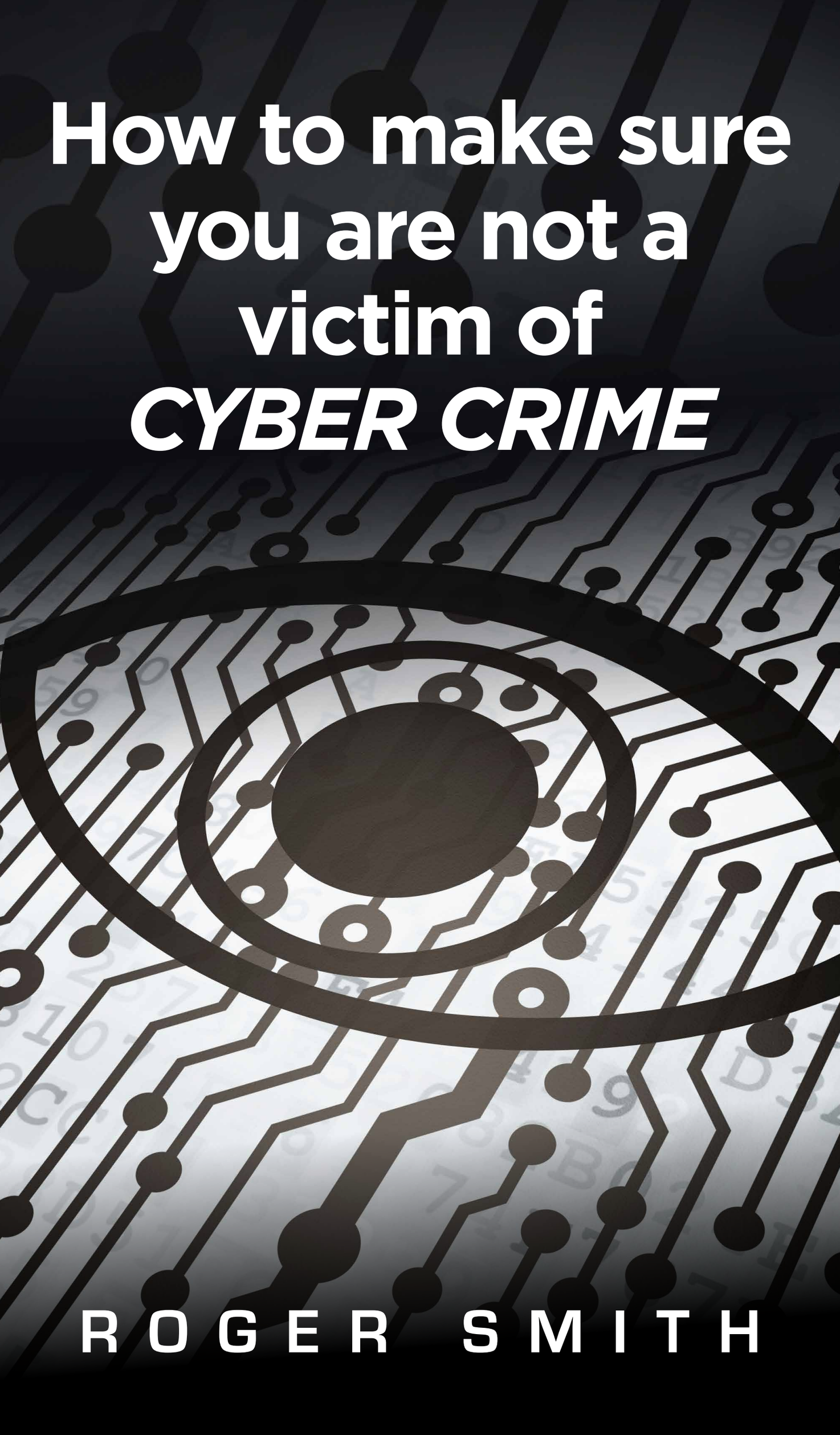
How to make sure you are not a victim of *CYBER CRIME*



ROGER SMITH

Manager and Owner
R & I ICT Consulting Services Pty Ltd

The abbreviated content in this document is taken in part from the book “The CEO’s Guide to Cyber Security” and “The CEO’s Guide to the “Cloud””.

R & I ICT Consulting Services (The SME Security Framework)
PO Box 368
Kippax ACT 2615
AUSTRALIA

Connect At
Email: Security@rniconsulting.com.au

Downloads at: www.rniconsulting.com.au and www.smesecurityframework.com.au

www.au.linkedin.com/in/smesecurity
www.twitter.com/smesecurity

Design
Leanne Chow www.leannechow.com.au

Note: The information in this guide is of a general nature only. When making decisions regarding your own business it is strongly recommended that you seek qualified advice tailored to your own particular needs and business situation.

Front cover: istockphoto.com

How to Make Sure you are not a Victim of Cyber Crime

Is this eBook right for me?

Not quite sure if this eBook is right for you? See the below descriptions to determine if your level matches the content you are about to read.

Introductory (this book)

The Introductory level content is for people who are new to the subject. It provides information on the fundamentals of personal Cyber Security and includes step-by-step instructions on how to start protecting yourself. After reading it, you will be able to execute basic Cyber Security tactics.

Intermediate

Intermediate level content is for people who are familiar with the subject but have only basic experience in executing strategies and tactics. This content covers the fundamentals and moves on to reveal more complex functions and examples. After reading it, you will feel comfortable leading projects related to Cyber Security.

Advanced

Advanced level content is for people who are, or want to be, experts on the subject. In it, we walk you through advanced features of this aspect of Cyber Security and help you develop complete mastery of the subject. After reading it, you will feel ready not only to execute strategies and tactics, but also to teach others how to be successful.

Foreword

Roger Smith is an independent Information, Communication and Technology (ICT) and business security consultant, security trainer, and author who specialises in inexpensive and highly effective security strategies for small and medium businesses and not for profit organisations.

He has developed and authored the SME Security Framework and the Security Policy Training Course, which are considered to be the definitive guides to helping SMEs protect their organisations using the principles of Technology, Management, Adaptability and Compliance. He has also written a chapter for the new “Security 3” book that has been published on Amazon.

This vast experience has given Roger a broad knowledge of hundreds of ICT and Security tactics used by some of the most successful and well-protected organisations in the world.

A special Thanks to Kathleen Charles

Kathleen Charles has been writing and editing promotional materials for various businesses for several years. Her extensive experience in sales and marketing allow her to assist businesses in meeting their communication goals by harnessing the power of the written word. She also writes creatively and is currently training to be a children’s yoga instructor. Kathleen holds a Bachelor of Arts from the University of Colorado, and enjoys creating healthy, delicious food for family and friends as well as any form of fitness. Currently, Kathleen and her family reside in Brisbane and they all enjoy exploring and learning about their local area.

Contents

Introduction

Cybercrime is quickly becoming one of the more common forms of crime people experience. Once thought of as a victimless crime, cybercrime has proven it takes very real victims indeed. It is no longer possible for people to just bury their heads in the sand and say, “It won’t happen to me.”

I believe the old adage about fishing is apt when considering Cyber Security. “Give a man a fish and you feed him for the day; teach him to fish and you feed him for life.” You can invest money, time and energy in technology, buy better firewalls, track what everyone is doing, but what happens when the technology changes? If you adopt the attitude that protecting yourself on the internet is your own responsibility, no matter happens with technology, you will always be protected.

Today, a 12-year-old with some computer knowledge and an internet connection can download applications that can turn him/her into a novice cybercriminal. At a more advanced level, criminal organisations that control cybercrime offer guarantees, and engage in price wars and under cutting with aspirations of creating the largest crime organisation on the internet.

They use sophisticated command and control systems; they write malicious code that exploits vulnerabilities in everything from IOS on iPhones to high end server platforms written in Linux and Unix for the cloud. They target everything and everyone that is connected to the internet.

So don’t think it can’t happen to you. If you have anything that connects to the internet, you are a target. You are vulnerable and, most importantly, you may already have been hacked even without realising it. With regard to the internet, we are naïve and we trust too easily. For some reason, the internet has removed a lot of our inhibitions. This trust is what cybercriminals exploit to the best of their abilities.

Conduct an internet search for a celebrity blunder, a copy of the newest hit song release or the newest popular movie, and somewhere on the results page there will be a link to a site that is infected with malicious code. That website is written purely to attract you and people like you. It is designed to infect your computer or mobile device with malicious code. Cybercriminals create web sites designed solely to attract users so they can then steal their money and identities.

Although all of the search engine companies have some type of vetting process, there will always be links that are new, have somehow slipped through, or the malicious code is unique and undetectable. The problem is that even sites like MSN and The Australian have been infected. The tell-tale sign is usually the request to install some type of Java or Adobe patch from these sites. Always read the warning.

Use the internet at your peril! However, if used correctly and with a high level of paranoia and common sense, then we may all just survive this decade with our money in the bank and our identities intact.

I class the internet as the most dangerous place on the planet. Using cyber space is like walking down the darkest and meanest alley in your town, with your hands and feet shackled, wearing a blindfold, with your money and identity in your back pocket and a big flashing neon sign saying “Rob Me”.

Fortunately, the problems can be easily rectified. For one, technology is one of the problems, so do not rely on technology alone to protect you. Front facing internet security devices do have a place in Cyber Security, but more importantly, you must learn to understand what the criminals are doing and how YOU can protect yourself. If you protect yourself, then everything else you do on the internet will be manageable and you will be able to see the dangers and take appropriate action.

The Mobile Environment

Everyone I know has a smart this or a mobile that. This is the way that technology is leading us. Everyone wants to be connected to the internet, their friends and family, work and their social media lives, but with that desire for connections comes the need for responsibility, added protection and the use of caution.

The business world is starting to understand the importance of constant connection. Mobile devices are the new face of marketing and advertising. With cutting edge content so readily available, and search engine optimisation (SEO) used by marketers, everyone is after your attention. Small businesses can now compete with global organisations using the same marketing techniques and by using the internet environment even more effectively.

Cybercriminals can reach us this way as well. They are after us in ways that we could only dream about five years ago. They target the ill-informed, the innocent and the uneducated to make sure they have constant revenue for their criminal coffers.

The way to protect yourself is to make sure that you are not ill-informed, that you are better educated and that you are less naive than people who regularly lose their identities on the internet.

The Basics of Cyber Crime

To most of us, cybercrime is something we read about in a newspaper or online. We often feel that what we hear is of little consequence to us in the real world. Unfortunately, that has all changed in the last few years. Today's cybercriminals are getting smarter; the tools they employ are less obvious, and the payday they receive when they are successful is much higher. We should all to learn how to protect ourselves from cybercrime.

Crime has been around for years and so has crime fighting. In previous years, crime was most often one on one, such as a mugging in the street or the pick pocketing of a purse or wallet. With the introduction of banks, trains and stage coaches, crime evolved to be often one against many.

With the advent of the internet, it is now possible for one person to steal from millions of people at one time. This happened recently with Sony in 2011 and Adobe in 2013, and will continue to happen until we learn the basics of how to protect ourselves. In both of those cases the theft of millions of users' information, including credit card details, was stolen from both companies. In the case of Adobe, the criminals even stole the source code, Adobe's IP (Intellectual Property), which gave the criminals another attack vector.

Currently, most of the western world is moving everything to the internet. We use the internet to relay messages and letters; we play games; we use it to bank and pay our bills. The increased use of the internet means that most businesses and organisations are now utilising it in more ways.

This has prompted the phenomenon called cloud computing. Cloud-based computing and systems are cheaper to use and they give the user a better experience. All of the social media sites are cloud-based systems. It used to be called diversified computing; now it is just called the "Cloud". Cloud-based systems are becoming more and more prevalent in the business world. An example is the use of CRM (Customer Relationship Management) systems by business to track their clients.

However we look at it, the internet has become an essential part of both our work and home lives. Most parents with young people in the family have probably heard, "I cannot live without my—***insert technology here*** -," and they often feel the same way! We all know how important our connection to the virtual world can be.

The problem is that criminals have realised that as well. Many people now keep 50—90% of their personal information stored using some form of electronic data. Buying habits, email, banking and other personal information are all now available electronically.

Cybercriminals, just like mainstream criminals, aim at the easiest targets to translate into easy rewards. They also target the ill-informed. For example, many mac users believe they cannot be infected, but the truth is, they can. And it is the user, not the firewall that will be the target, because the user is easier to get around.

They also use semi-legitimate processes in very illegitimate ways. They corrupt your email using phishing and spear phishing attacks and they corrupt your favourite web sites with malware and spyware. If you use peer to peer systems to access perceived free music, films, games and applications, they corrupt the information that is available with Remote Access Trojans (RAT's), viruses and worms. Unfortunately, in most cases, if something on the internet is promoted as "free", it is illegal in some way. This is not an absolute, but is true the majority of the time.

The internet has made criminals harder to find. They cross international boundaries with impunity and they steal anything that they can get their indiscriminate little hands on. Cybercriminals are the twenty-first century version of a biblical plague.

Now, that's the bad guys; the good guys, on the other hand, are constantly playing catch up. They are restricted by laws and boundaries. Frequently, criminals have developed technology well before law enforcement, the business world and mainstream users have seen its potential. The most obvious example of this was android and the app market. This was infiltrated, compromised and infected from day one. In this landscape where it is difficult to rely on law enforcement, it makes sense to educate ourselves, so we can protect ourselves.

The Basics of Cyber Security

Cyber Security is the actual process used to protect electronic information and data.

The most important information for criminals to obtain is related to the victim's identity, because that information opens up several doors for them. It is important to decide early on what information is important to keep private and protected and what information is not. Basic address information is an important component of personal identity, as are tax file or social security numbers, email accounts and passwords, and banking and credit union accounts and passwords. The latter are particularly important, because they not only form part of your identity, but also detail where you keep your money. Protection involves separating your "real" life from your electronic life.

It can be relatively easy for some people to gauge other people when they meet face to face in a social or business environment. In those real life situations, you use your five senses (well, maybe not taste!):

- Sight—what do they look like and what is their demeanour?
- Smell—do they have an odour?
- Touch—how do they shake your hand?
- Hearing—what do they sound like?

All of these combine to form your initial level of trust and involvement with the person you met.

In the virtual world, we are unable to use our basic senses in this way. You can only base your first impression and the level of trust you feel based on what you see and sometimes hear on your computer or mobile device. Sadly, it is quite easy for some people to create fictional online persona and provide untruths when it comes to who they are and their background and/or qualifications. This is how criminals gain trust and subsequently, personal identifying information from their victims.

In this mini guide we will focus on three components related to keeping personal information secure:

Technology: Everything you do on the Internet involves some level of technology. That includes mobile phones, tablets and computers as well as operating systems and applications. The technology component also includes audio-visual (AV).

Common sense: Your common sense will keep you safe. If it appears too good to be true, then it probably is.

Paranoia: A healthy dose of paranoia is required when you are dealing with the internet. Many people are out there to take advantage, so it is acceptable to be worried about it.

If you combine your use of technology with common sense and some healthy paranoia, your personal information will be secure and much more difficult for criminals to access.

Cyber Security is an ongoing process. With every change you make to your personal information and/or your technology, your security needs to be re-evaluated. Not necessarily changed, but definitely checked.

The bad guys will initially attempt to come through the front door, so to speak. They will check to see if it is locked and then if that lock is secure by rattling it and pushing against it. The moment it becomes too difficult they will invariably go elsewhere. The cybercriminal is after the low hanging fruit, the easiest system to access, or the laziest target.

However, that said, be careful to not only securely lock your front door, but also ensure you have not inadvertently left the back window open. The bad guys are not geniuses, but they have systems and processes that make it appear that way.

Remember that you personally are not a target. The primary target of cybercrime is your device. Once they have infiltrated that, then whatever information they are able to hack is the icing on the cake. 80% of all compromised systems have been compromised by an automated system, virus, worm or Trojan, or through some combination of those. By defeating the mindless automaton, your level of protection will be a lot greater. By ensuring the criminals do not gain a beach head on your device, you are defeating their first line of attack. If you secure access to your systems, then the bad guys will move on to someone less protected.

So, what will make the bad guys attack someone else? Let's find out!

The Top 10 Things You Can Do to Protect Yourself

For the purposes of this mini guide, we have looked at ways to protect your online security and come up with what we believe are the 10 best. This is not the be all and end all of your requirements, but it is a good place to start.

1. Create Safe Passwords

We are beginning to hear that the use of passwords will be replaced with new technology, and I, for one will be the first to embrace it. Until that time we are left with the need to create and manage a vast array of passwords for the internet and work.

Passwords can feel like the bane of our existence! It seems that everywhere you go on the internet, you have to create a username and password.

No matter what your password is used for, it must have three essential components:

- It must be complicated (i.e. no more “1111” or “password”).
- It needs to be more than seven characters.
- Probably most importantly, it has to be easy to remember.

Feeling daunted, yet? Don’t.

Fortunately, there are easy ways to create a complicated password. We have developed three ways to create a complicated, easy to manage password.

METHOD ONE

Use regular words in the following format:

Find two common things that you use regularly and are easy to remember, such as cup, watch, time, desk, chair. Then use a number or symbol to separate them. So Cup and Time could be Cup#time, Time34Cup, #CupTime. The combinations are numerous and difficult to crack.

METHOD TWO

Use a phrase related to something you encounter often, and then use the beginning letters in each word of the phrase to create a montage of letters.

For example, take the phrase “I play golf every Saturday at the club,” and use the first letters of each of those words. You now have: “ipgesatc.” Now make it complicated by inserting numbers or symbols you can easily remember: Ipg3s@tC. When you use this method, you can write down the initial phrase anywhere and no one would understand what it refers to.

METHOD THREE

Use an actual complete phrase; any phrase will do. For instance, “I hate passwords.” Keep the spaces because password crackers hate spaces. And add a couple of extra symbols or numbers. An example: “I h@te P@ssw0rds!” Even include the quotation marks. This would now be a very secure password. It is easy to remember and again, you can write down the initial phrase and no one would know what it is for.

In addition, to make it easier to remember the purpose for that password, use a generic phrase followed by the website that the password will be used on (“I h@te P@ssw0rds!”amazon). Again, these passwords are easy to remember, but very hard for criminals to crack.

2. Make Each Password Unique

Now that you have a secure password, the next step needs to be to make sure it is unique. The easiest way we recommend to do this is to add part of the name of the website, or the purpose for that password, to the password itself. Refer to Method Three above to see an example of this.

The reason for creating a unique password for each website or purpose is quite scary. Cybercriminals use a process called “roll up”. In this process, when they discover your username and password on a website, they try the same combination of username, email address and password on other sites. They do not carry this out themselves; they use scripts and processes to test thousands of sites in seconds. This process then copies all hits to a log file that they go through later.

What happens next is frightening. Here is a hypothetical:

If you have a weak password on your internet mail account (for example Google, live or yahoo) and someone cracks it, they now have access to your email. The first thing they do is change your password and I can guarantee that they will change it to something complicated and difficult to crack. They now own your email account and to get it back will take a vast investment in time and resources. In most cases it is too late to salvage the account by the time you gain control again.

They go through your email looking for information on other accounts you may have, such as bank accounts, PayPal accounts, work accounts, social media accounts, etc. They then go to those websites and use your email address to receive a "forgotten password" for each site. They are now able to reset your passwords on these sites as well. The amount of damage they can do depends on the amount of information they gain from your deleted, sent and saved emails.

They now have access to your information and in some cases access to your electronic persona. This is bad. Many websites require you to fill in some highly sensitive information, including your Tax file/social security number, date of birth, address and sometimes previous addresses. Cybercriminals can use this information to begin to build a profile of their victims.

"Social log on" is the newest trend in single sign on processes initiated to bring about more convenience. It allows you to use your social media website log on information to log onto the new site. There are two problems with using social log on:

1. You no longer use individual logins for different websites, which makes your login less secure.
2. Cybercriminals can put a website up that requires you to log in with your social log on. Once you do, they log all of that information. They now have access to your social media site, and can post to it on your behalf.

3. Change Default Passwords

Most, if not all hardware devices have an initial password, or default password, to access the device. This is designed so that when you first receive the device you can set it up to your requirements. This includes the modem/router that you purchase for your home internet connection. Most devices are configured through a web-based interface, or web page.

Every manufacturer has this sort of management feature. Some will ask you to change the password the first time you log on; others will not. The problem exists with the ones that do not ask.

Default passwords should be changed. It is not too difficult for an older child in the home to figure out how to change your router/firewall configuration to allow their own systems to have access to peer to peer or inappropriate content. Changing the default password to a secure password restricts access to that internet-based device and makes your home internet connection more secure.

4. Install Reliable Anti-Virus Systems on All of Your Devices

Protecting your password and making it unique is a waste of time and money if your computer has been compromised with a Virus, Worm, Trojan, malware or spyware (malicious code). A virus, worm or Trojan has two roles. First, it aims to destroy the system that it has installed itself on, either immediately or after waiting in the background for a specific trigger.

Secondly, it is designed to copy all key strokes and mouse moves to a file, which is then uploaded to its command and control centre. In addition to these two roles, in order to replicate itself, it copies itself across networks and over the internet looking for new targets.

Most malicious codes have a number of payloads, or tasks they are programmed to complete. This combination is designed to confuse and manipulate the user. For instance, a virus may be designed to have two payloads: one could be to cause problems for a computer by hiding all of the information. This type of virus can be easily removed by a professional.

However, the second payload could be to lie seemingly dormant and ineffective, while recording everything that happens on the computer. This is one of the reasons that we, as an IT company, always recommend that if and when you detect some sort of malicious code, the computer be rebuilt from scratch. Although that tends to be more expensive, the recommendation is made to protect our clients.

Anti-virus products are designed to protect personal computers, mobile phones and tablets from malicious code being run on them. These systems can be purchased, or can even be found for free. As with most products, you get what you pay for, but overall, there are a number of effective free anti-virus products out there.

No matter what system you are using, all operating systems and applications can be struck down by malicious code. Cybercriminals will always go after the biggest bang for their buck, which is why they target the most used applications and the most popular operating systems on the market.

The newest problem is “ransom ware.” This is the process where a business compromises your computer either through a spear phishing attack or a compromised website. The business then makes a ransom demand, something like: “We will remove this software as long as you pay $69 to our account.” When this happens you have two choices: you can pay the requested amount not knowing if you will get your information back, or you will need to rebuild your computer from scratch. Either way is expensive. Thankfully, most anti-virus systems will catch ransom ware.

5. Purchase the Newest Applications and Operating Systems

Whenever a new operating system is released, it is accompanied by great fan fair and mass advertising. Most of the features of new operating systems are touted as being easier to use and more secure. These claims are often actually true. The newer operating systems are typically designed based on lessons learned from previous versions. Thus, the newest incarnation of an operating system will always be more secure than the last. This is also true of free operating systems such as Linux.

In the case of applications this is also true. Applications are not normally advertised as much as newer features on operating systems, but newer applications are also typically safer and easier to use.

The newer the operating systems or the applications, the more secure the system is. This is why we recommend that if possible and not too expensive, people should purchase the newest versions of operating systems and applications.

Additionally, the number of free applications commonly available on the internet (e.g. java, flash and acrobat), should also be the newest and latest versions. These applications are free to download and the software companies try to keep on top of problems associated with them.

6. Install Recommended Updates

So you now have latest and greatest operating system and applications. You have installed your antivirus and you consider yourself safe. Not just yet. Criminals can still find a way in and they realise that all software has vulnerabilities. These vulnerabilities either allow an attacker to gain extra access or they don’t. Criminals are constantly looking for ways they can use applications to highjack your system. They write malicious code to use these holes in the software to attack computers, phones and tablets.

Fortunately, designers and software engineers know this. To ensure their products are as secure as possible, they regularly release patches to close holes in their software. These are released as updates (not a critical security issue) and patches (security problem). All applications and operating systems have a way to inform us humans that they need to be updated. Typically, they inform us when we open the application or system. These updates should be installed as soon as possible after their release.

7. Use Social Media Cautiously

Although all social media platforms are web-based, they have a software component as well. Systems like Facebook and Twitter have hundreds, if not thousands of servers running the operating system as well as the application. This all comes down to the “cloud”. Every time you connect to the system you will be connecting to a different component running the same system.

The use of social media requires awareness on two fronts: the social component and the technology component. The technology of how the platforms work is extremely intricate and difficult for most people to understand. However, the same principles we have previously discussed still apply. The owner and writer are always looking to make the system more secure, while criminals are always looking at ways to exploit the system. In most cases the bad guys are winning.

We are all targets when we use social media platforms. Examples include malicious code targeted at Internet Explorer that adds a person’s mobile phone number to the log on for Facebook, and accepting “friend requests” or invites from people you do not know.

Social media use has to be tempered with caution. It seems people act less cautiously on the internet, in that virtual world. Whether you are always connected and using social media and sharing frequently, or you only use it once a day or less, we all have to exercise caution. Criminals are increasingly obtaining people’s personal information in this way.

The problem with social media is some people live their lives in the environment. They tell all of their “friends” where they are, what they are doing, where they are going and who they will be with, and they take photos to prove it. Not only are cybercriminals receiving information about what you are doing, but now also “normal criminals” (could be your friends) are learning more about your whereabouts. In this way, the next time you are going on holiday, they can be lined up outside your house ready to steal everything you consider important. It is wise to use restraint and caution when sharing on social media platforms.

8. Avoid Peer to Peer—P2P

Peer to Peer is a technology that was developed about 10 years ago. It was developed after Napster was sued by Metallica for breach of copyright. When Napster was shut down, P2P was developed in its place. Napster used a single location as its source and this is what was shut down. Removing the source removed the problem. P2P does not have a single source; in some cases it has hundreds of sources all over the internet.

It was developed to allow internet users to download data as a trickle instead of a download. The technology was used to download large files over bad internet connections, without using all of the available bandwidth to do it. This process was called torrent or torrenting.

Most of the time a torrent is used to download information for free. The main agenda on P2P environments is to download music, movies, applications and software. Once it is downloaded to a torrent, the application becomes a part of a worldwide network and its information is no longer stored in one location. Instead, it is stored on the hard drive of everyone who has downloaded the data, enabling anyone to now download it from one of those hard drives. This makes it very difficult for law enforcement to keep up with.

While this may sound pretty innocent, in fact, it isn't. Firstly, it involves stealing intellectual property that someone may have spent years developing. However, there is an even darker side to torrents. The torrent application does a number of things when it is installed. It creates a space on your hard drive that the internet has complete access to through the software. It tunnels straight through your firewall and allows anyone or anything to use the space for any purpose. This includes pornography, child pornography and high end criminal information.

In addition to that, when you use a torrent to download something you are also allowing numerous other internet users with the application to use whatever you have downloaded to "seed" the downloads. P2P software works on the principle that once you have downloaded something, you allow the rest of the internet to use that download as a part of someone else's download. This means that you are uploading information to other internet users.

But the worst thing about torrents is that they are also used by cybercriminals to store and create command and control systems for their nefarious and insidious programs. Some of the torrents have been used in bot net attacks and virus outbreaks.

9. Remember: Not Much is Actually Free

The number of times I have heard people claim that everything on the internet is free is staggering. It's not free! Here are a couple of examples of what can happen to give people the misleading impression that whatever they want is free.

1. Software companies will release software that is fully functional, but also full of restrictions as to its use. This software is designed as a teaser so that you will purchase their product once you realise the version you have is too limited. It is smart marketing. In addition, a number of software companies market a "lite" version of their software that allows the user to do many things as is, but will become even more functional once the full version is purchased
2. If you see the words "free download" when you are looking for a movie, you are in a dangerous area. Criminals understand the power of the word "free" and they exploit it frequently.

So you want a copy of the latest film that has just been released to the cinema and don't want to pay for it? Well, of course, a free download is what you are looking for. 99.9% of the times that you see a product offered for free, the download is riddled with malware, it is poor quality or, in the case of software, it just plain does not work. They are only interested in getting you hooked.

10. Use Common Sense

This may sound hard to believe, but the use of good old common sense is actually one of your best defences. Our basic five senses are quite useless in the digital world. The saying "something smells funny" has a literal meaning in the real world, but in cyber space the meaning is purely figurative. It is based on a feeling that something is not quite right, something is nagging at you and something does not make sense.

This is where common sense comes into play. In the rush to download the newest movie or song, in our constant search for the newest celebrity gossip to post to our social media page, we forget to think about where we are getting our information.

These rules of common sense should always apply:

- If it sounds too good to be true, then it is.
- If an item is promoted at 10% of the price seen in stores, hear the alarm bells ringing in your head.
- If it is offered for free, there is a good chance that it is a scam.
- If they want to give you money, but you have to give them money first, it is a scam.

That extra 10 seconds to think, or a cooling off period, will allow time for your common sense to kick in and often prevent you from falling victim to a scam.

11. An Added extra: Back it Up

How many times have you heard people say: “I couldn’t call you because I lost my phone”, or it broke, or it fell in the bath? In today’s world we are tied to our mobile devices in many ways.

Our mobile devices often contain detailed information on all of our contacts, our emails, our calendar events—so much of the most important information in our lives, and yet most of us do not have a backup of the system.

Therefore, the 11th tip toward protecting yourself against cyber-attacks is to back up your devices; make sure the information is stored in more than just one place. Often we can back up to our computers when the systems synchronise; otherwise, the devices can be protected offsite. An example of offsite protection is Apple and iCloud.

I work most of the time on my tablet or phone. I use a system that backs up all of the information that I create to the cloud. The only time that I could lose something is if either device failed before it had a chance to upload the new information to the cloud.

Conclusion

When it comes to the internet, protecting your identity, your money, and your data are of utmost importance.

Good individual cyber hygiene is critical to making sure that you are protecting not only yourself, but also everyone that you have contact with. It ensures that people you know are not going to get a nasty malicious email from you because you contracted a virus. It ensures that if you see something that appears too good to be true, then you realise that it is and do not pursue it. It ensures that when you want to know about the latest celebrity scandal, you will not agree to install the malicious script when you visit a website to find out about it.

It all comes down to taking responsibility for our actions online. Think to yourself:

- Cyber security is my problem—I will not rely on someone else to protect me.
- Cyber security is my problem—I will do everything in my power to protect myself as well as my friends.
- Cyber security is my problem—it is in my own self-interest to protect myself.
- The internet is an unsafe place. Be smart about making yourself and your systems safer.