a fair amount of control.

## ***How do you avoid spyware and adware?***

The following practices can reduce the likelihood of inadvertently downloading unwanted spyware and adware:

- Be selective about what you download to your computer. If you don't have a reason to trust the company providing a piece of software, hold them to increased scrutiny. Visit their Web site to learn more about the people behind the technology, as well as the technology itself.
- Read licensing agreements. Don't just scroll to the bottom and click the "I accept" button when installing freeware. Instead, read each agreement carefully and look for language pertaining to information-gathering activity.
- Watch out for antispymware scams. The Web is rife with "antispymware" tools that do little or nothing to prevent spyware, and some even make it worse. Purveyors of these tools often provide free scans, which almost invariably identify hundreds of spyware programs on your computer. They then immediately ask you to buy their bogus product.
- Beware of programs—especially free ones—that flash clickable ads in the user interface. Their presence is a red flag, and it's possible someone is watching how you respond to them.
- Keep your Internet browser up to date. Because browser security holes are a common pathway for spyware and adware downloads, it's important to apply any and all security patches when they become available for your browser.
- Disable scripting and active content unless you really need it. Scripts—especially ActiveX controls—are common tools for installing spyware without your knowledge or consent. You can always turn on scripting should you need it for a trusted site.

These recommendations go a long way toward reducing the amount of unwelcome software on your computer. However, even the most vigilant users can't stay on top of everything. That's especially true as the methods of spyware distribution continue to evolve, becoming ever more sophisticated. Fortunately, despite the widespread existence of fly-by-night antispymware vendors, it's possible to get effective spyware protection tools from trusted security experts. With a good antispymware solution, you control what gets in, what stays out, and what remains on your computer. In the end, that's the only way to get a handle on unwanted, uninvited software: by taking control.

Spyware and adware aren't going away anytime soon, and fortunately, you can take charge of the situation.

### ***Top Tips***

1. Install a good antispymware tool—but watch out for antispymware scams. The Web is rife with "antispymware" tools that do little or nothing to prevent spyware, and some even make it worse. Make sure you get your tool from a trusted vendor.
2. Be selective about what you download. If you don't have a reason to trust the company providing a piece of software, hold them to increased scrutiny. Visit their Web site to learn more about the people behind the technology, as well as the technology itself.
3. Read licensing agreements. Don't just scroll to the bottom and click the "I accept" button when installing freeware. Instead, read each agreement carefully and look for language pertaining to information-gathering activity.
4. Beware of programs—especially free ones—that flash clickable ads in the user interface. Their presence is a red flag, and it's possible someone is watching how you respond to them.
5. Disable scripting and active content unless you really need it. Scripts—especially ActiveX controls—are common tools for installing spyware without your knowledge or consent. You can always turn on scripting should you need it for a trusted site.