**The Most Common Internet Security Issues**

**1. HACKERS**

Hackers are people who attempt to breach or avoid online security measures for a number of reasons.

* Their motives are, occasionally, honorable in that they simply wish to highlight shortfalls to corporations and other website owners so that they can tighten their security up.
* Other[hackers](http://www.security-faqs.com/ebay-hacker-caught.html) look to make financial gains by copying private information, whilst others are purely out to cause mischief.(trouble)

Irrespective of the hacker’s reasons for doing what they do, they can pose a serious threat to your security.

**2. VIRUSES**

Computer viruses are programs which are designed in order to gain entry onto unsuspecting users’ computers. Once they have gained a foothold within a computer system they will then attempt to duplicate themselves before spreading via email, networks and/or removable storage devices. Typically, their remit is to corrupt or destroy data or otherwise damage the operation of the machine on which they reside.

Viruses can be acquired in many ways but some of the more popular ones are through email, [peer-to-peer downloading](http://www.security-faqs.com/the-risks-of-peer-to-peer-file-sharing.html), internet messaging services and downloading infected files found on the internet.

**3. SPYWARE**

Spyware can prove to be a major annoyance as its goal is usually to collect personal information and browsing habits in order to deliver targeted advertising to you as you browse the web.

[Spyware](http://www.security-faqs.com/spyware-and-how-to-get-rid-of-it.html) is software and, like a virus, is often deceptively added to the user’s machine.

In addition to increasing the amount of advertising you are likely to see, or affecting the type of adverts served to you, it can also impact upon the performance of your computer by hogging resources.

**4. WORMS**

A worm is a self-replicating program which will attempt to spread itself around your network, either via routers, the internet or by email.

Unlike a virus, a [worm](http://www.security-faqs.com/7-days-later-confikerc-wakes-up.html) does not need to attach itself to another program in order to spread.

While a virus has to attach itself to an existing program, a worm does not – it can replicate and spread on its own.

Worms too can cause disruption to computer systems because of the excessive amount of bandwidth that they sometimes use.

**5. PHISHING**

In some respects, phishing is a confidence trick, designed by would-be (possible) thieves in order to part unsuspecting computer users from their most precious personal and/or financial information.

Traditionally, phishing attempts looked to acquire data such as **bank account details, social security numbers, and credit card numbers, either for direct financial gain or to facilitate identity theft.**

Over the last few years, however, other forms of data and information have become valuable too.

Phishing attempts are now just as likely to target users of [**social networking sites**](http://www.security-faqs.com/5-types-of-social-networking-scam-4-identity-theft.html) in order to try and steal their accounts either to use them as a launch pad (start) for socially engineered scams or as a means of spamming the victim’s friends and other contacts.

Phishing scams usually arrive via email and are designed to appear to be from legitimate organizations so as to trick the recipient into responding with their personal information.

Many will even spoof email headers so that they appear to have come from a trusted source, or link to fake websites that are clones of the official sites that they purport to be.

**6. SPAMMING**

Spam is any form of unsolicited message, be it email, private forum message or even [Tweet](http://www.security-faqs.com/4-ways-to-spot-a-twitter-spammer.html).

Those behind spam know that the response rate to their rubbish will be incredibly low.

They continue, however, because they can send many thousands of spam messages out every hour of the day at next to no cost.

Therefore, even an incredibly tiny response rate can lead to huge profits for the spammers.

[Spam messages](http://www.security-faqs.com/spam-what-is-it-and-why-is-it-still-here.html) don’t usually pose any threat to your security but can be incredibly annoying and distracting.

It is, however, possible for savvier spammer to hide other unwelcome items within their spam messages, such as viruses, worms, spyware and other malware.

**7. IDENTITY THEFT**

[Identity theft](http://www.security-faqs.com/protection-against-identity-theft.html) is a growing problem, both online and off.

This crime can seriously damage a victim’s finances for many years.

Identity thieves acquire information about someone through a variety of means of which the favorite is phishing.

If they can get personal data, such as names, dates of birth, social security numbers, etc, then they can quite literally steal the identity of the owner of that information.

That fake identity can then be utilized in a variety of other crimes, such as credit card fraud, bank fraud and a whole host of other financial misdemeanors, all of which will be blamed upon the victim who will then have an incredibly hard job of clearing their name, recovering the money they have lost and then repairing their credit file.

# [How to Fix Common Internet Problems](http://www.wikihow.com/Fix-Common-Internet-Problems)

**1) Manage your browser’s cache**. Make sure you know how to [clear your browser cache](http://www.wikihow.com/Clear-Your-Browser%27s-Cache), which includes your cookies, temporary internet files, browsing and download history, form data, and so on. You can also do an intensive clean by [deleting your usage history tracks on Windows](http://www.wikihow.com/Delete-your-Usage-History-Tracks-in-Windows). To deal more specifically with cookies, read up on how to:

2) [**Clear your Google search history**](http://www.wikihow.com/Clear-Google-Search-History). Though Google Search History is designed to customize search results to fit your needs, many people aren’t comfortable with being tracked by such a huge and powerful organization.

3) **Stop ads and spam**. One of the easiest ways to do this is to use an ad-blocking program. Try [Adblock Plus on Firefox](http://www.wikihow.com/Remove-Ads-from-Mozilla-Firefox-Using-Adblock-Plus) or [Adblock on Google Chrome](http://www.wikihow.com/Remove-Ads-on-Google-Chrome-Using-AdBlock). (You can also go through a special procedure to specifically [block ads in Hotmail](http://www.wikihow.com/Stop-All-the-Ads-in-Hotmail).) Make sure you also know how to [prevent and block spam](http://www.wikihow.com/Stop-Spam).

4) **Avoid bugs**. Make sure you know how to [avoid getting a virus or worm on Windows](http://www.wikihow.com/Avoid-Getting-a-Computer-Virus-or-Worm-on-Your-Windows-PC) and [get rid of adware, spyware, and viruses](http://www.wikihow.com/Rid-Your-Computer-of-Adware%2C-Spyware-and-Viruses) once you do have them.

5) **Restrict certain sites**. Make sure you know how to [filter porn from your computer](http://www.wikihow.com/Filter-Porn-Web-Sites-on-Your-Computer). You can also [restrict web browsing on Internet Explorer](http://www.wikihow.com/Restrict-Web-Browsing-Using-Internet-Explorer).

6) **Speed up your connection**. Use these tips to [maximizing your connection speed](http://www.wikihow.com/Maximize-the-Speed-of-Your-Internet-Connection) (or [speed up your wireless Comcast connection](http://www.wikihow.com/Make-Your-Wireless-Internet-Connection-Faster-%28Comcast%29), if applicable). You might also want to [test whether or not your internet service provider is limiting your bandwidth](http://www.wikihow.com/Test-for-Bandwidth-Limiting-by-Your-ISP).

7) **Find your computer’s address**. You can look up either your [IP address](http://www.wikihow.com/Find-out-Your-IP-Address) or your [MAC address](http://www.wikihow.com/Find-the-MAC-Address-of-Your-Computer) (which is built into your hardware).

8) [**Secure your wireless network**](http://www.wikihow.com/Secure-Your-Wireless-Home-Network). If your network has no password (or even a lousy one), it’s be vulnerable to being used by nearby computers and devices. If you bank, shop, or transmit any other sensitive information online, you run the risk of allowing it to be seen by strangers.

9) **Avoid compulsory registration and login**. [Use BugMeNot](http://www.wikihow.com/Avoid-Registration-in-a-Website-Using-BugMeNot) to bypass many sites that require registration.