Home Computer Policy

Published By

Secure IT Foundation / SecurityBrad.com

"It is possible to secure a computer to the highest standards, but the final level of security is determined by the user's behaviour. No standard can guarantee secure user behaviour."

Version: 1.0

Status: Final

Published: 24 October 2009

1. Introduction

The Secure IT Foundation publishes the Secure Computer Standard to help secure computers at home. However, there are two parts to a home computer, the home and the computer. We publish the Secure Computer Standard to help secure your new computer but who helps secures you and your home, in particular the people who will be using the computer within the home? Usually the answer is no one.

The Secure IT Foundation wants to help address the lack of consistent and reliable home computer security advice. Under the banner 'Level 5', we supplement the drive to get consistent computer security from manufacturers and suppliers with the Secure Computer Standard by publishing two additional documents.

The Risk Profile Questionnaire gives home computer users the means to identify what is important to them and what steps they need to help move towards the goal of risk free computing.

This Home Computer Policy is a set of rules to help home computer users use a computer safely. Without some basic security rules, even the most secure computer in the world will always be at risk from the weakest link in the security chain, namely you!

2. Legal Note

This document is written using best practice and knowledge available and improved using peer review and public scrutiny, however application of the Home Computer Policy does not guarantee data security and the Secure IT Foundation and its volunteers cannot be held legally or financially liable for any foreseen or unforeseen consequences for using the contents of this document in the production of a secure computer or a secure person.

It is provided for guidance only, for use as an aide to establish a security posture for your home computer. We cannot guarantee your ability to meet your own policy and advise you engage a security professional to assist you with the design and execution of your own home computer security plan if there is a risk of loss due to your usage of the home computer.

In short, we are legally liable for what you paid to use this document, nothing! If you were charged to complete this document, do let us know at secureitfoundation@gmail.com as it is a free service offered to the public and should not cost money to complete, other than consultancy fees to assist with completion.

3. Contents

4. Introduction

In the UK during 2008, 13% of corporate computer networks were compromised, nearly 10% suffered identity theft and 6% had confidential information stolen[1]. These are major corporations with combined security budgets of billions.

What is your budget for home computer security? Fifty for a well-known security package and perhaps thirty for a lock for a laptop. What chance do you have of securing your own computer if the professionals cannot get it right with almost unlimited money?

Very good actually! Corporations need to make computers accessible to the world, in the case of Internet web sites, and to have their own computers used by hundreds of staff. Your computer is for you and only those you give permission to use it. You have a level of control that is not usually possible in big companies.

With control comes responsibilities, as it is you who has to make sure your computer is used securely. You have the choice of what information you give to other people and who gets your money. If you do not see any problem with the world knowing everything about you, and can afford to lose your money, then rules are not for you. You need a different kind of help! As you are reading the Home Computer Policy, it can be assumed you do care about your information and your money.

The best set of security policies available to the corporate world has been written by the Information Security Forum. The ***Standard of Good Practice for Information Security*** is over 370 pages long and costs thousands to produce and maintain. However, it is useless for home computer security as it is written in technical business English. The Secure IT Foundation has taken its concepts, added in years of practical implementation of corporate security governance and distilled it into simple rules for the home computer user.

As the newly self-appointed security officer for your computer, you need a set of rules that you can follow and then enforce with those who you let use your computer. This is where the Home Computer Policy comes in. The Secure IT Foundation has written this set of rules so you do not have to be a security expert, to be an expert in computer security.

Before you go on and read the Policy, it is assumed that you have read the Secure Computer Standard, secured your computer to Level 4, and that you have completed the Risk Profile Questionnaire and taken all the actions recommended or employed a professional to implement the controls. Home computer security is the marriage of securing the computer with securing the user. Unless you do both, you are looking for a quick divorce!

[1] http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecdownloads/page9935.html
http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

4.1. Security is in the mind

Security is an odd concept. You cannot hold it or touch it but is controls and impacts your life daily. Cameras, monitoring and big brother like states all exist to achieve one aim, to control human behaviour. Do this, don't do that, warnings, penalties. All there to control your behaviour, for the benefit of society. Problem is there is little apparent benefit for you if you comply, apart from not being penalised.

In reality, governments usually do have good intentions and impose controls for your own benefit. Cameras do help solve crimes, monitoring of the Internet does stop terrorist actions and child abuse. Warnings are given because someone has ignored an obvious danger before, penalties so your inappropriate behaviour has a real impact in your life, where it hurts in your bank balance!

The reason why security is a good thing is poorly explained though. It gets lost in the sea of negativity with the focus on extra costs and not what it might help prevent, so it is perceived as a bad thing. As the rewards for security are always that bad events did not happen to you, you will only see the rewards if you can picture the impact of the bad event that did not happen.

So in terms of home computers, the bad events usually are the computer gets hacked, your information stolen and used to make criminals money at your expense. Possibly your secrets could be made public to the world. Think about the real consequences about these events, and this is your reward every time they do not occur. The Risk Profile Questionnaire helps you consider what may be a threat, only you can put a value on these threats, as it is about your life.

Security is in the mind, as only you can see the rewards for adopting a secure approach to home computing and only **you** can implement it.

4.2. Understand your computer

Your computer is just a collection of electronics that is a fundamentally simple as a light switch but more complex than the technology to put a man on the moon. There are two parts to your computer. The physical device you can hold in your hand, the hardware, and the things you can do with it, using the software. The hardware only knows 1's and 0's, as it is basically a very large line of light switches, which are on or off, shrunk into a tiny chip. The combination of lights on or off means something only to the software, which told it to turn on and off the light switches to do something.

Software is the commands, given in a code the hardware understands, that lets a computer know you are typing a letter or doing your tax return. It is written by humans so prone to errors. These errors are what lead to your computer being insecure. Fixes for the errors are given out all the time in the form of updates or patches which you need to apply. Occasionally there are errors with hardware which are corrected with software fixes to change how the hardware works, these are often called firmware updates.

A fast computer requires the latest hardware and software to be working efficiently and in harmony. A reliable computer requires hardware and software computer to repeatedly perform the same tasks over and over without errors or unexpected results. A secure computer requires the hardware and software to work securely but also for the user to use the computer securely. This combination of

human and computer makes home computer security more complex. However, a fast computer is one without viruses or hackers slowing it down and a reliable computer is one where the software does not start performing unexpectedly. A secure computer can be fast and reliable with a secure user. A secure computer will never be fast or reliable for long with an insecure user.

4.3. Understand the Internet

The Internet is a military creation, never forget that! It was designed by the US so that wars could be fought with computers directing the war, sending information from one place to another. If one part of the military network were destroyed then it would not stop the information getting to other locations. The benefits of connecting computers were easy to see, and soon adopted for education and commercialisation, creating what you now know as the Internet.

In reality, the Internet is collection of computers linked by wires and wireless signals, sharing a set of commands. In the centre are the computers, which are the means that allows you to type in www.google.com and your computer understand where to direct your request in computer language. Your Internet Service Provider (ISP) acts as your gateway to other ISPs and computer networks. So when you go to web page first your computer has to connect to your ISP who forward your request to see a web page onto many other people until the response is sent back to you and you see the web page. If you thought only you and Google know what you are searching, you are much mistaken. Your ISP will be able to see the request, like a post office can see your envelope but unlike the postal service the Internet postman can read the contents. Any other computer along the way until you get to Google's computers can also read your request including government and military, and they all can see the web page sent back by Google to you. Posting a letter is more private than using the Internet, do not assume what you do on the Internet is anonymous or secret EVER! No better tool has ever been created which can allow governments understand what people think and do. Power is control and the power lies with governments and the computer and telecommunications corporations. Google may aim to do no evil but what would you if they did? Sue them, use another large corporation who may be worse, stop using the Internet? All you can do is use the Internet securely, but never give your trust to it as one day it may not be there for you.

4.4. Language of computers

Sadly, computers were spawned from the use of applied mathematics and physics so were not initially designed to be used by the public. Over time access to computers grew to today's levels, however much of the skill in computers is still based on understanding the words and workings of a 1960's scientist. This 'geek speak' has only got worse over the years but security requires a level of understanding of this obscure language.

This is not the document to teach you computer speak so if you see a phrase or word you do not know then look it up on Wikipedia or Google! Just like visiting a foreign country, you will need to use a phrase book to help you get by, until you become fluent.

4.5. The world is a bad place!

If we lived in paradise then there would be no need for security. Good karma would rule, theft would be unknown and we could be proud of being whatever we want to be or do regardless of opinion.

History has shown this is not the case, and humans will kill, steal or take opportunities when presented, even if it is known to be a bad thing. You have secrets because you consider other people would view your actions in a negative light if you made them public, else they would not be secrets!

The golden rule of home computer security has nothing to do with computers. It is about **trust**. If a stranger comes to your home and asks you for your credit card details, as he wants to steal money from you, would you invite him in and hand over your card? Unlikely we think, but why not? The answer is you do not trust the stranger. Strangers are usually distrusted as part of human behaviour. You assessed the risk of the stranger and believe it to be high enough not to perform the actions requested. On the Internet you cannot see the person coming into your home so you cannot use your usually method of deciding to trust the person. Normal behaviour rules no longer apply.

4.6. Trust nothing

Your first step to a security mind is to start not trusting anything or anyone. Your new assumption when using the Internet has to be that you do not give out your trust to anyone or anything unless the trust can proved to you. If it cannot be proved to your satisfaction then you say no and even if it can, you should still think twice first! This goes against human instincts to give people the 'benefit of the doubt'. On the Internet there is no room for doubt or to hope it will all work out ok. No one will save you from your own actions.

If someone breaks into your home once, you will improve your home security and hope it will not happen again. If it does happen again, you improve your security until you are considered no longer a viable target for thieves. Once it is easier to break into the home next-door then thieves will typically take the easier option. On the Internet how do you when thieves have broken in to your computer? How do you know when to improve security to take action to fix a problem? The answer is only when it is too late. Only when you have a virus, or the computer stops working as you expect, or you are missing money. Be secure from the start and there will always be easier targets than your computer on the Internet.

The issue is there is no time for reaction with computers. Due to the speed they work, the time to break in to a computer or a virus to spread can be microseconds. A burglar will need at least a few minutes to open a door; a bicycle thief has to remove the bike lock. In the real world there is always time, that gives you a chance to react. On the Internet you do not have this luxury, so you have to adopt a hostile approach and trust nothing. This approach may be completely against your own personal beliefs and instincts, but on the Internet nobody knows you are a nice person who strokes cats and gives to charity. You are just another sheep waiting to be fleeced. Speaking softly and carrying a big stick only scares those within hitting range. On the Internet, scream out 'fuck off, go away' and there will be others to take your place in the line of victims. Normal rules of life do not apply here so don't be timid with security.

4.7. Don't be yourself

Lying in life is generally a bad thing, however on the Internet normal rules do not apply, so it is time for you to be an expert liar. When you meet someone new then do you give them your real name? Why do you do this? It is because your real identity may be known by the person in the future and if you want to continue friendship, then lying at the start is a bad thing to long-term relationships.

On the Internet there are only a few circumstances where lying or using a false identity is illegal, like entering into legally binding contracts e.g. bank transactions, buying goods, or where you are using the false identity to perform other illegal acts e.g. access teenage chat rooms for sexual gratification. Each country has its own rules but outside of these there is no reason to be yourself all the time. No one expects a person with the nickname 'romeoginger234' to be called that in real life, normal rules do not apply.

As you now trust nobody as your immediate response, why would you want to tell everybody your real name and personal information? Only trusted people get that information after proving themselves to you. You are not a sheep, so time to act like a wolf. Create yourself an Internet identity which has no relevance to your real information, a new web based email account goes a long way towards this, and make up a fictional character to be you. This fictional character is distrusting, paranoid and security minded who says no all the time and doesn't get intimidated. A giant on the Internet to be respected. The only limit is your imagination, so be bold. The advantage of having a new character is it stops you transferring your own weaknesses or insecurities in real life onto the Internet and helps separate the behaviour needed to act secure, if out of character for you. One day you will have to insert your government issued id card into the computer before using, until then don't be yourself.

4.8. Understand your enemies

Humans are simple creatures really, only seeking basic needs and wants like food and shelter. Capitalism has added the need for money and status over the years. If you cannot earn money and status by hard work then in today's society the answer for some, is just to steal it. It is easier to spend a few hours work on a computer to steal money than robbing people in person, and the Internet removes the need to meet the person being robbed in person. The Internet is open to anyone with access and treats all equally regardless of wealth, status, class or location. Is it a surprise that the Internet is full of bad people when it is making their lives so easy and profitable? The bigger the Internet becomes, the bigger the number of potential victims.

How does a criminal make money from you? Either you give away your personal information and banking details or they find a way to take it from you without permission. Your identity is worth money as it can be used to commit further crimes like obtaining credit in your name or other fraud. Your computer is worth money as it can be used to send spam emails or break into other computers, avoiding paying for electricity and internet connections as you provide it for them, and making you the fall guy if the hackers are traced back. Your information can be worth money if you have secrets stored on the computer and you get blackmailed. The number of scams on the Internet is increasing as the lack of security knowledge allows criminals to keep making money. By securing your computer and yourself then the number of potential victims goes down. By telling other people of the work of the Secure IT Foundation and this Policy, you can help reduce this number further. If there is no money to be made on the Internet then criminals have to find new ways of making money.

5. Home Computer Policy

Security is an 'all or nothing' process, either you are secure all the time or you are not. Not acting securely should only be done after considering the impact of your behaviour and deciding it is a low enough risk to take. It should be your choice to make, not the criminals.

The Home Computer Policy is divided into six key areas. Only by understanding and addressing all areas will you have a secure computer experience, as ignoring one element can be all that is required to enable your security to be compromised. A secure computer has defence in depth, layers of security measures and processes to protect you even if one defence fails.

- Hardware
  Covers the design and set up of your computer's hardware to ensure it is secure, fast and reliable.

- Software
  Covers the security of the operating system and your use of applications.

- Networking
  Covers the design and setup of your computer's network access to the Internet and to other computers.

- Security Management
  Covers the management of your home computer security.

- Computer Usage
  Covers your day-to-day usage of the home computer.

- Other computing devices
  Covers your usage of other computer devices like mobile phones, mp3 players, and gaming computers.

Each policy comprises of a list of rules with a reason why you need this rule, and the actions you need to take to meet the rule. Remember these rules are for your benefit, and ignoring them only makes you a bigger target for criminals.

Example:

Keep your teeth clean

Reason
Without cleaning, you will have bad breath, people will avoid you and you will be lonely and unemployed!

Action
Brush your teeth at least once a day

5.1. Hardware

This area of the policy covers the design and set up of your computer's hardware to ensure it is secure, fast and reliable.

5.1.1. Buy a computer that fit for purpose

Reason

While having the latest and greatest new computer is usually a waste of money, your computer needs to be fast enough to do everything you want. If you want to play the latest games or produce home movies you need more speed graphics capability and hard drive space than someone who just reads emails and views web pages.

If your computer feels slow now, perhaps it is time to replace it. If you want to change the use of the computer and start a hobby like video editing then do not expect it to be capable without new hardware. Computers do wear out and parts can need replacing in three years or less. A slow computer is a waste of your time and will cost more to maintain. Only keep using a slow computer if you have no money to buy a new computer or have plenty of available time not to care. Bear in mind a slow computer will take longer to maintain and likely to cost you more money if you engage a professional.

Action

- Plan for buying a new computer every three years. Bear in mind a fast computer built in 2007 will be fast for longer than a fast computer from 2005, as hardware has improved considerably in recent years.
- Set aside money to replace parts when it goes wrong or needs a service, just like a car.

5.1.2. Have more than one hard drive

Reason

Hard drives are mechanical devices and wear out. Do not expect your hard drive to last more than a couple of years in use. Just like a car, some are made badly in the factory and can fail immediately or in a few days or months. If the only place you have your data is on your computer hard drive then you are at risk of losing it all. By having more than one hard drive in your computer you can copy the data from one drive to another yourself, or you can have computer copy data automatically for you as part of the back up process.

With two or more hard drives and a compatible computer you can even use RAID technology to copy the data automatically all the time without you needing to take any action or notice any difference. Current technology allows the extra hard drive to be external to your computer and may be easier to implement yourself as you do not need to open the computer case.

Action

- Use multiple hard drives in RAID 1 or better, else have your computer backup regularly from one drive to another. Real time or daily backups are best, the longer time between backups means more information to recreate if you have a hard drive problem.

- Use an external hard drive to keep a copy of your computer's hard drive as part of your backup process. Store this separately to your computer when not making backups.

5.1.3. Handle your computer with care

Reason

Computers are full of delicate electronics and break surprisingly easily. Laptops are stronger than desktop computers but will break if dropped. Even if the case stays in once piece, your hard drive can be damaged especially if dropped when the computer is switched on. Remember your information is stored as 1's and 0's, not as you see it on screen, so any damage and it can stop working completely and may not be recoverable.

Action

- Always handle computers with care.

5.1.4. Shutdown, not pull the plug

Reason

If you do not shutdown your computer using the software commands, and pull the plug, you will damage your computer. Unlike a TV which can be switched off at the mains without damage, your computer is made of multiple parts than need to work in unison. It must be shutdown properly to avoid hard drive damage.

Action

- Always shutdown your computer using the command in the operating system.

5.1.5. Remove external devices properly

Reason

Always remove external devices, like hard drives, by using the software commands to remove. Due to the way computers work, not all your data may have been written to the external device if you just pull it out without using the commands in the operating system. You could be at risk of losing information if you do just yank the USB or Firewire plug out!

Action

- Always remove devices from your computer using the command in the operating system.

5.2. Software

This area of the policy covers the security of the operating system and your use of applications.

5.2.1. Harden your operating system

Reason

Your computer, as supplied by the manufacturer or retail shop, will give you an insecure computer. It will be a compromise of settings that allow it to work in the majority of situations for users. It will not be designed to be secure out the box and is a risk to your secure use of the computer. You need to have your computer secured to a security standard like the Secure IT Foundation's Secure Computer Standard to remove the risks you are given by the supplier. The process of changing settings to make a secure computer is called 'hardening'.

Action

- Have you computer hardened to a home computer security standard by a security professional.

5.2.2. Harden your software

Reason

The software on your computer, as supplied by the manufacturer or retail shop, will give you an insecure computer. It will be a compromise of settings that allow it to work in the majority of situations for users. It will not be designed to be secure out the box and is a risk to your secure use of the computer. You need to have your software secured in the same way you need your operating system hardened.

Action

- Have you software hardened to a home computer security standard by a security professional.

5.2.3. Download software at your own risk

Reason

Not all software available on the internet has been designed to do the job it advertises. Some has been written by criminals to pretend to do good things, like check your computer for viruses or spyware, and actually will steal your information or deny you access to information unless you pay extortion money. How do you know which is good and bad? In some cases, you don't! Only download software under the advice of a professional. Do not rely on your own judgement unless you are certain of the software provider. Your Anti Virus software only will protect you against known risks, a new virus spread by criminals will always be unknown for a period of time to your Anti Virus software. If in doubt, do not download it. Even having recommendations from friends does not make it safe, especially if they do not use a computer securely themselves. Do not give away your trust easily as you can never take it back on the Internet.

Action

- Only download software when advised by a security professional or you trust the source of the software.

- Never install new software just to make something work immediately or because a web site says you need to install it. Always confirm with a security professional first.

5.2.4. Update your software daily

Reason

Once you have software installed on your computer, it needs to be updated daily to protect you against new risks. Hundreds of new security issues are reported daily for software. Update everything on your computer including your operating system, browser, browser add-ons, office software, games, music applications etc . If it is installed, then at some point you may need to have it updated to prevent hackers getting access to your information or misusing your computer. If you do not know how to update your computer, have it maintained for you by a security professional. Software like Secunia PSI or Belarc Advisor can help you know what must be updated if used daily. Having personally worked with Secunia commercially for many years, it is easy to recommend Secunia as a company with good intentions. However applying security updates can be a complex process, and even with advice from Secunia or other scanning software vendors, do not expect to be able to fully patch your computer without the use of a security professional or expert knowledge.

Action

- Update your software daily or employ a security professional to update it for you.
- Only use known software scanners as recommended to you by the Secure IT Foundation to check your computer. Scam websites will offer you fake scanners and free checks and it is often hard to know what to trust.

5.3. Networking

Covers the design and setup of your computer's network access to the Internet and to other computers.

5.3.1. Use a hardware router

Reason

Even if you have a software firewall on your computer, it is costing you speed and performance when your computer is dealing with hackers. The best solution is to let a dedicated computer called a Router to perform the task of networking and security. Your Internet connection should be plugged into a router and your computer connected to the router by cable or wireless connection. The router has an inbuilt firewall which makes accessing your computer difficult from the Internet unless you allow it. Added benefits include sharing your Internet with multiple computers in the home handy when people have multiple devices that connect to the Internet like games computers, picture frames and music players.

Action

- Use a hardware router in the home to manage your Internet connection

5.3.2. Secure your router

Reason

Routers are good devices but they are controlled by software. This software itself needs updating regularly and its settings need changing from supplied defaults i.e. the router needs hardening. Due to number of devices available it is impossible to give advice that covers all devices. Typically you need to ensure that you set a strong password and that all open ports to the Internet are closed. The best advice is to employ a security professional to advise you on the purchase and settings for your router. The router is main defence from the Internet and has to be right else you will be at risk.

Action

- Harden your router settings and update it frequently. Employ a security professional if you are not certain of how to do this yourself.

5.3.3. Secure your wireless network

Reason

If you have wireless access available on your router then you are at much greater risk than if you only have wired connections for your computers. The issue is geography! You know where all your cables go and what is connected with wired networks. With wireless networks these allow people up to 1000m or more away use your network. Would you run a wire over 1000m to give a stranger Internet access? Unlikely we think, but this is the risk that wireless networks can allow. To secure your wireless network, settings need to be changed to use encryption to hide your information from anyone within range and to deny access to people you do allow to use your network. Set a strong password and use WPA2 (AES) strength encryption where possible. If you have devices that cannot

work with the highest level of encryption then use two routers to separate the secure computers from the insecure computers.

Action

- Secure your wireless configuration by using a strong password and the highest level of encryption available.
- Use two routers to separate secure and insecure computers.

5.3.4. Be extra careful when not using your home network

Reason

When you use a wireless public Internet connection, or a wireless USB Modem, often called a dongle, you are at risk. You are no longer protected by your router, and are dependent on your computer's software firewall to prevent unauthorised access by hackers. Even with a firewall in use, information you send and receive on the Internet like web pages, emails or social networking can be read by anyone with access to the network you are using, unless it is secured by encryption. The risk is highest with public wireless connections where the person next to you could be reading everything you do on the Internet. Do not trust networks to be totally private, and be especially careful with your use of the Internet away from your network. Unless you are certain what you are doing is secure on a public connection, do not use it and wait until you are home. Consult a security professional to advise you on the best way to use public networks securely, especially if you travel with personal or financial information stored on your computer.

Action

- Do not trust public networks on wired or wireless connections. If you are unsure of using your computer securely on a public network, do not use it.
- Consult a security professional if you travel with a laptop and carry personal or financial information on the laptop. If possible do not travel with personal information that is private or cannot be replaced. What is not there, cannot be lost or stolen. If you must travel with information then ensure you use strong encryption on the whole drive with pre boot authentication.

5.4. Security Management

Covers the management of your home computer security.

5.4.1. Manager your users

Reason

If you let other people use your computer then there is a risk that your personal and financial information could be accessed by the other users, intentionally or accidently. Ensure all other people who use your computer has their own user account, and their account is only given the standard user rights, never administrative rights. Avoid the use of built in guest accounts as these should be disabled as part of hardening.

Be aware that the files on the computer will be segregated but any removable media you use with the computer will be visible to other users. Never install software to see 'something cool' or turn off security measures at the request of the user. You control your computer and can say no!

Action

- Ensure all people with access to the computer has their own account and password
- Only create standard not administrative accounts for additional users
- Be prepared to refuse a request to install software

5.4.2. Check your security

Reason

Just because you have hardened your computer, update it frequently and take the utmost care on the Internet does not guarantee your security. You have minimised the risk of bad things happening but do not assume you are completely safe. New ways to break into computers are discovered every day, changes can be made by accident to lower security like turning off firewalls or Anti Virus software, so you need to check your security on a regular basis or employ a security professional to check for you. Simple port scan checks will let you know if your router is working correctly. Nmap online is an example of this type of security check.

Action

- Check your home computer and network security on a regular basis or have your security checked by a security professional on a regular basis.

5.4.3. Plan for the worst case

Reason

If you plan for the worst-case scenarios in life, like having your computer stolen or accidently damaged, then you will be able to cope if it were to happen. Imagine having all your photos and videos stored on one computer, and then it is stolen. In the case of a laptop, just dropping it can destroy it. Unless you have a second external hard drive with a backup or copy of the information in another form, it will be lost for good. Even a simple file corruption can make your computer

unusable. It can take up to 48 hours to rebuild software on a computer, even longer if encrypted, but as little as two hours to restore with a full backup from the day before. To be even more secure, make a copy of all your information on an encrypted disk and give it to a trusted friend to hold, in case all computers , hard drives and removable media are taken by a burglar. Remember to update the disk on a regular basis but having a spare copy of all your information for previous years is better than no information at all. Also think about how you would access telephone numbers of your ISP or security professional if your computer is stolen or damaged.

Action

- Always make regular backups of information you cannot afford to lose, consider paper copies if only available on the Internet.
- Make a second copy on an encrypted disk and give to a trusted friend or security professional to store on your behalf. Update the information stored at least once a year.
- Complete the Risk Profile Questionnaire on a regular basis to check that your risk profile has not changed, or if it does change then amend your security management accordingly.

5.4.4. Help make other people secure

Reason

Once you have got the security bug, tell the people who use your computer how to use the computer securely. Point them to the Secure IT Foundation web site and help spread the word of having a secure home computer. The greater the number of people who are security minded when they use the Internet means less potential targets for criminals, which in turn can make scams and hacking less profitable than other non Internet based crimes. Sharing the responsibilities of managing the computer security with children will help make it second nature to the next generation of computer users. No one else will teach them security until they are in employment, which is too late. Learning security is like learning a foreign language, and best done early.

Action

- Inform every person who uses your computer, that you are in charge of security.
- If a user wants to be allowed to use an administrative account, then ensure they demonstrate to you an understanding of the Home Computer Policy and can accept the responsibility that comes with it.

5.4.5. Consider your home's physical security

Reason

A secured computer will be a wasted effort if it is easy for burglars or thieves to take it. Do check your home's window and door locks, fencing, lighting and alarms on a regular basis. Do not ever leave your computer in a public or shared work place unless you can touch it. Even positioning your home computer in a publicly viewable window can make it attractive to thieves, or make your Internet usage viewable from outside your house.

If you must leave it unattended, lock the computer to a fixed object with a security lock, use the screensaver and account locking options available to you and be quick. Thieves can cut a laptop cable lock in under five seconds, older cables could be opened with toilet roll!

Action

- Never leave your computer in public display
- Never leave a laptop without a lock, and only for as short a period of time as possible.
- Be aware who can see you enter passwords or PIN numbers.

5.4.6. Ensure you comply with the law

Reason

You can make a lot friends by giving others access to your Internet connection or your computer but bear in mind you are legally liable for their actions. Unless you are able to prove it was not your behaviour that was illegal e.g. due to a virus or hacker, then all illegal acts will be assumed to have been you! Even if you prove your innocence to police or a court, you will have your computer, hard drives and removable media seized for up to several years before it is returned. It may not be returned working, or in some case may have secret monitoring software installed to check if you repeat the illegal behaviour. In short, allowing others to do illegal acts is bad thing, not just from the potential penalties but also from the unexpected consequences like losing access to your computer without warning.

Action

- Ensure all users of your computer and network comply with the law.
- Be prepared to ban or disconnect users who do break the law using your network or computer

5.4.7. Consider a UPS system

Reason

An uninterruptable power supply (UPS) will give you time to save your work if you lose power at home. It is not much more than a battery with 5-30 minutes of emergency power for your computer but without it your computer will shutdown like you had pulled the plug out and you risk hard drive damage and information loss.

Action

- Consider using a UPS if affordable

5.5. Computer Usage

Covers your day-to-day usage of the home computer.

5.5.1. Keep changes to a minimum

Reason

Outside of security patching and updating to existing software, keep the number of changes you make your computer to the minimum. The quickest way to make a computer stop working is to install and remove additional software to try something out or make something work. If you don't know what you are doing, allow a security professional to manage your computer, who can also advise you on software choices. A reliable computer is one that has a fixed set of uses and never changes unless necessary.

Action

- Only install software you need.
- Consult a security professional if you are uncertain if software changes are really needed and to advise you on new uses for your computer before you change your computer.
- If you must try additional software, make use of virtual machines to avoid making changes to your own computer directly.

5.5.2. Keep passwords secret

Reason

The information needed to access your computer is a password. This is your password and only you should know it. Just like bank PIN numbers and security details, never tell anyone your password unless it is the only way for a trusted security professional to manage your computer. Even then, your security professional should use their own administrative account and password, so if you give out your password you should still change your password as soon as possible afterwards. The only exception of when keeping a paper copy is ok, is when it is kept in a secure location like a safe just in case you were threatened to reveal your passwords. Much better to change your passwords than need time in hospital. Also think of what about if you were to die? Would all your information be lost forever?

Action

- Keep passwords secret
- Never write them down or say them out loud.
- Be aware who can see you enter passwords or PIN numbers. If you suspect you are being watched, wait for the person to go, or move location yourself! Don't forget cameras can have a longer range than your eyesight.

5.5.3. Be careful with social networking

Reason

Before the Internet, if you wanted your friends to see an embarrassing picture of your antics you had to take it to them in person or post them a copy in the mail. You had some control who saw your photos and videos. Social networking is just a new way of doing existing things like having friends and sharing information. The problem is that the number of people who can see your antics is now in the millions and sharing can be done instantly. That picture could be on the Internet permanently as everyone can make their own copies without you knowing. Having friends is good but remember your security mind and only let the world see what you want them to see. If you are in doubt, don't share that picture or video with the world!

If you publish, blog, text or diarise your life on the Internet in any way, ensure that you do not use real personal information and never give out your home location or address. You may not see a problem, but advertising you or your children will be in a certain location would make it easier to target by predators or criminals. Don't give away your own travelling habits in case you inadvertently tell the world when your home is empty. Burglars do use the Internet as well, and love easy targets.

Action

- Used closed social groups if you must share potentially embarrassing pictures or videos online.
- If you have any doubts as to your profile security, have a security professional check your settings. 10 minutes work could save your reputation for the rest of your life.

5.5.4. Remember not everyone is honest on the Internet

Reason

Like social networking, using instant messenger, chat or telephony software has its own risks. Have you ever had a suspicious scam call on your telephone? Well the same people also operate on instant messaging, chat rooms and Internet telephones. In keeping with don't be yourself, use your fictional character not real information for talking to people. Either they know you in person and know your real identity or they do not. On the Internet it makes little difference, unless you are using the fictional character to deceive people for illegal acts. Never use any real piece of information and you will be hard to track for stalkers and other undesirables found on the Internet. If someone does not know your real name, then they should not have your trust.

Action

- Never use or give out your personal information on public chat rooms, instant messaging or Internet telephone services.
- Restrict access to known friends only and be suspicious of new 'friends'. Anything that sounds too good to be true usually is a scam, don't lose your money to stupidity!

5.6. Other Computing Devices

Covers your usage of other computer devices like mobile phones, mp3 players, cameras, videos and gaming computers.

5.6.1. Consider every device as a computer

Reason

Modern electronics has become so complex that virtual every device in your home will have a computer built into it just to manage and use the device. Games machines, smart phones and music players all are obviously computers underneath but what about your TV, set top box or hi-fi? If it can get Internet access, it is a computer and must be secured as well.

Action

- Check all your devices, that have Internet access, have been set up with secure settings e.g. Wireless network security settings.

5.6.2. Use computer devices securely

Reason

Anything that has Internet access is at risk unless it has a basic level of security built in or added by its settings. Any device that is capable of holding your personal or financial information is a risk as it can be lost or stolen. You may have all your pictures secured on an encrypted hard drive, but what the pictures still on the camera or memory card? Those video tapes of times you do not want to share with the world. Anywhere you store personal information insecurely, you should aim to secure it as soon as possible.

Action

- Always remove personal information from computer devices and place into secure storage on an encrypted hard drive, as soon as possible.