CYBER SECURITY BOOKLET

ZICT | Division Of ZIE

Table of Contents

FOREWORD

Engineer Jacob Kudzayi Mutisi
Chairman for the ICT division (ZICT) of the Zimbabwe Institution of Engineers.

With a mobile penetration rate of 102% and the growth of the internet, emails, mobile money, internet banking, social media, mobile application. Technology is rapidly evolving and is becoming part of our daily life. While it provides fantastic opportunities to transact and communicate more efficiently and effectively, enhance processes and achieve greater prosperity, it is also open to criminal abuse by cyber criminals. This booklet has been developed to assist you to take the necessary steps to defend your business and yourself against cyber criminals.

ZICT the Information and Communication Technology division of Zimbabwe Institution of Engineers has recognised the changing face of our day to life through the use of mobile devices to communicate and to transact now requires security against intrusion.

This booklet aims to identify common types of cyber crimes and the ways you can protect yourself from them. It is not an exhaustive list, in what is an ever changing landscape, but by following the advice given you can improve the protection of yourself and the knowledge of the existing systems. The ZICT crime survey shows for the first time that card cloning fraud, mobile money, internet abuse are the most prevalent crimes committed against people in Zimbabwe and these are some of the areas that will be covered in this booklet.

We hope that you find this booklet to be both useful and informative. We also hope that it encourages you to protect your business and yourself in today's online virtual world.

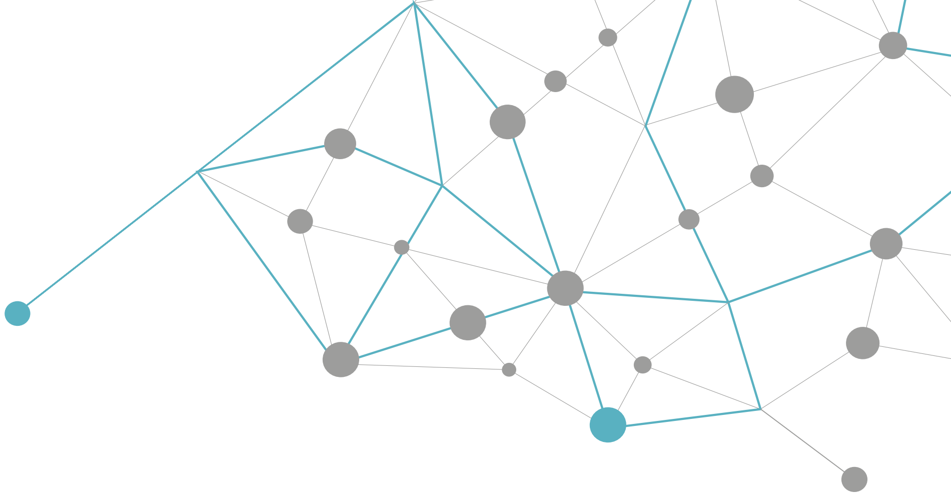
Message from the Minister of ICT, Postal and Courier Services

As the Minister of ICT, Postal and Courier Services I am enthralled by the level of interest and engagement of our nation and civil society as a whole in matters pertaining to the security of our Zimbabwean cyberspace. The Internet and digital technologies are revolutionising our society by driving economic growth and providing new ways to connect with one another. The use of technology is transforming the way business is being done by making it more effective and efficient. Consequently, there is an increased flow of innovation and productivity, thus driving the expansion of the cyberspace.

The ICT sector is a key sector in Zimbabwe and the vision is to create a knowledge-based society with ubiquitous and secure information systems by year 2020. The aim of the Government is to embed the use of technology in the day to day life of every Zimbabwean. This would imply that government services, businesses, lifestyle as well as the physical infrastructures would be centred on digital infrastructure.

In Zimbabwe, ICT has been hailed as the engine for economic growth and yes it is, only to the extent that it is valued as such by the country's citizens. Why do I say so? It is all our responsibility to safeguard the cyberspace from attacks which can render the individual, the corporate and government to be communication-less just as the rural Zimbabwe in the 50s.

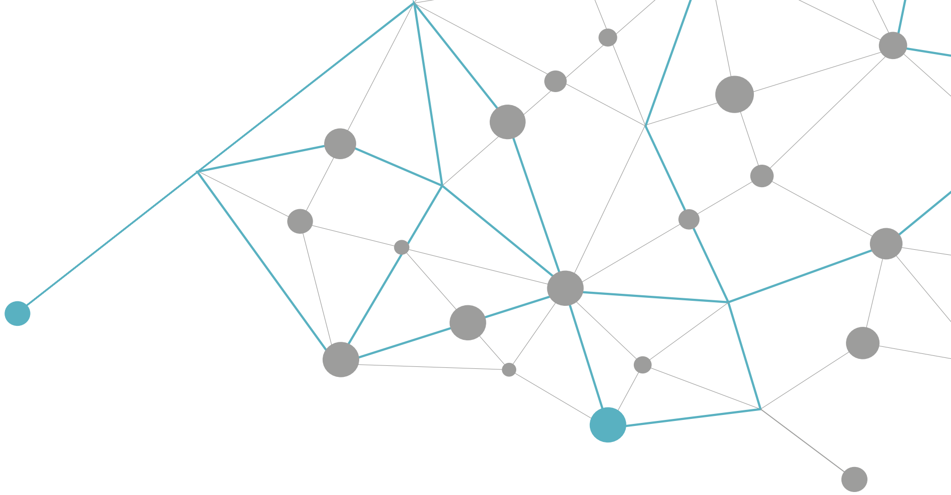
The vocabulary we have now did not exist in the 50s. The word 'cyber' itself did not exist in the 50s. It came into being in the 80s. We now hear of cyber threats perpetrated by governments on governments, cyber terrorists, hackers, cryptojackers and many more who threaten our communication infrastructure, steal and abuse our data, and render our computers inoperable. Therefore a serious attack can render the national ICT engine seized.



Through our stakeholders and partners the Ministry of ICT, Postal and Courier Services undertook an initiative to educate and protect our nation on cyber threats that exist in Zimbabwe and beyond. This booklet will provide the perfect opportunity to promote cybersecurity awareness and safety tips, ultimately changing behaviors to protect people against cyber threats in Zimbabwe. According to recent estimates, cyberspace now encompasses more than 2 billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, desktop computers and industrial control systems that run our power plants, water systems and more. While the vast majority of the Zimbabwe's cyber infrastructure is privately owned, the security and economic implications are so profound that their protection is of national importance. There is no escaping the reality that our lives, homes, economic prosperity and national security are impacted by the growth of these technologies and the internet that is now really available.

Cyber threats are on the rise globally and are proving increasingly sophisticated, and difficult to mitigate; the imminent threat of cyber-crime to National Security means that Zimbabwe must be prepared and, in the position, to prevent and respond to evolving cyber threats.

Hounourable Kazembe Kazembe
Minister of ICT, Postal and Courier Services



INTRODUCTION

Cybersecurity is an essential part of how we live in today's world. This Cybersecurity booklet contains much information on the need for cybersecurity awareness, providing a jargon-free guide to simple and effective practices. This booklet has been specifically designed to offer advice to everyone on staying safe in the cyber world. We are all using our mobile devices, on social media, using the internet and mobile money transacting.

With limited resources and turbulent economic conditions, Zimbabwe government has prioritised innovation and growth over online security and risk mitigation. These issues are often seen as expensive, burdensome and time consuming. It is important though that these areas are recognised and assessed and that everyone is aware of the risks that they face from cyber criminals.

Zimbabwe is a cashless society with 96% of all transactions being electronic which means we all rely on the internet or mobile technology to do business. We communicate, buy and sell on it, contact our family, friends, suppliers and customers on it. However with all the opportunities it brings, it is important to remember the risks.

Every day in Zimbabwe there are reports of mobile money fraud, internet fraud, emails scams and social media abuse. There are criminals who take advantage of the anonymity of the technology world to deceive, hack and steal if the opportunity arises.

If an attack is successful it could have a devastating effect on yourself and/or business. Reputational damage, financial loss and property loss. For business, theft or loss of data can have a considerable effect on a company's reputation, including a loss in customer confidence, and may lead to significant fines.

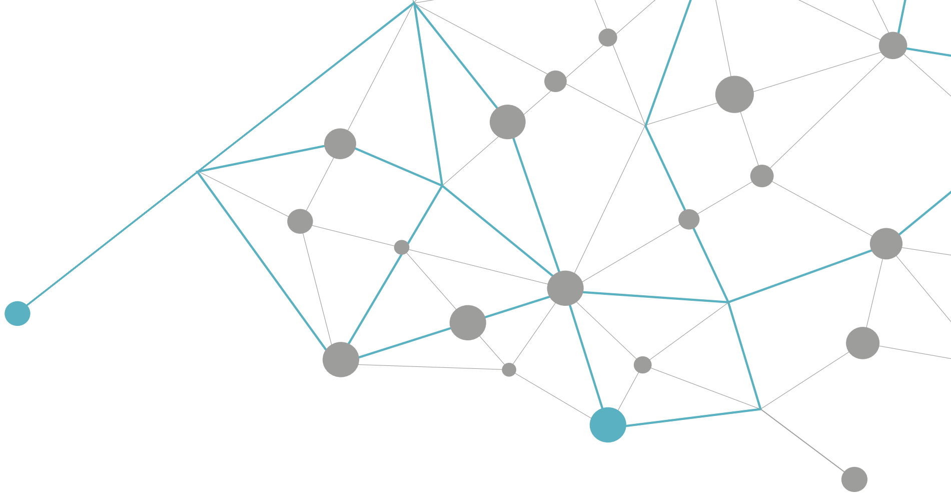
This does not mean you or your business should not use the internet. All that is required is to be aware of the threats, and this booklet can make a significant difference to your chances of becoming a cyber criminal target.

CYBERSECURITY

USING SOCIAL MEDIA

Take care what you share

Computers, smartphones, and other devices are invaluable resources that provide individuals of all ages with the unprecedented ability to reach out and interact with the rest of the world. Zimbabweans are able to do this in a number of ways, including the use of social media or networking sites. Social media can be a hugely fun and powerful way to keep in touch with old friends and make new ones, share your interests and keep up to date with the latest trends. Unfortunately, social media like WhatsApp, Facebook, Twitter, YouTube, Pinterest and LinkedIn are just as popular with criminals, you may be surprised to find out why. Anyone who has spent time on social media knows exactly why it is so addictive and entertaining. You can get instant, live responses and feedback on your opinions and sometimes even take part in conversations that can make a real change to peoples lives, influencing anything from what someone wears or eats, to the government and politics of a nation.



But everyone knows there is a dark side to social media too. Because of their widespread popularity, they are also used for nefarious purposes that include cyberbullying, harassment, stalking, fake jobs, fake deaths and hacking in your other accounts.

Anatomy of a hack

Let us assume one is a hacker and wants to take over your online identity. When you sign up to anything on the internet, from online banking to email, you are asked to provide the answers to a number of security questions which include your mother's maiden name, your pet's name, your school, your date of birth, your childhood nickname and so forth.

Now think about your social media accounts. If I have your email address how much research would it take me to get the answers to those questions? Are there pictures of your pet on Facebook, do you mention its name? Does anyone use your nickname in the comments section? Is your birthday mentioned? Is your school mentioned.
You get the idea, right.

Once a hacker has done a social media research he/she just needs to click on the 'Forgotten your password' link in your email account. And from there he/she simply uses the personal details discovered to answer your security questions.

Now the hacker has command of your primary email account and can use that to go through all your online accounts and click on 'password reset'. This will send a reset request to the mail account that the hacker now controls, allowing him/her to change all your passwords, locking you out.

Consider for a moment how much damage a hacker could do to your life if they had that kind of access.

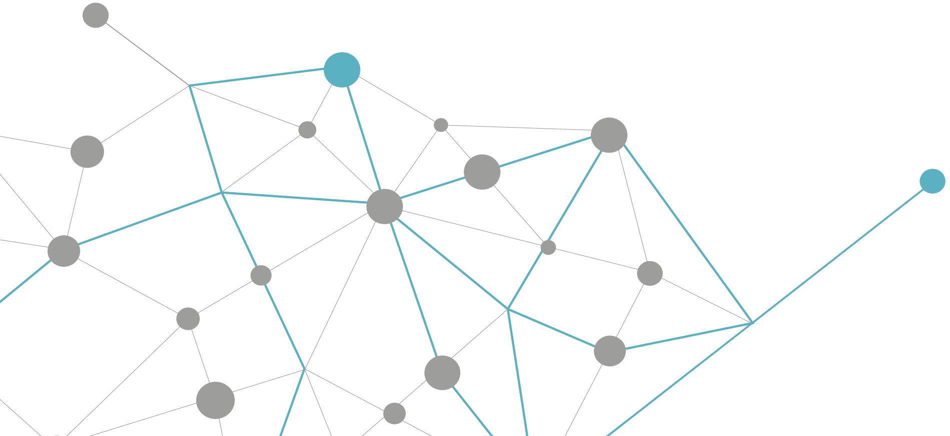
Be careful what you share

The steps to take staying safe while still enjoying social media are:

Think before you post: Be wary of putting up any information that could be used to break into your online accounts. That means guarding your home address, email addresses, phone numbers and date of birth. Consider using your security questions as another layer of security, treat them like a password; fill in the answers using made up, complex codes or phrases.

Keep the public and the private separate: Everyone wants to share personal things sometimes. If you need to then the best thing you can do is post privately. Check the privacy and security settings on your social media sites so that only family and friends can see your posts. The settings are there for a reason.

Try not to let the world know where you at all times:



Telling everyone where you are at all times also lets them know when you are not home. Anyone watching your Facebook, Twitter feeds and LinkedIn know exactly when it is the best time to turn up to your home uninvited, and steal your stuff because you have posted your pictures and location.

Tidy up after yourself: If you have stopped using a site, delete the account. Do not leave it lying around, unattended for anyone to pick up.

Think twice, post once: What you post online stays online, forever. Always take some time to think if what you are about to share is something you will still be happy for anyone to see in the years to come. Imagine someone you respect reading your post, feel uncomfortable? Or try this; would you have a permanent tattoo of that post on your body? If the answer is NO then it is probably best not to hit 'send'.

Know who your friends are

It can be exciting to build up a big list of 'friends' but how well do you know all of them?

In fact, how well can you know such a big, diverse group of people?

If you trust them like you trust your family then by all means share everything. But would you, for instance, let them into your home when you are not in? If not, think twice before you let them into your confidence.

If something looks or feels suspicious, delete it

Requests to sign up to something you haven't heard of, friend requests from people you do not know, online advertising and unknown links in emails and tweets are all ways cybercriminals try to steal your personal data. Do some research before you click. Or just delete it

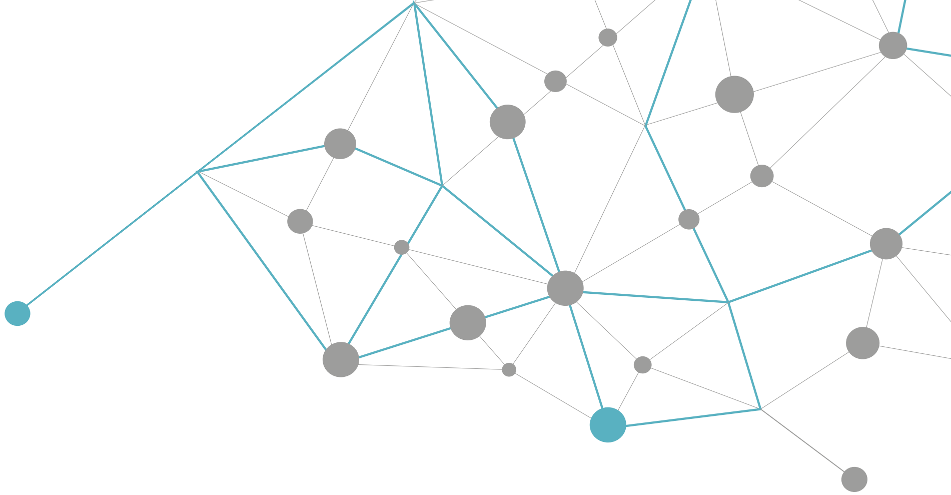
MOBILE MONEY SECURITY

Paying bills, shopping, transferring money, checking your bank account, you can save up time and energy by just doing all these things from your phone, no matter where you are. But the question is how safe is your money? There are over 9 million mobile money accounts in Zimbabwe with most subscribers on Ecocash Mobile Money. This is a huge market for scammers also to carry out fraudulent activities. You need to protect your phone and your account's information from hackers, thieves, and malware.

How to protect yourself against Mobile Money Fraud

Register with a trusted agent

Whether you are on Ecocash, One Wallet or Telecash, you can be at risk if you do not register or do transactions with a safe, trusted and an accredited agent. The best option is to register at your nearest mobile money operator. Once registered, learn how to transfer and receive money yourself. Avoid giving your mobile phone



to agents or friends when transferring or receiving money. Take total control of your stuff. If you face any problem, your operator's nearest branch office is the safest place to seek solution.

Set PINs and passwords on your phone

Some people feel really uncomfortable setting up passwords to lock their phone or tablet. If you are somebody who is forgetful then this may not be a great solution. However, the best protection against somebody gaining access to your accounts from your phone is by using a device password. This means whenever somebody goes to open your phone it will require a passcode before unlocking.

This is a great solution if you are often moving around and traveling with your devices or allowing your friends to use your phone more frequently. Protect your phone/tablet with a strong password and set up a SIM card PIN so that it can't be used in another device.

Make sure you do not use the same numbers as your mobile money PIN or ATM PIN. Even better than using a numerical password is to use the "fingerprint" technology that is available on most new smartphones.

Do not store account login details, any passwords or account numbers on

There are **over 9 million mobile money accounts in Zimbabwe**, this is a huge market for **scammers** also to carry out **fraudulent activities**.

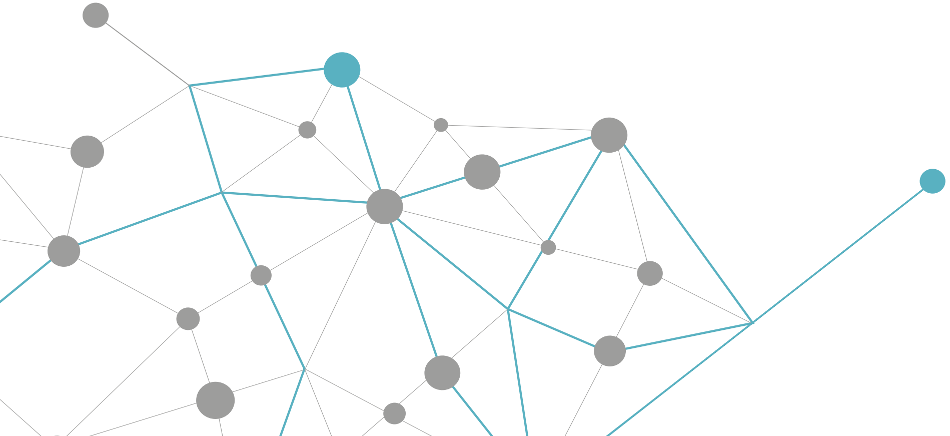
your mobile device. Keep them safely stored elsewhere. In fact, do not store any sensitive personal data on your device. If you're recycling your phone or passing it on to someone, make sure you delete all such personal information first.

Choose your mobile money PIN wisely

When choosing your mobile money PIN, select the numbers at random, memorize it and never disclose it to anyone. Many people use their date of birth, phone number or other IDs (School, work, voter ID etc.) as their PIN and as a result get scammed. Choose a strong PIN that no one can easily guess.

Use only your bank's official app

Our banks in Zimbabwe allow their customers to transfer money from bank accounts to mobile money and vice versa. If you are using any of these banks for this service, verify that a banking app is official before you download and install it.



Additionally, do not download an app anywhere apart from Google Play, IOS or Windows App Store. These are the safest places to download apps for your mobile device. If you have any doubts, check with your bank first. Using your bank's app avoids the risk of you logging on to fake sites. Also remember to log out of the app or mobile site when you've finished.

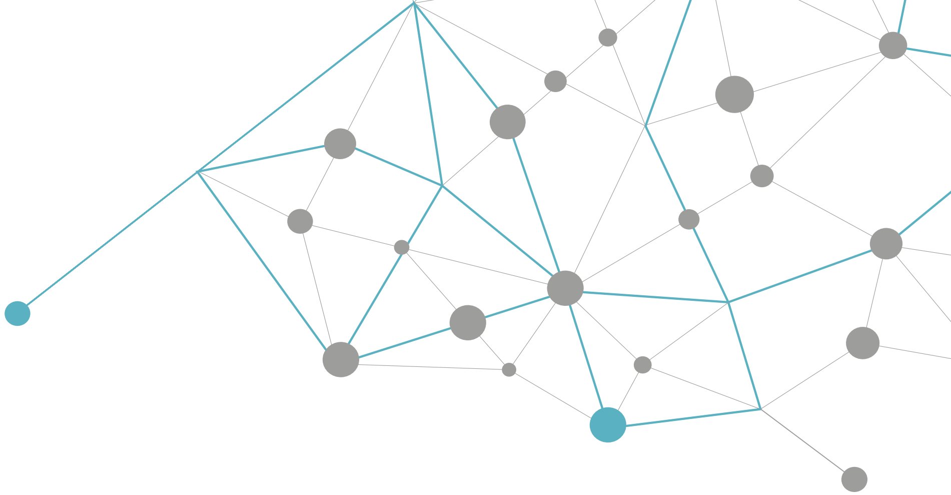
Avoid public (risky) Wi-Fi

Do not carry out sensitive and financial transactions using public Wi-Fi or unknown networks. Public connections are not very secure. All places that offer a public Wi-Fi hotspot must warn users not to share sensitive information over their network. The open nature of public networks makes them vulnerable you never know who may be poking around and watching what you are doing online. Make sure you use a secure connection when making any financial transaction or communicating with your bank.

In addition, any compromised devices or USB keys that are connected to the local network could pass on malware to your mobile or tablet. You can get around these issues by disabling Wi-Fi on your device and using your cell network instead. It is good practice anyway to turn off Wi-Fi and Bluetooth when you are not using them.

Beware of fake SMS scammers

Be aware that some scammers send SMS messages purportedly from your bank, or your mobile money operator requesting your personal identification number, or PIN; account number; or other vital information. Any such request



for information is almost certainly fraudulent or phishing attempts.

Always tell your bank or your mobile money operators about any suspicious emails or texts you receive. Do not click on dubious links in emails or text messages. Never send financial information by unencrypted email.

Protect your mobile device with security app

Install mobile security app and keep it updated. Do not forget to install updates for your device operating system and banking app too as they become available. You are more vulnerable to evolving threats if you have outdated versions of apps on your mobile phone/tablet.

Back up your data so that you can recover it if necessary. If possible, get a tracker for your mobile device, so that if it is lost or stolen you can locate it via GPS (Global Positioning System), remotely lock it and wipe your data.

Watch statements and report suspicious activity

If you are ever in doubt about your mobile money accounts being compromised do not hesitate in taking action. You can change your PIN many times over when you feel it is a good idea. Often times your gut instinct may indeed be correct without having any solid evidence.

Also be sure to log into your mobile money account every so often and make sure there is no suspicious activity. Check for any money transfers or withdrawals which you didn't authorize.

These 10 good practices are just the first step to take in ensuring the safety of your mobile money. As prevention is better than cure, make sure you are always up to date with mobile developments, the mobile security risks they pose, and ways to counter them.

BANK CARD SECURITY

Consumers in Zimbabwe are now paying with bank cards due to cash shortages. For thieves, that plastic represents a lucrative spending opportunity. So far in 2018, the number of bank cards compromised at merchant card reader (through card cloning) are over 154 cases card with most of the cases not being recorded. Bank card cloning is typically done via skimming devices that capture card data. Credit card skimming is a form of card theft where criminals use a small device (or "skimmer") to steal your card information from legitimate places of business. These skimming devices can be attached to ATMs or designed to look like a proper card reader.

How to protect yourself against skimming or your card being cloned

Keep your card in sight. If you are in a store or restaurant, make sure you hold onto your card or keep it within your sights at all times so that you know it is only being used on the one machine.

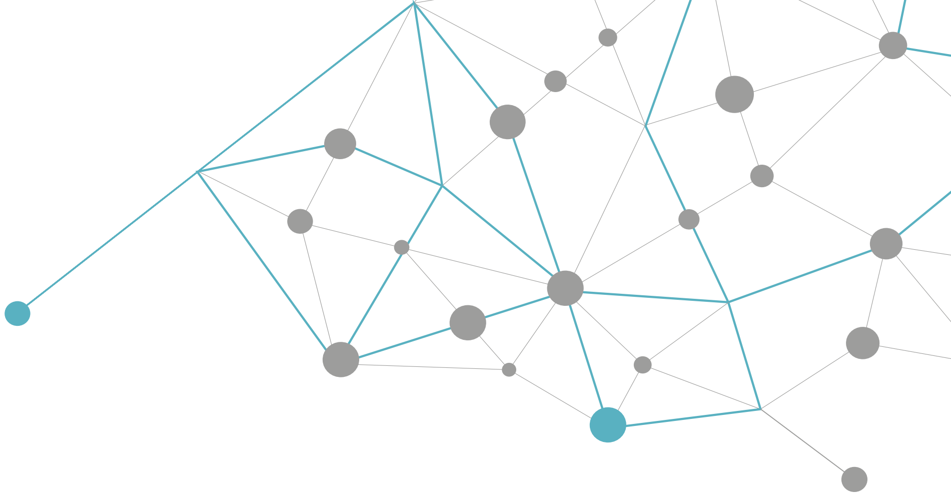
Never share your PIN. Do not tell anyone your PIN, do not write it down and definitely do not keep a copy of it in your wallet together with your card.

Be discreet with your PIN. As petty as it might sound, covering the keypad as you enter your PIN could help prevent someone stealing from you.

Look for signs of tampering. Before you use an ATM, always check for any suspicious features. Also try wiggling parts of the machine, because legitimate ATM machines are solid constructions that do not usually have loose or moving parts.

Avoid outdoor ATMs. While this is not always necessarily true, an ATM inside the mall is generally safer than a lone outdoor ATM on the street, based on the logic that the former location makes it harder to tamper with.

Check your bank card statement. Checking your bank card statement is a good habit, and itis now easier to do this regularly thanks to online banking.



Doing this is important because you can identify fraudulent transactions as soon as they happen, and your account can be frozen to prevent more theft. Report suspicious activity. Immediately call your bank, the ATM provider (where applicable) as well as the local authorities if you suspect your account has been compromised..

Notify your bank when you go overseas. Letting your bank know where you are will help them identify legitimate transactions you make when you're abroad. It can similarly help them detect suspicious activity, and allows them to contact you if they want to verify a transaction. If you're going away for a long period of time, it is also wise to inform them that you are not planning to use the card for a while.

Set Up Daily Alerts With Your Bank. Most banks give you the opportunity to set up alerts. You opt for text message alerts, because it gets my attention. I have set up the alerts so that any transaction greater than $0.01 using my bank card results in a text message being sent to my phone. You will know right away if I have been compromised.

Sign Up For 2-Factor Authentication: Many banks give you the opportunity to sign up for 2-factor authentication. That means that a username and password is not sufficient for signing into your account. Instead, you need to have a text message sent to your phone, or an email sent to your account. You are usually given a number of options for setting up this higher level of security.

Consider A bank Card For Your Everyday Purchases: Bank cards can be dangerous. For too many people, a bank card serves as a source of temptation to spend more money and get into debt. But, if you have the self-discipline to manage your bank card responsibly, it can be a wonderful tool. Although banks are generally good about putting cash back into someone's checking account during a dispute, it does not always work perfectly.

KEEPING OUR CHILDREN SAFE

Today's children love our phones, computers and the internet, it is really that simple. Many parents know their kids would be on our devices all day if they were allowed and that is because all children see is the good stuff. Games, videos, animals, chatting to friends, answers to any question you could possibly think of, made up celebrity gossip, pop music, Google Earth and sport.

But like so many things in life it is what they do not know that is the danger. They have no idea about password security, trolling and 'netiquette', phishing, cybercrime, hacking and the myriad of other security and safety issues most adults take for granted.

The internet can be a wild and unregulated place, an environment totally at odds with the desire we all have to protect our kids, but one they cannot wait to dive into, so where do you begin?

CONTROL THE ENVIRONMENT

All applications come with safety settings, get to know them. There are also some powerful, dedicated software programmes available that can allow you to filter access to specific sites and programs, receive email alerts if restricted sites are viewed and even record keystrokes.

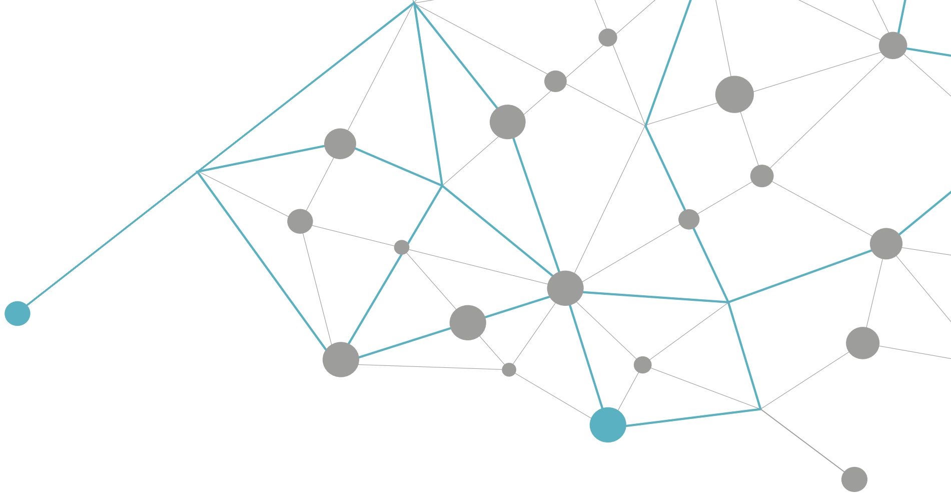
Many children probably do not need that level of surveillance but do some research to see what's available and use what is appropriate. But remember, no system can deliver 100% safety.

Stay together

If your children are young never, ever, let them surf the net alone. You would not take them to a new city and let them run free, in and out of stranger's houses all day long would you? So do not leave them alone online, no matter how strong your security settings.

Have an honest conversation

Most parents want to retain their children's innocence while still letting them have some freedom. It is a delicate balance but you can start to achieve it by having a genuine and open discussion about the dangers they could run into. How direct you want to be is up to you, and depends, of course, on the child, but it is important to at least start to talk about the idea of inappropriate content and the existence of bad people. You do not have to scare them, just try to prepare them with the basics before one of their friends or an older brother or sister tells them to do something silly.



Train a mini 'CIO agent'

Children are so often interested in the things their parents and older siblings are enthusiastic about so try to show them that being switched-on about digital security is for the smart kids.

Next time you have to update your system software or install a security patch, get your kids to do it with you and tell them why it is necessary and how it could help. Then when they have done it, congratulate them on being the families first ever digital security agent (you could even give them a codename).

Do some security investigating online together, show them how to create strong passwords, make a game out of it and tell them how much more grown-up and better prepared they are than other kids their age and while you are doing it, you may even learn something yourself.

PASSWORD SECURITY

Better locks & smarter keys

Passwords are the keys to your digital world, we need them to access everything from bank accounts to email. They can be inconvenient, but they're vitally important if we want to keep our information safe. Here we discuss some ways you can secure your accounts by choosing better, stronger passwords.

Passwords are an easy to understand, simple to use and low cost security measure. They have become the standard way we manage our security online and the way we prove our identity, not only to the corporations we do business with every day but also to our friends and family when we communicate with them through email and social media.

In the days of, for instance, face-to-face banking, we would have relied on a combination of our signature, photo I.D., account number and, often, a personal familiarity with the member of staff behind the counter to validate who we are, in the internet age we are exclusively known by just two things; a user name and password.

And it is the success of this two-factor procedure, user name and password, which has made the system so vulnerable. The fact that we need a password for every single account, profile, app and log- in, along side the requirement for increasingly complex passwords has led to what is commonly called 'Password Overload'.

The demand on most users is, quite frankly, unrealistic and many users will cope by breaking the cardinal rules of password management; re-using passwords across multiple sites, using the simplest, shortest passwords they can and making their passwords childish and easy to guess below).

How do passwords get hacked?

There are a number of common techniques hackers use to crack your passwords,13 many of them rely on simple, easily available, pre-written software that you do not need any special skill to use. Having said that, there are also many ways we make ourselves vulnerable with poor password 'hygiene'.

Cracking your security questions: Many people use the names of family, pets, age, birth date, favourite colour/song/sport stars and celebrities as a basis for their passwords. If you have posted information about any of these on social media you are at risk of having your accounts hacked.

Using simple passwords: The worst thing you can do is to be among the users of the 10 most commonly used passwords. Using passwords under 10 characters, without any combination of upper case letters, special symbols (like *&^%$£@) or numbers is putting your security at risk. One of the main reasons that we do not change our passwords to something much more complex and challenging is that nothing bad has happened to us... yet. Even if we get our email hacked mostly we just change that password and go on as before. Do not wait until real damage has been done to take action.

Reusing passwords: It is hard making and remembering a different password for your email, banking, social media and shopping but remember, if you use the same password for all of them then if one of these gets hacked they all do. Using one password for everything means you could lose it all.

What can you do about it?

Nothing is impossible to hack but you can make cracking your security as hard as possible by following these 10 points:

1. Make sure you use different passwords for each of your mobile money, social media, bankcards and other online accounts.
2. Consider using a password manager. They can generate, record, encrypt and store password information for all the websites you use and help you log into them automatically. Accessed with a master password it means you only have to remember one, secure password and the manager will do the rest.
3. Check the strength of your chosen code by using a reputable password strength analyser website.
4. Never enter your passwords into public or shared computers like Internet cafés or at the library.
5. Equally, never enter your password if you are using an unsecured, public Wi-Fi connection.18
6. Change your passwords regularly and do not ever reuse a password or base a new password closely on an old one.
7. Do not tell anyone your password. Ever.
8. Use at least ten characters of mixed lower case, upper case, numbers and special characters. Mix the numbers up with the other characters, do not string them all out together at the beginning or end of you password. Try to create your password with the maximum number of characters allowed by each site, the longer the better.
9. Never leave your device unattended and logged-in. 10. Make sure you are never watched when you enter any of your passwords.

CYBER CRIME

Be aware, stay secure

From organized criminal gangs to covert surveillance and even hacks by foreign nations criminal elements seem ever- present and ready to exploit any weakness in the new and emerging areas of communication and data storage. Most of us use the internet without any problems, but anyone can fall prey to cybercrime if they fail to take basic security precautions.

Activities that at first glance seem completely harmless such as using email applications, searching the internet, downloading les, playing games and signing-up to new websites and services can all leave your computer or mobile device vulnerable to infection from viruses or spyware leading to data loss, identity theft and even serious fraud.
The best line of defence against becoming a victim of this kind of attack is to be as aware as possible of the tricks and techniques cybercriminals use to try and get access to your computer; because the only way they can get in is if you let them.

Gone phishing

Phishing is an attempt, usually through email, to gather personal information or to compromise technology for the purpose of financial gain or malicious activities. Phishing emails typically include a link to a fraudulent site or an attachment containing malware, clicking on the link or downloading the file will activate the program.

Every day millions of phishing emails are sent out to unsuspecting victims all over the world. Some are easy to detect as frauds but others are very convincing. How can you tell a real email from a scam? Below we have collected six ways you can spot a potential phishing email:

1 . The message has a suspicious or mismatched URL

If you are at all suspicious check the integrity of any embedded URLs. The URL in a phishing message may seem to be perfectly valid but if you hover your mouse over the top of it you will see the actual hyperlinked address appear. If the hyperlinked address is different from the address that is displayed, the message is probably fraudulent.

2 . The message has poor spelling or grammar

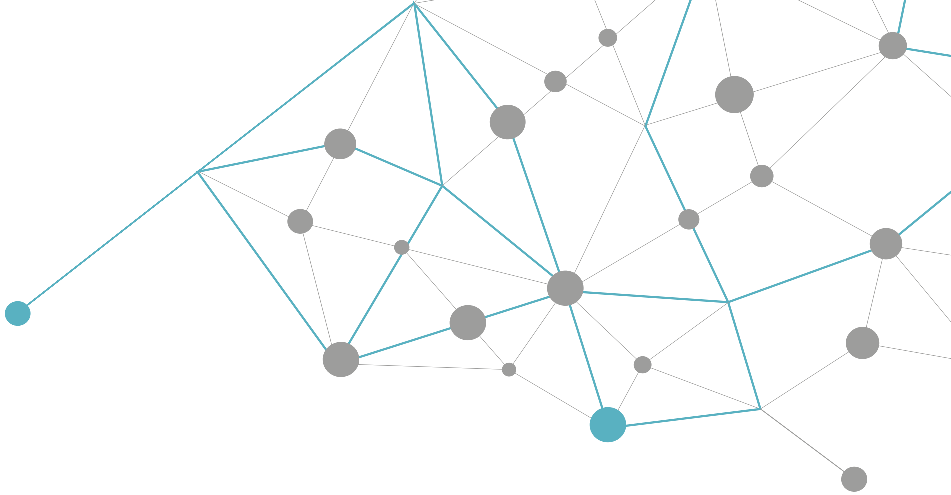
When a major organisation sends out a message it is usually checked for spelling, grammar, and legality, if a message is filled with spelling mistakes it probably did not come through a major corporation's legal department.

3. It asks for personal information, especially passwords

No reputable company will ever ask you to send or confirm, passwords or log-on details via email. Either, the company already knows this Information or it is a scam, there are plenty of other ways they can confirm your identity.

4. It lacks a personal greeting or any customised information

Legitimate emails from banks, credit card company's and other security conscious organisations will often include partial account numbers or user names as forms of address. Greetings like 'Dear User' should ring alarm bells.



5. It is an emergency

Messages that say you must act now to avoid losing money or having your access cut off are usually trying to get you to act without thinking. Take your time and investigate, double check the hyper-link and use an alternative way (call a known number, pay a visit, go to the web page by typing it in manually etc) to contact the sender.

6. Something just seems 'wrong'

Maybe it is the slightly off logo or the odd way the message is worded but sometimes things just do not quite seem right, learn to trust that feeling. The truth is, the best defence we have against fraud is our common sense.

If in doubt, throw it out

The best thing to do, if you have any doubt at all about the legitimacy of an email, link or attachment is simply to delete it. Do not open it, forward it or save it to show someone later, it is much, much better to be safe than sorry. So, phishing is the most common way a criminal can get you to infect your own computer or steal your private data. Once they have done that what else can they do? One thing might be to launch a ransomware attack:

Digital hijacking

Ransomware is an increasingly popular method hackers are using to make money out of you. It is a digital blackmail and it comes in two types:

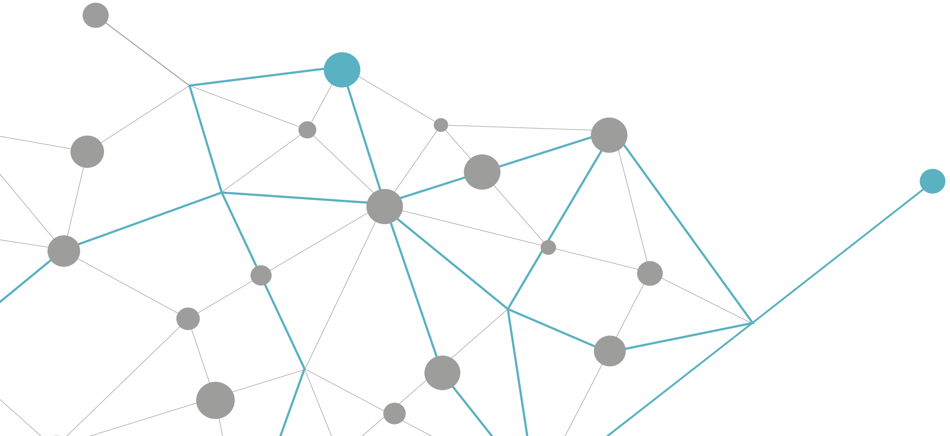
Lock screen ransomware

Locks your screen with an image demanding payment and displaying payment details.

Encryption ransomware

Encrypts all the files on your hard drive (also on network drives, external hard drives, USBs, and even cloud storage), preventing you from opening them and demanding payment to regain access.

Occasionally the ransomware virus will also send the user a message purporting to be from a law enforcement agency stating that illegal online activity has been detected and the payment is a fine to avoid arrest.



What you can do

There is no guarantee even if you do pay the ransom that you will ever get your files back. It is not like you can complain to anyone if the criminal does not keep their end of the bargain. It is also increasingly likely these days that the person contacting you has simply bought a ransomware virus from a professional criminal programmer and does not even know how to restore your data to you, even if you did pay.

You should face the fact that your data might be irretrievable although it is always worth seeking professional advice from a reputable computer specialist to see if your computer can be repaired and your data retrieved.

Keeping your most important and personal files backed up on a removable external storage drive is the only way you can be sure your data is safe.

What you can do

There are things you can do to reduce the likelihood of an attacker being able to hijack your system:

Firewall

Install a firewall and configure it to monitor and control traffic coming into and leaving your

Be watchful

If you notice that your Internet connection is very slow, use a system tool to check the amount of traffic your modem is handling.

If it seems very high and you are not downloading or uploading anything, that might well indicate you are part of a Botnet.

Internet
attack
protection
Mobile
devices
Compute
Internet
Cyber
security

Trusting Technical Support

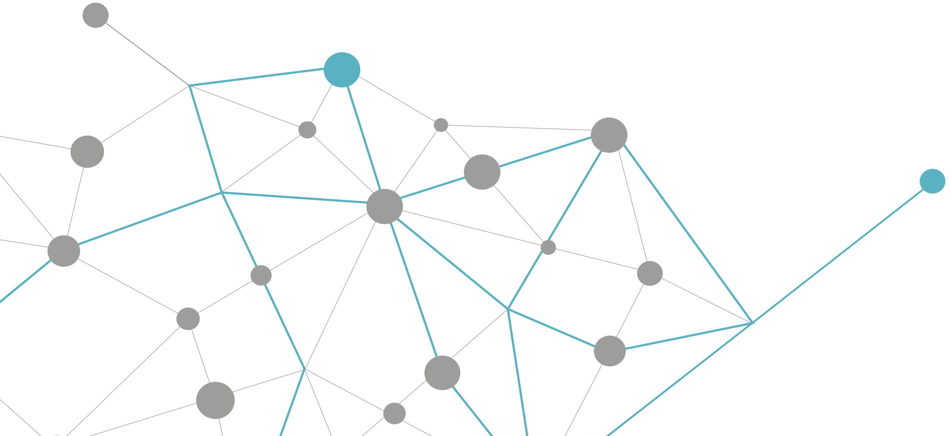
Some fraudsters will even impersonate your internet service providers' technical support department. They will tell you they need you to give them remote access to your computer so they can remove malicious les or software they have identified.

If you have not contacted your internet service provider or computer help desk you can be sure that an offer like this is fraudulent.

How the scam works

Hackers use your Internet Protocol (IP) address to identify your Internet Service Provider. Once they know who supplies your broadband connection it is a simple matter for them to pretend to be legitimate technical support from that company.

The fraudulent technician convinces you, either by communication windows on your screen or via a phone call, that they need to take control of your machine in order to delete infected files from your system. If you give them access they will instruct you to make a payment to remove the allegedly malicious files.



What you can do

Never give remote access to anyone you have not specifically requested to work on your machine.

Ignore the technical support window, close it and/or put the phone down. Call your Internet service provider directly using a number you are familiar with or have used before and explain the situation.

If you have allowed remote access your system is probably compromised. If that is the case you should disconnect the device, reinstall your operating system or take it to a reputable computer support service to have the system reinstated. Keeping thorough backups of your data will greatly help here.

Fraudulent phone calls

It is not just 21st century, cutting edge technology that cyber criminals use to get hold of your security information, the telephone is as popular with criminals now as it has ever been. Known as vishing (voice-phishing) fraudsters will call and pretend to be from your bank, to warn you of suspicious activity in your account, your cable company or even from the police force claiming you have been the victim of bank card fraud. All with the aim of relieving you of your account details and passwords.

Be particularly vigilant if:

Someone calls to tell you your bank card has been used fraudulently. A caller suggests you hang up the phone and call them back to verify they are genuine; criminals can keep your phone line open by not putting down the receiver at their end making it seem you are through to the security number you dialed. Someone asks you to transfer money to a new account, even if they say it will be in your name.

What you can do

Never feel pressured into doing something that makes you feel uncomfortable. If something seems wrong stop and take a moment. And never be afraid to just put the phone down, be polite, but be firm.

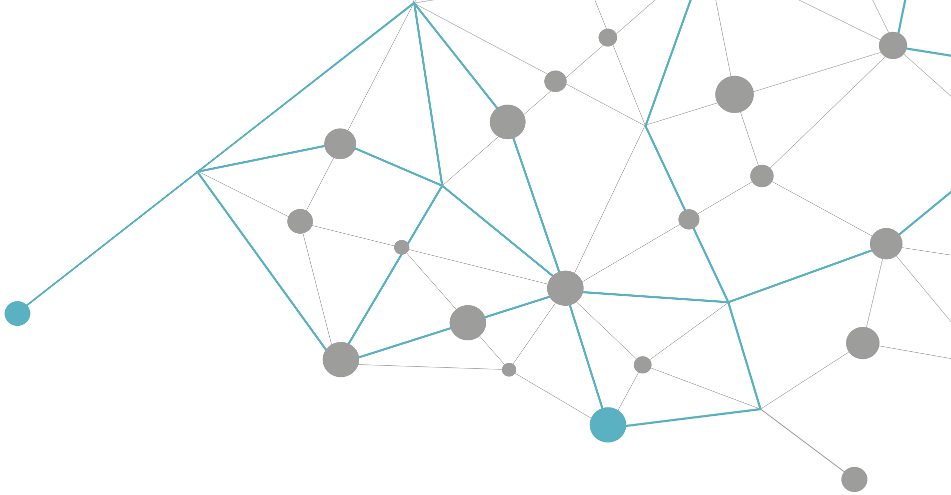
WORKING TOGETHER

Employers these days are more and more dependent on their information systems, gathering, storing and using ever increasing amounts of data. They have a responsibility to their staff to be open and honest about what kind of material is being collected and how it is being stored, while employees have a responsibility to ask; how can we all help to keep our data secure?

We all have the right to work in an environment that is safe and secure, both physically and digitally. Creating that kind of culture is not just down to adhering to departmental policies, it is a state of mind.

Balancing the risk

Wherever there are people there will be risk, that is just how it is but there is, and always must be, a balance between risk and freedom. If you cannot keep your data safe then you are not a fit company to do business with, but you need to make sure that the security processes put in place are there to help, not hinder. Knowledge must be able to flow, you need to be able to respond to situations in a fluid way. It is a balance. Here are some of the ways we can protect our data, our customers and each other.



Passwords

Do not tell anyone your work passwords, under any circumstances, ever. And that means not writing it down on a sticky note and attaching it to the front of your PC, OK? For more information see our section on Passwords.

Email

We have all done it, it sounds obvious (it is obvious) but that does not stop thousands of us doing it every day - try really hard to make sure that you are sending your email to the right person. Sending confidential or sensitive information out to someone we should not is one of the top ways we can embarrass ourselves and put our company at risk. Just take a moment to consider if the email should be encrypted and double check the recipient before hitting ‘send’. Also, do not use your work email for anything other than work; you will just get your in-box full of spam and increase the likelihood of a phishing attack.

Lock your screen

Whenever you leave your desk put your computer into sleep mode or activate the screen lock. That way, if someone wants to see what you have been working on they need your password (as long as it is not written on a piece of paper on the underside of your keyboard).

Taking work home

Check your organisation's policy on taking business files home. If it is allowed, make sure you encrypt the data before you remove it or put it on a password-protected drive so if it gets lost the information is still protected.

Report Lost or Stolen Devices

If you do lose anything with work related data on it, make sure you let the relevant department know as soon as possible. As awkward as it may be to admit it will be far, far worse if sensitive information gets into the wrong hands and your company is unprepared.

Think before you click

Be very cautious about downloading anything from the internet onto your work computer, especially 'executable' (.exe) files. It is almost impossible for you to tell if a file is what it says it is or if it is really harbouring a virus waiting to infect your business' system.

Engage with ZICT Information and Communication Technologies division of Zimbabwe Institution of Engineers

If your company has an IT or Information Security department go and see them. Ask what they are doing to keep your data secure and what you can do to help, and find out who you need to contact if anything goes wrong so you are ready. Do not forget, ZICT are here to help you, one of them even wrote this book.

There is, perhaps, a tendency to think of them as, at worst, an enemy and at best an inconvenience but please try to remember; they are dealing with a brand new threat in a brand new environment.

We are the first organisation to deal with the dangers and the possibilities of the mobile money, card cloning and the internet, these services are new for all of us. Some of us are more comfortable with the changes it is bringing, others less so.

But, ultimately, this is the digital age, it used to be enough to make sure the windows were locked and the alarm turned on at night when you left work but it is not just money and equipment that can be stolen now, a business that loses it is data can lose its customers, its reputation, everything. It is a 21st century workplace, let us engage with it together.

CYBERSECURITY FOR EVERYONE

STAYING SAFE

A little effort goes a long way
The Internet… it is not the Wild West, it is not the Haunted Forest; there aren’t trolls under every bridge and bandits in every canyon. What we’ve just been talking about are some of the worst-case scenarios so please, do not close this book and swear never to go online again, just put some e ort into thinking about and updating your security. We promise it is time well spent.

Following a few sensible procedures will greatly reduce your chances of ever being the victim of cyber crime or identity theft.26 Many criminals are looking to do the least possible work to get the maximum gain. In just the same way a household that leaves it is front door and windows open is far more likely to be robbed than one that’s sensibly locked, a computer or account protected by a few smart security procedures is a much less attractive target to a hacker than one without. The lesson is: let’s not make it easy for them…

Protect your devices
Keeping your operating system, apps and web browser up to date is one of the easiest and most effective things you can do to keep safe.

Make sure you turn on the automatic update feature to get the latest versions of operating systems and security patches.

Protect your data

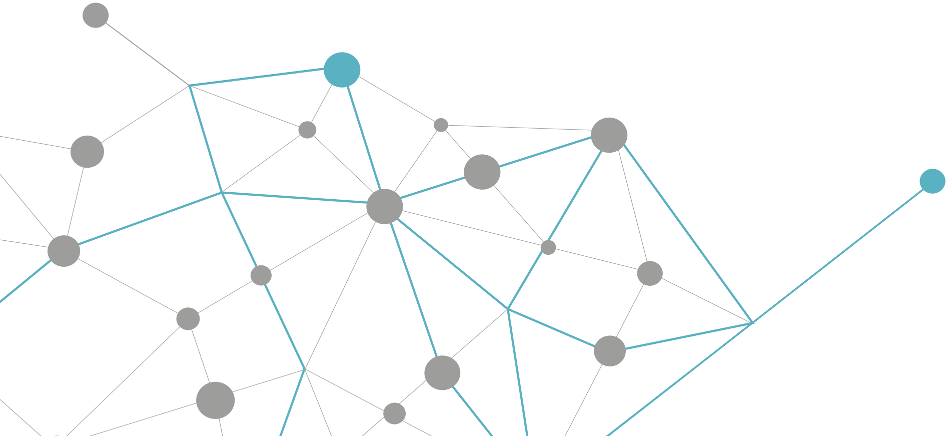
Use intelligent passwords and keep different passwords for separate accounts - check the 'Password Security' section of this book for more.

Only send information over a secure connection, look for the **https://** or padlock icon in the address bar when you are sending any sensitive information like credit card details. If you do access password protected accounts or sites on a public or shared computer remember to sign out and close the browser window when you're done.

Install some protective software, preferably a security suite which includes antivirus/malware and firewall components.

Do not share too much

Think about how you use social media; set privacy and security settings and consider what a criminal could do with the information you post. See the 'Using Social Media' pages.



Do not get hooked

Beware of phishing; links in emails, tweets, bogus websites and too-good online offers are all ways hackers will try to steal your personal information. Learn to be suspicious and do not be afraid to delete something if it feels 'off'.

Back it up

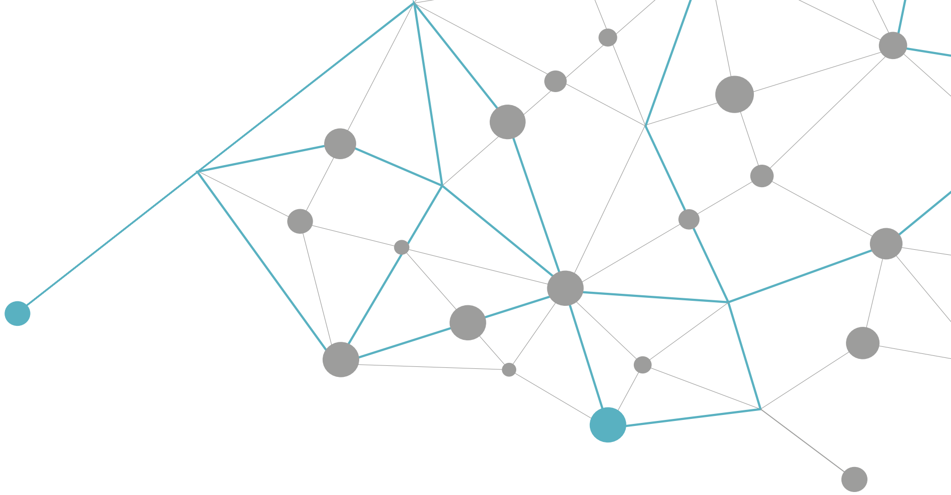
It might sound annoying but regularly backing up all your irreplaceable photos, work files and other digital information onto a removable drive will ensure they are protected, no matter what happens to your hard drive or cloud account.

Be prepared

If the worst happens, have a plan. Keep a real, pen and paper copy of the emails, phone numbers and addresses of your friends and contacts in case your identity and accounts are compromised. Make sure you know the correct numbers to cancel credit cards and freeze bank accounts and find out the names and numbers of the relevant fraud or law enforcement departments so you can limit the amount of time a criminal has free access to your finances.

Think before you act

Many scams rely on us being too eager to take advantage of a super special, one-time-only, limited, low price offer. These too- good-to-be-true frauds often hide a malicious intent. Try to learn
how to see through them. Read about how others have been scammed and what tipped them off, remember, we would all like a free holiday and an iPad but the chances of getting one by filling in an online form are non-existent. It is a scam.



Lastly...

Just because the online world is digital doesn't mean it is not real. It is made up of real people with real lives and feelings.

It can be easy and exciting to get swept along with the crowd sometimes but what happens online matters and can have genuine and lasting effects on everyone involved. Always treat others as you would like to be treated. Be kind, be aware and stay secure. Thanks for reading.

If you need any assistance do not hesitate to contact us on cyber@zict.org.zw

Telephone: +263772278161, +263 4 746716
Physical address: 256 Samora Machel Ave. East, Eastlea, Harare, Zimbabwe