Strategic IT Management Ltd

info@sitm.co.uk
www.sitm.co.uk
01453 840 451
01453 764 739

Phil Battrick, Managing Director of SITM offers a few pointers to help you (and your computer) stay safe online.

So, now you've got your lovely new PC, and a nice fast broadband connection, it's time to take your life in our hands (or at least that of your computer) get online, and see whether all the hype, half-truths, and scare-mongering are true. Will our PC really be destroyed within seconds of going on-line or receiving an email...?

At the extremities, there are 2 distinct views on the internet; it's the root of all evil and is responsible for most of the problems in the world, or, it's an incredibly powerful tool for democracy, and empowerment.

The reality is that if you think about the internet in terms of real life, there are some areas you probably don't want to visit at all, some where you'll need to keep your wits about you, and many where you can roam in complete safety...

The internet truly has something for everyone. No matter what your interests (illegal, immoral or otherwise) there will be websites, newsgroups, and discussion forums that cater for it.

The internet respects no boundaries, be they geographical, political, or religious. It's also impossible to "police" the internet, and calls from politicians or other public figures for the Government to ban certain sites are entirely pointless. To start with, when you connect to a website it could be sat on a server next door to you, but equally, it could be anywhere in the world. Hence the laws we observe here don't necessarily apply in the country where the web site is hosted.

So, is it really like the Wild West out there?

To a certain extent it is, in that there's almost no enforceable regulation, but that doesn't mean you can't be safe when you're out there. So here are a few rules to make your experience on the internet a safe and enjoyable one...

1. Get some decent antivirus software on your PC. This doesn't need to cost a fortune, and free software is available... AVG's free version is pretty good, and for one-off scans to make sure everything is OK, we're fans of Malwarebyte's product MBAM.
2. Don't believe everything you read. Even respected sites like Wikipedia come with a health warning, which is that the content is created by "ordinary" people, who may not actually know what they're talking about. You probably know people like this in real life; lack of information on a topic never stops them from expressing their opinion... Cross-reference several sources of information before accepting something is true. Even then exercise a healthy scepticism.
3. Ignore pop-ups telling you you've won a prize. You really haven't.
4. If something looks too good to be true, it will be too good to be true.
5. Never type your credit card number, password, or any other confidential information into a web site unless the address begins with https:// and your browser displays the closed padlock symbol next to the address bar. These indicate that the site is safe and that your data is encrypted.
6. Don't use file sharing sites that allow you to download the latest films, games, or music releases for free. First they're illegal, and second, they're usually completely riddled with viruses.

sitM
Strategic IT Management Ltd

info@sitm.co.uk
www.sitm.co.uk
01453 840 451
01453 764 739

Email is something else that's revolutionised the way we communicate with each other, but again, there are a few ground rules you should observe in order to prevent your PC from catching something nasty...

1. Microsoft will never email you updates
2. Your bank will never email you asking you to click on a link to update your security settings
3. There is no such thing as a lottery that works by selecting random email addresses
4. Never ever ever send your bank account details to anyone in an email
5. Email is not a secure means of communication so don't treat it as such
6. Ignore and delete emails claiming that for every person you forward the message to Microsoft or some other benevolent corporation will donate money to a worthy cause. They are fake. There is no way Microsoft or anyone else could track messages like this
7. If you're not sure about the legitimacy of an email always err on the side of caution
8. Don't click on links in emails unless you're certain about the source of the email
9. If in doubt, DON'T OPEN IT!!

Social networking is a relatively recent phenomenon, but one which is growing at an alarming rate. There are many sites, such as Facebook, Twitter, LinkedIn, MySpace, Bebo and many others, all of which can be great tools to keep you in touch with friends and family.

Many of these sites allow you to set up your profile, and put in information about yourself. This can be a great way for people to gather information about you for the purposes of identity theft. For example, if you put your date of birth into your Facebook account, unless you know how to alter your privacy settings, that information is available to anyone who logs into Facebook, not just the friends you've connected with. Be careful how much personal information you place on these sites.

If you want a single piece of advice to take with you whilst on the internet, let it be this:-

If something looks too good to be true, it will be too good to be true.