A Basic Guide to Cyber Security

Simple steps anyone can take to improve their online and mobile security

by Chib Nwokonkor

Index

INTRODUCTION

Welcome to this e-book on basic, personal cyber security.

It is written in a manner which aims to be entertaining, interesting and relevant. There are an endless number of heavier tomes which outline the commercial approach to establishing cyber security awareness in the workplace and this in no way aims to be one of those. The summaries at the end of each section will outline suggested approaches which you can take to improve your online security, which should have minimal cost in terms of time and money.

I may write a follow-up book in a much more dour and technical manner but until then this should serve to put a smile on your face and help protect your personal data in equal measure.

Forgive my lack of Americanisms and the many cinema-themed references herein. I am British and didn't have many friends as a child. Not that being British necessitates loneliness. Movies were a substitute of sorts. I turned out okay so it can't have been that bad. Can it?

Anyway, I am eager and willing to hear from my many happy (or otherwise) readers. Feel free to contact me by email with any pointers, suggestions or marriage proposals. I promise to possibly read and not respond to all of them.

Scouts honour.

This book is dedicated to my wife, Rebekah. She's a doll.

Not literally.

Now, enjoy.

THE MOVIE

It can be argued that cyber security has only been a recent addition to our newspapers or social media newsfeeds. Until the term began appearing on the evening news, we could all peacefully tuck into our TV dinners, comfortable in the knowledge that our bank accounts were safe, our personal details were not for sale to the highest bidder and something as unnerving as the 'dark web' was simply another name for one of the bad guys in a Tolkien story.

Alas, cyber security has been an issue for much longer than the term or the media would have you believe. We are all aware that passwords are there for the safety of the users, the data or the organisation in question. We have watched enough movies to know that a security breach is immediately followed by a deafening klaxon, revolving red lights and the inevitable commencement of the self-destruct sequence.

Or was that just me?

Either way a security breach is not a good thing to happen.

And the consequences of a security breach can be as inconsequential for some as necessitating a quick virus scan and password update, requiring the reinstallation of an operating system, or even the end of an organisation and a way of living for tens, hundreds or thousands of people.

The issue is something which we have been aware of for as long as we have been using computers and mobile phones. Today we have fingerprint and retina scanners in the computers which we carry in our pockets and handbags. Every significant place of work requires its staff to use security passes as a matter of course. And if you find that you are no longer in possession of the necessary identification to enter the place of work you have been attending for almost a decade, you might suddenly find yourself with an unexpected day off, followed swiftly by a reprimand or worse.

The fact is, cyber security is an issue which can and does affect lives.

How so, you might ask.

Can you imagine a hospital working without any computers? And we're not simply talking about laptops, desktops and servers. I mean X-ray machines, personal data collection devices, electronic stethoscopes, defibrillators and life support systems.

Now I am not and have never been a medical professional, but I would imagine that a modern hospital would not work very effectively without the many and varied computer based devices which are used there on a daily basis.

So instead of those devices suddenly disappearing, what if they were compromised? What do I mean by this?

Well a defibrillator is a fairly common device. It is important and it is recognised as being something which can effectively save lives. And when it is used it usually does make all the difference.

Now of course I am not about to suggest that the device has a 100% success record in saving lives, but it is obviously important enough that it is commonly found at places of work, in non-emergency vehicles and we can even purchase them to keep in our homes.

What if no matter how diligent you were in ensuring the device was properly assessed, charged and serviced on a regular basis, you were told that it will fail to operate at least 50% of the time.

No matter how much time and energy is taken doing your research to find the best manufacturer, the most positive industrial testing results and so on and so forth, the device will fail more often than it can ever be effective.

People would be up in arms. There would be a refusal to spend money purchasing something which is less than a beta product at best. Alternative solutions would be found, costs would spiral out of control and the widespread use of a potentially life-saving piece of portable equipment, would be reduced in a moment.

Today we are seeing a rise in the use of electric or hybrid cars. Vehicles which produce zero-emissions, or are close to realizing that goal. And it is wonderful of course. Sustainability is the foundation of my life's work.

Hand in hand with the development of these eco-friendly vehicles is the development of automated or self-driving technology.

It isn't something new. In fact the idea has presented a popular theory since the 1950's along with the flying car, which funnily enough does now exist also. Car manufacturers covering the entire spectrum from Audi to Volvo have proposed and developed self-driving vehicles for almost a decade. A few years ago I watched a very entertaining movie called "I Robot" featuring Will Smith. It was based on an Isaac Asimov novel of the same name. A few scenes in the movie showed the main protagonist driving his car from one place to another, and at various times, being driven by the car in full-automation mode. This was very entertaining because at the time the film was first released, the idea of self-driving cars was not just alien to the public. It was pretty much seen as being impossible. The fact that the self-driving cars featured the Audi four ring emblem and looked very attractive was largely a positive attribute as well. I certainly wanted one, and I generally enjoy driving. In actual fact, it appeared that almost all physical labour in the movie had now been automated and was being done by robots or computer based systems.

Later in the movie, things went terribly wrong due to the introduction of some malicious code which caused the many automated systems to turn against humanity. I will try not to ruin the ending, if I haven't already.

That is a fear however.

Not simply that the systems we automate may choose to turn on us. That is not impossible of course and is something I discuss in another book.

What I am suggesting is, what if someone, an organisation, a company or a government, decided to use our dependence on automated devices against us? What if they were able to use our dependence on computerised data collection systems to skew our buying habits, to influence our

choice of personal hygiene products, or even to determine the outcome of the election of the perceived new leader of the free world?

Yep, I said it.

The fact of the matter is, anything that is not impossible must therefore be possible. And within the lifetime of a current generation, the idea of placing a man on the moon would have had you laughed into the nearest insane asylum.

So if we discount the possibility (probability) of powers within our comprehension having excessive control over our data and exercising the ability to use that power for their own gain, irrespective of the consequences, then everything else must be alright.

I would say no.

Although I would be the last person to suggest that we simply accept defeat and hand over all of our private information to everyone who asks for that information, I am at pains to point out that things can go wrong in technology, even with the best will in the world.

SUMMARY

Protect your private data by taking the following steps.

- Use passwords which are made up of a combination of upper and lowercase characters, numbers and where possible, symbols too.
- Don't use simple words, names or dates of birth.
- Don't write down your passwords in a place which they can easily be accessed.
- Avoid storing your passwords in the cloud or if you cannot do this then consider partially obscuring your passwords in a manner which can be deciphered only by you and no one else.
- Back up any and all important information regularly and store it offline in more than one place. For example I backup my work at least daily and ensure it is stored in triplicate in separate, secure physical locations.

SLOPPY CODE

Long before the beautiful graphical user interfaces or GUI's, which we use today became the norm, computer terminal users depended on something called the command line interface or CLI. Now the CLI was basically a set of characters and rules which you entered to perform a required task, whether that is updating a file, finding text or manipulating a data field. It was either powerful and efficient or time-consuming and obstructive depending on the user. Being a fully paid up member of the Bring Back Dos 5.0 society (BBD5... actually don't look for it, I just made it up) you can guess which camp I fall into. Clue, I didn't use a mouse.

The CLI even made its presence felt in many of the formative movies of my youth. Here is a by no means exhaustive list of the culprits:

- Akira
- WarGames
- Flight of the Navigator
- Jurassic Park
- Hackers
- Neon Genesis Evangelion
- The Lawnmower Man
- Neuromancer
- Ronin

To name but a few.

The CLI separated the administrators from the users, and if you owned a pocket protector and a shockproof floppy disk holder, you were automatically accepted into the CLI camp. Actually that was totally made up as well.

I digress.

The CLI was a way of getting things done, which didn't require 4k image rendering, motion sensitive keyboards or a VR headset either. It was a huge computing realisation of form following function and not the other way around.

However most people were not and are not geeks.

Most people don't want to have a degree in software engineering before they can be allowed to write an email.

And that is of course a good thing. Without the development of the GUI, the computer might still be relegated to the dimly lit halls of specialist education, research and DARPA (the US Defence Advanced Research Projects Agency). We might not have the wonders of Facebook, Twitter and overheating mobile phones which we enjoy today.

So we should be grateful and I am sure, many of us are.

However one consequence of our growing dependence on the GUI is the need for larger programs to be written. Larger programs means more code. And more code means a greater possibility for errors

to be introduced. What is more these massive code libraries make it much harder for erroneous code to be found. I would liken it to finding a needle in a haystack, but that would be incorrect as a needle can easily be found if you have a big enough magnet.

An error in code can have a small impact on our day to day lives. Shortly after leaving university I entered the world of work and found myself discussing technical developments in programming, hardware and artificial intelligence (A.I) on a regular basis with my similarly minded friends. Yes, I had some friends. Anyway, the discussion touched an issue which one of my friends was quite annoyed about. For no apparent reason, her main desktop computer would shutdown or reboot itself at odd times of the day. She might be doing some work, playing a game or simply have the computer on in the corner whilst she was doing something else and the computer would fail. She had re-installed the OS (operating system) tried various AV (anti-virus) tools, and monitored some of the processes which lead up to the system failure. Ultimately, none of those measures had proven to be effective. Now, as the title of this book is not "A Basic Introduction to IT Support", I won't go into the details of how we found a solution to the problem she was having. I will point out though that her computer was just over a year old at that time and had been subjected to very little use in the time up to the failures beginning to make their presence felt.

What was especially annoying was the fact that a system failure could occur at any time without any prior warning at all. One moment everything was fine, and the next she would be looking at a blue screen filled with indecipherable text and listening to the wails of a suddenly strident PSU (power supply unit). Not a good thing.

The question which later presented itself was, what if the core of this failing computer system, had been the CPU (central processing unit) of an aircraft mid-flight.

The worrying thing is, the many CPU's in an aeroplane are not vastly different to those found in the average laptop or desktop computer. The code that makes up the software which is running on the systems is recognisably similar and in fact, machine failures do occur.

Thankfully it is now incredibly rare for a correctly maintained and updated aircraft to fail for technical reasons. This has more to do with stratospherically (see what I did there) high standards in aircraft hardware and software engineering than anything else.

SUMMARY

- Save your work, constantly and securely. Either directly to a reliable USB drive(s) or a secure cloud location. Not just on your computer.
- Keep your software updated and ensure any official security patches are applied as soon as they become available from a trusted source.
- Don't procrastinate. Do what you can now, don't put it off until tomorrow.

Which brings us back to today.

CLICK OK

Earlier on, I had noted the developments in automotive technology which have led to the growing interest in automated vehicles. The idea of stepping into your vehicle, entering your destination or knowing it has been automatically uploaded from your cell phone, so you can sit back and enjoy the ride is an interesting one. Wouldn't it be nice to just get in, click OK and watch the world go by?

Companies as diverse as Google, Tesla and Uber have motorcars on the streets of the world, operating fully automated for at least some of the time. Aside from all of these companies having spent in combination, less than a tenth of the time in the automotive industry which Mercedes-Benz has done; they all have something else in common. All their automated systems have already had at least one publicly noted failure. In one case allegedly, the failure cost a man his life.

An automated system can only be as good as the programming which went into developing it. If we stray into the territory of artificial intelligence (A.I) and self-learning systems, faulty programming can be the root cause of a catalogue of errors.

If we don't apply the same stringent rules and standards which are present in flight planning and aircraft development, as well as accept the high costs which go hand in hand with that level of care, then we must surely expect to find ourselves in a position whereby we are positioning our lives at the mercy of substandard software.

It is common knowledge that humans are prone to errors when it comes to vehicles. We might drive too fast, or indeed too slowly for the circumstances surrounding us. We may fail to maintain our vehicles correctly and thus increase the possibility of a physical failure occurring which could have been avoided otherwise.

Instead of pointing the finger of failure at the inevitable march of technology, a better approach would be to determine how best to avoid errors occurring in the first place. How can we apply multiple error-checking layers which co-operate with one another and are able to feedback relevant information to the operator?

It works in aircraft, though most passenger carrying planes enjoy the benefit of having both a Captain and a First Officer on hand to address the many thousands of pieces of information being thrown at them during the course of each flight. Some aircraft even accommodate a Flight Engineer in the cockpit too.

Such a drastic and personnel-heavy solution doesn't translate so well into the average family car.

So the data which is thrown up in real-time must be assessed, resolved or redirected to the operator, be that another onboard computer, or indeed the human being at the wheel. With increasing speeds and more densely occupied conurbations, the quantity of information which is needed to be assessed per second increases exponentially.

You can reduce speeds considerably which might help reduce the incidence of collisions, though is likely to annoy a large part of the population through what they might perceive as wasted time on

longer journeys. I would argue that travelling a few miles per hour more slowly is likely to use up less time than an extended stay in hospital or worse.

What if we do achieve digital oneness, the virtual nirvana of perfect programming for our self-driving cars. Every car is able to respond to what is happening around it in milliseconds. Vehicles performing overtakes in a gradual and safe manner, changing lanes without swapping paint and parking half an inch from every kerb. That would surely be wonderful. And I am sure it will be.

If.

A two letter word which manages to encompass so much meaning, malice and potential in such a small place.

The above scenario of self-driving car heaven would be effective if and only if every single vehicle on the road were self-driven at all times without allowing the operator, or should that be passenger, to intervene in the control of the direction, speed or deceleration of said vehicle at any time during its journey. The occupants of the vehicle would very quickly become nothing more than passengers.

Which might be fine if we were on train tracks, but alas the road is a much busier place.

And besides, I'm not sure if I would bet that most people are happy to buy a car over which they have no control once they have set the destination.

Then again we may find ourselves at a point in time where the very idea of buying a car for personal use might be seen as a fallacy.

I feel another book coming along.

SUMMARY

- Be aware of what you choose to click on.
- Do not leave your planning to an automated system or to automated Virtual Assistance. Check any and all developments instead.
- Use digital tools to assist you. Do not solely rely on them.
- Apply common sense to all that you do online, just as you would in the real world.
- Do not blindly click on anything which is presented to you, no matter how official it appears to be.
- Do not follow auto-install procedures with any software. Instead click the advanced or manual option. It is rarely advanced and instead it will give you the opportunity to determine exactly what is being installed.
- If in doubt, do not hesitate to use the tools at your disposal to read reviews, learn about other people's experience of the software in question and ensure you take relevant knowledge onboard.
- Do not carry sensitive material in public without remaining aware of its security at all times. And if you must do this, ensure you travel as directly as possible between locations.

BLAINE THE MONO

I once read a sequence of books by the esteemed author Stephen King, titled The Dark Tower. In my more reflective times I have wondered if the more positive attributes of Roland Deschain, the main protagonist in the series, had found themselves into my psyche. Fortunately or otherwise I have little appreciation for wielding twin steel cannons or battling man-eating crabs. I did enjoy the series however and am sure I have the books in my library somewhere.

One of the many significant though fairly short lived characters in the series was a riddling monorail named Blaine. Specifically therefore, Blaine the Mono.

Blaine was an A.I controlled monorail, programmed to cover vast distances at amazing speed and react instantly to developments around it, of which there were very few as a consequence of Blaine operating mostly on an elevated track or through deep subterranean reinforced glass tunnels, thus allowing travel at near supersonic speeds.

Shades of the Hyperloop. This is beginning to feel a little like Back to the Future Part 2!

Anyway, Blaine had been operating for many hundreds of years following the fall of humanity for reasons at that point unclear. It may have been self-destruction following global political breakdown, the much-hinted eventual rise of the machines or even the inevitable outcome of a surely insane decision by the most powerful nations on Earth, to adopt an ostrich-like climate change policy. Not that I am hinting at anything.

So following nuclear war or something equally calamitous like the cancellation of "I'm a Celebrity", Blaine is forced to operate without human interaction for hundreds of years. Being solar powered and self-aware, Blaine lacks neither power, knowledge or time and is driven mad as a result.

When the characters of the book come across Blaine the mono, it (should I say he...) decides to present a challenge to them as they go on their journey. Not a simple game of I-spy either. The consequences of failing the challenge are suitably awful for a Stephen King story of course. I would urge you to read the series, or at least get the CliffsNotes.

If a system can run without human intervention yet exists purely to cater to a human want (as opposed to a human need), whilst having the potential to become self-aware, how long would it continue to operate as planned before if determines that the best way to protect the carbon based organism it is designed to transport, might be to minimise the exposure of that carbon based organism to any and all external forces. Why would it let you get out of the vehicle, at all?

This is quickly becoming a philosophical discussion on a dystopian future as opposed to simply urging you to update your passwords every few days!

The crux of the argument is, if we were to hand over control and authority on what we do and how we live to entities which do not depend on us, require us or even recognise us as being important somewhere down the line, are we not failing to secure our well being in exchange for a perceived "easy life"?

It may seem far-fetched or that I am influenced by a lifetime of bad movies but remember, whatever is not impossible must surely be possible.

So knowing what you now know, is thoughtless dependence on the march of technology really a good idea?

SUMMARY

- Question everything. Without sounding as if I've been watching too many Bourne movies back to back, it is always important to check the validity of the information which has been presented to you.
- Avoid following the crowd. Understand the consequences of your actions and the hidden meaning in public communications.
- Remain calm and consider your options at all times.
- Always have cash available, ideally in small quantities on your person. Try not to depend too heavily on credit, debit cards or contactless transactions.
- Have a charged portable battery pack or at the very least a charging cable on your person, ready at all times. To have it and not need it is better than the opposite.

DODGY DOWNLOADS

I have a mobile phone. In fact I have more than one as I am sure do many of you. The phone has become an extension of me. It is a central component of my day-to-day life, as a terminal for reference information, scheduling and entertainment. Sometimes thinking back to the days of the Filofax and personal organiser, I wonder how we were able to get anything done. Now information is a mere click away. New software can be downloaded at the click of a button and "isn't there an app for that", is heard to echo up and down the city streets.

It is so easy to download software from the internet and run it on our mobile phones. The same phones which we use to harbour our most private information, to access our bank accounts and read through those cringe inducing Pinterest updates we wrote way back when.

A lot of the apps we download might offer unwanted and undocumented features. Not too good eh?

Even if the use of your phone continues unimpeded by what you are downloading, the consequences of a lack of care and consideration can be financially and emotionally damaging. Maybe to yourself, or someone else.

The NIMBY principle (Not In My Back Yard) might apply to some, but surely not to all. The global financial crisis we recently experienced which is thankfully over (ha, funny) was originated by a decision made by one person to do something which was questionable perhaps, but certainly not illegal. The potential consequences of those actions were so vast as to be at that point, beyond both belief and conception. The unfortunate reality is an ongoing bad dream for many.

In recent times the media has thrown up many entertaining stories which have roots in all of this:

- Man robbed of phone has it returned for not being particularly desirable
- Toddler racks up $1000's playing online games on parents tablet computer
- Holidaymaker accumulates massive data charges bill whilst NOT using mobile phone
- Shock story - Santa Claus is not real

Admittedly I made the last one up, Santa is obviously very real. The personal communicator device which we have seen for years on endless Star Trek episodes is now with all of us, in our pockets and handbags, on our desks and glove boxes. If you have ever misplaced, or worse, lost your mobile phone and all the information therein, the stress caused can apparently be worse than that caused by a house move, the breakdown of a long term relationship or even as bad as stubbing your toe.

I do like to raise a smile but the dangers of compromised data security are serious and potentially vast. Apps are small, low cost pieces of software which can be downloaded and accessed anywhere at any time as long as you have access to Wi-Fi or a data connection. The convenience offered therein makes apps uniquely attractive and an increasingly prominent part of our everyday lives.

Even within the heavily self-policed app stores of Google and Apple, it appears that not all software is as it seems. At its most innocuous, properly downloaded software may introduce additional code to present unwanted advertising to the user. A program may have a hidden purpose which runs in the background, obscured by the programmer to maximise the presence of the program and assist in the undertaking of more nefarious activities. It is common knowledge in Penetration Testing

(software and system security specialist) circles that modern Distributed Denial of Services (DDOS) attacks are increasingly based on cellular technology as opposed to the usual computer terminal methodology with which many of us are more familiar. Online data is accessed more widely on mobile technology today, than it is on desktop technology. Yet the percentage of tablet or mobile phone based devices which are running established and paid for AVAM (anti-virus and anti-malware) software is less than a tenth of the number of desktop based systems which are running the equivalents.

SUMMARY

- Download established Internet Security software from the relevant app store for your mobile technology.
- Use the software and keep it updated.
- If you do not have similarly established internet security software on your laptop or desktop computers, rectify that problem immediately.
- If you depend on an IT department for your data systems management, ensure they have procedures in place to maintain the integrity of your data and the digital wellbeing of your organisation.

UP IN THE AIR

I mentioned Wi-Fi in the last section. Purely in passing though I was not dismissive of its importance.

Wi-Fi has become an important part of our everyday lives, whether it is used to share information within a workplace, stream music around the home or to watch YouTube videos when you really ought to be finishing that assignment you're due to hand in tomorrow.

Wi-Fi comes in many forms however. Not simply the A, B, G, N and AC types. I mean private and public. And by private and public, I mean known and unknown.

Just because the SSID of a Wi-Fi hotspot looks as if it might be valid, doesn't mean it is trustworthy or that it has not been spoofed (named in such a way as to draw in unsuspecting users). Not all Wi-Fi networks are official and what is more, it doesn't take anything more than a laptop or tablet with wireless connectivity to setup a fake Wi-Fi hotspot.

And this is how to do it.

Really? I am not going to explain how to setup a fake Wi-Fi network. I will say this however. If you are able to setup a small Wi-Fi connection at home, it takes a similar level of technical ability to setup a fake Wi-Fi hotspot.

What is more once that fake hotspot exists, the individual or organisation operating it has access to arguably all of the information which passes through that network. Which really isn't a good thing, for you.

The fact remains, identifying trustworthy public Wi-Fi channels is becoming increasingly difficult. My advice would be to avoid using any and all public Wi-Fi and ideally most private Wi-Fi unless the latter was established by yourself or a trusted source.

My mobile phone company loves me because I use a lot of data.

My bank hates me because I never lose money from my accounts.

So I guess that evens things out.

SUMMARY

When establishing your own Wi-Fi network, considered hiding your SSID.

Furthermore in addition to the above, always use password authentication and consider establishing White-lists (approved IP addresses) where possible.

Never ever use public Wi-Fi.

If you must use public Wi-Fi, do not use it to conduct any important transactions at all.

WHAT DOES THE RED BUTTON DO

Hopefully by now you haven't retreated into the corner of the room and curled yourself into the foetal position. The reality is, should things ever go terribly wrong in the world once again, the main currency is more likely to be water, minerals or information than anything else. Simply depending on our governments to take care of our data security is a failing we can all easily avoid. The security of our families, our friends, peers and ourselves can be improved significantly just by applying the small steps you learned through the course of reading this short e-book. It was designed to entertain as much as to inform, so I hope you come away enlightened and encouraged at this point.

Cyber Security is a massive issue and a journey of a thousand steps.

Like every journey worth taking, it is worth taking care and doing it properly.

It makes things a lot more fun in the long run too.

And of course, if you find yourself in a position where you are not sure what is being done to your data, device or private information, pull the plug or push the big red OFF button. After all, knowledge without the power to use it is akin to nothing.

Thank you for taking the time to read this e-book.

Should you have any further questions please feel free to email me using chib@zanshuri.com, or visit my company website Zanshuri.com to learn more about the sustainably centered products and services which we have to offer.

Have a great life.

Chib Nwokonkor

Chief Executive - Zanshuri Ltd

The end