

Adept ITTM & Internet



Security Report 2010

© Copyright 2009 - 2010

In 2009 we undertook a complete and thorough audit of our security and back-up measures. The results were rather alarming and we would like to share them with you, along with our recommendations, so that you can review your own measures objectively to see how adequate or otherwise they are.

If you think there is room for improvement in either your security or back-up procedures, or both, we would be happy to supply you with a personalised, free, no-obligation recommendation and estimate.

Background Information | [Recommendations](#) |

In 2005 it became a criminal offence to “steal” unsecured WiFi ‘bandwidth’. This means that if you knowingly connect to someone’s open wireless network to browse the Internet and send email you could be charged and criminalised. There have been court cases over recent years where unscrupulous people have been found to have driven around residential and business areas with their laptop and gained access to open networks. One BBC report quotes a lawyer who states “It’s positively encouraged to have an open wireless network these days ... Most people use very standard default passwords so it’s very easy to use someone else’s WiFi.”

Having someone use your Internet account for free is bad enough, but once they find your network they potentially also have access to all your files on your computer: business contacts, financial records, bank statements, the list is endless. Even US President Barack Obama is reviewing America’s cyber security measures.

| [BBC Report: Barack Obama Cybersecurity Review](#) |

Crime on The Increase

On 1st September 2008 the BBC ran a report that the recession had already seen an increase in crime; the government expects it to worsen before the recession is over. | [BBC Report: Leaked Letter Predicts Crime Rise](#) |

As well as basic breaking and entering and the theft of equipment such as PCs, laptops and external devices such as USB flash drives, external hard drives, back-up discs, etc, it is likely that so-called “cybercrime” will increase dramatically as well, not to mention “insider attacks” by laid-off staff. | [BBC Report: Insider Attacks](#) |

Finally, one older version of WiFi security, ‘WEP’, has been compromised on a number of occasions and in London one man has been arrested and charged under the 2003 Communications Act for using someone else's WiFi network without permission. All new WiFi equipment now uses the more secure WPA security system.

The Security and Back-Up Audit

Having operated businesses in the IT and New Media industries for nearly thirteen years, we had presumed we had secured all of our networks and data as much as possible. However it soon became apparent that despite regular back-ups and a certain amount of security in place, we were leaving ourselves open for, at best, data theft or at worst the loss of the entire business in the event of a fire or flood.

Wireless Network (WiFi)

Our WiFi network is secured with an obscure password and has ‘MAC address filtering’ in place. This means that even if someone were to ‘hack’ in to the wireless network by cracking the network password, the router would not give them access to the Internet or network files due to their PC or laptop not being registered with the system by their MAC address. This address is specific to each individual network equipment such as routers, USB WiFi adapters (often built-in to new laptops), etc.

However, we did need to upgrade some of our equipment to ensure that all devices on the network were using the latest security protocols.

Data Security

Despite having a secure WiFi network, we soon realised that if someone were to steal our PCs or laptops, they would have access to sensitive business and financial information.

Although one of the laptops had a password in place, this can be ‘hacked’ and once bypassed the data itself was not protected.

Back-Ups & Disaster Recovery

Back-ups have been undertaken on a weekly and monthly basis, however, we realised once again that the back-ups were not secure – if someone were to steal the discs they would have easy access to important business and financial information.

Furthermore, all our back-ups were being held in one location and in the event of a fire or flood, our entire business would be at risk.

Recommendations

Wireless Network

Ensure that you have all levels of security in place and operating correctly. This includes the latest security protocols such as WPA encryption and MAC address filtering.

Data Security

All business, personal and financial data should be encrypted so that if your PC, laptop, external hard drive, USB flash drive or back-up discs are stolen no one can access the information. We recommend using encryption software to encrypt data to at least AES-256 (Advanced Encryption Standard).

This standard has been approved for use by America's federal departments and agencies to protect sensitive information and after the National Security Agency conducted a review and analysis of AES, the Committee on National Security Systems announced that the design and strength of AES-256 are sufficient to protect classified information up to the 'Top Secret' level.

This encryption can either be software-based or hardware-based, e.g. hardware-encrypted USB flash drives and external hard drives are now available at reasonable cost. Encryption can also be enhanced with biosecurity, for example fingerprint scanners are now commonplace on many new laptops and can be added to older laptops with an expansion card; there are also fingerprint USB flash drives available for easily transporting data securely.



Protect Your Family on The Internet

We recommend that children under the age of 18 are not permitted to use laptops or PCs in their bedrooms. Ensure that you have a workspace available in a communal area, even if it's just a dining room table or the sofa in the family lounge.

Make sure laptop or PC anti-virus and firewall software is up-to-date and has the family or child settings in place - secured with a password only you know. This will allow you to block undesirable websites and disable unwanted chat or messenger software.

Take an interest in your child's social life and make sure they know the person they're chatting to online in the "real world"; e.g. are they a school friend, family member, etc.

As in the real world, teach your child to be extra careful if they are contacted by complete strangers - public, open "chat rooms" should be avoided at all costs. It is much safer to use a secured MSN/Windows Live Messenger connection.

The only chat rooms that should be used are those that are "moderated" by a person who has been vetted by the organisation providing the service; for example, the BBC often have live "chat sessions" after popular television programmes so that viewers can talk to the presenters, actors or programme makers. The moderator ensures all messages follow certain guidelines laid down by the service provider, therefore allowing for an enjoyable and safe experience by the user.

If using so-called "social network" sites such as Facebook, bebo, twitter, MySpace and MSN/Windows Live Messenger - accounts should all have the highest security levels set.

This means that only the person's closest friends and family can see their details and contact them - and only after being given permission from that person.

This also applies to mobile phones - advise your child to be very careful who they give their number to.

Be aware of "cyber bullying" - does your child seem upset after receiving an email, text message or when using the laptop or PC? If you feel they are the victim of cyber bullying, let them know they are not alone:

*The Anti-Bullying Alliance recently found that **one in five** schoolchildren in the UK had been the victim of some form of online and mobile abuse.*

Even though those that use the web to target and bully others think that they can remain anonymous, this isn't the case. Even someone using a false name or email address can be traced and banned by social networks and email providers if they're found to be bullying others. DirectGov.

Have a look at the further information linked below - if you would like impartial, no-obligation advice, contact us using the link or telephone us on 0845 269 5087 or 07813 555 819 (if we are unavailable we aim to return your call within 24hrs).

Further information:

| [Wikipedia](#) | [UK Government](#) | [NSPCC](#) | [Contact Us](#) |

Don't Just Use Passwords

Passwords can be broken and no matter how complex or obscure you make them, it won't take long for a determined person to crack them. It is recommended that you use 'keyfiles' (a random mix of numbers and letters that can be hundreds of characters long); use the keyfiles in combination with passwords.

Once you have your keyfiles generated, you also need to secure them separately from the PC or laptop where the secure data is located. It is recommended you keep passwords and keyfiles on an encrypted or secured USB memory stick (flash drive), ideally secured via '[biometric](#)' methods e.g. fingerprints. Keep the USB flash drive with you at all times, (attached to your house or car key).

Consider Encrypting Your Entire PC or Laptop Hard Drive

By doing this you avoid the hassle of securing individual files or groups of files. Also, don't sell on or recycle PCs or laptops without first securely wiping the hard drive; data can be recovered from hard drives that have been 'formatted' in the normal manner.

Back-Ups and Disaster Recovery

Master discs for software and back-up CDs/DVDs should be held off-site, away from your main business or home – copies can be kept locally. In addition to this, it is recommended that back-ups are made to an external hard drive and the most important data uploaded to an online data storage service. We recommend the following:

- Daily back-ups to a secure external hard drive - you can then restore deleted or lost files
- Weekly back-ups to an off-site location - e.g. to an online storage service
- Monthly back-ups to CD or DVD - stored safely off-site

Security Mark All IT Hardware

We recommend, as a basic security marking option, permanent UV (Ultra Violet) marker pen. Invisible to the naked eye it 'glows' when under the correct UV light - all stolen-recovered property is checked for UV-marking when found by the police. Simply write your surname and postcode on laptops, portable hard drives, USB flash drives and all expensive items.

Products and Services

- * Encryption software starts at just £35.00.
- * Biometric USB flash drives start at just £18.00.
- * Secure External Hard Drives start at £65.00.
- * Online storage starts from **FREE**.
- * UV pen & light from only £7.00.
- * Basic security and back-up package: £165.00. This includes on-site set-up of one PC or laptop and basic training in the use of the encryption software and biometric USB flash drive (or hardware-encrypted USB flash drive).
- * Secure fire & flood proof data storage: from £12.00 per month. Store your back-up discs off-site in our specialised disc safe made from fire-proofed granite.

To arrange a **FREE**, no obligation security appraisal contact us on 0845 269 5087

Website: www.1adept-it.co.uk

Email: enquiries@1adept-it.co.uk

Tel: 0845 269 5087 * **Mobile:** 07813 555 819