CITY OF CAPE TOWN
ISIXEKO SASEKAPA
STAD KAAPSTAD

CYBER SECURITY
STOP. *THINK.* VERIFY.

CYBER SECURITY

This booklet explains the importance of cybersecurity and why it is vital to protect yourself, and your information, online. It also highlights different types of digital risks and threats, and provides advice and useful tips for staying safe online.

Making progress possible. Together.

smartcape

The SmartCape program's objective is to increase the digital capacity of City citizens to close the digital divide through digital literacy programs occurring concurrently throughout the city. **Scan QR code for more information.**

smartcape

Contents

WHAT IS CYBERSECURITY?

Cybersecurity is all about protecting your information and that of the company you work for against damage, theft and unauthorised access. Information security protects information in all forms, whether digital, paper-based or physical.

Technology has become a major part of everybody's daily life. We use smartphones, tablets and computers at home and at work; kiosks at City libraries, the movies and malls; and children and students use educational tablets at schools, colleges and universities.

With more and more people having internet access through 5G devices and networks at home, and internet usage on the rise, large amounts of personal information are being stored on devices and social media.

What information must be protected?

- Information stored on your devices, such as your smartphone, tablet, laptop and computer.
- Information you provide via online platforms such as Facebook, Instagram, Gmail and X (previously Twitter).
- Information you provide via apps such as WhatsApp and Snapchat.
- Information you have in tangible form, such as your ID, passport, birth certificate, marriage certificate and academic reports.

How to protect ALL your information

- Make sure that your passwords are difficult to guess.
- Never share any passwords with anyone.
- Recognise the signs of a scam or an attempt to steal your information.
- Know what to look out for to ensure that you are safe when doing internet banking.
- Be careful what you share on social media sites.
- Understand how cybercriminals work, and the crimes they commit.
- Have tools such as antivirus software installed on your devices to automatically protect your files.
- Keep your devices and antivirus software updated.

Why is the City of Cape Town taking cybersecurity seriously?

Keeping up with technology, the City offers a host of e-services to the residents of Cape Town, including emailed rates statements, online renewal of vehicle licences, etc.

Just like cybercriminals attempt to fool bank clients, some may try to trick residents by sending messages that appear to be from the City.

In line with its Integrated Development Plan (IDP) and good governance practices, cybersecure behaviour is important to the City. Therefore, it wants to inform all residents of best cybersecurity practices that offer protection against cybercriminals.

The City values are caring; accountability; openness and transparency; innovation; and service excellence. We all strive to be safe and that includes being safe online, whether using the City's e-services or other online portals and applications.

A caring city aims to have its residents' information protected. This includes their account information, personal information, profile details, email addresses and mobile numbers.

PASSWORDS

Passwords are used to protect your information, so it makes sense to choose a strong password that is difficult to guess. The more complex your password, the better the protection.

Remember, as soon as someone knows your password, they can log in and gain access to all your files, information, emails and other messages, and can also send messages on your behalf. When this happens, you have been hacked. To prevent being hacked, choose the strongest possible password.

Have a look at these useful tips regarding passwords:

- Make sure that your password contains both upper- and lowercase letters, numbers and special characters.
- A stronger password is a longer password. Try remembering a sentence and then replace some of the letters with numbers.
- Never share your passwords with anyone, ever.
- Set up reminders to change your passwords every month.
- Test your password strength at www.passwordmeter.com.
- Use different passwords for different sites. Choose a sentence or 'pass phrase' that relates to each specific website or service, so that it will be easier for you to remember.
- Change passwords as soon as you suspect that they have been compromised, or if you think someone else might know what they are.
- Have a parental lock on your devices or any websites unsuitable for kids.

Multi-factor authentication (MFA)

The purpose of MFA is to make it more difficult for an unauthorised person to access your accounts and data. It allows online services to verify that you are who you say you are.

MFA is a cybersecurity measure that requires users to verify their identity through multiple factors before being able to access a network or system. The user must provide a password, verify access by entering a code sent on another device, or confirm access with biometric data such as a fingerprint.

MFA should be implemented for these platforms or services:

- Cloud accounts, e.g. Microsoft Teams
- Email accounts, e.g. Gmail
- Financial services, e.g. ABSA, FNB
- Social media accounts, e.g. WhatsApp
- Online stores, e.g. Takealot
- Gaming and streaming entertainment services, e.g. Netflix

Authentication factors are ways of confirming your identity when you sign in on an account or app. For example, a password is one kind of factor – something you know. The three most common kinds of factors are:

- **Something you know** – such as a password or memorised PIN.
- **Something you have** – such as a smartphone or secure USB key.
- **Something you are** – such as a fingerprint or facial recognition.

Privacy

Privacy is a human right. This includes the right to:

- keep our personal information to ourselves;
- be free from any interference or intrusion; and
- have control over how our personal information is collected and used.

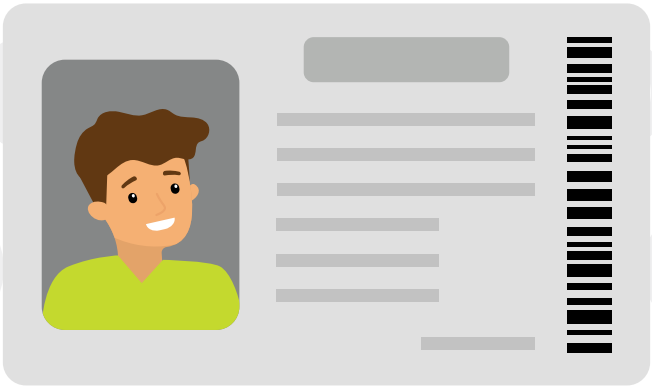
Personal information

The definition of personal information in the Protection of Personal Information Act (POPIA) is broad and extends to various types of data. Information that relates to an identifiable living natural person or juristic person (such as a company) qualifies as personal information. It includes all information about a person, their characteristics and identifying information, and extends to all confidential correspondence about the person or in reference to the person.

These include:

- Race
- Gender
- Age
- Income
- Mental health
- Sexual orientation
- Religion
- Marital status
- Biometric data
- Education data

Basically, personal information is anything that can identify someone.

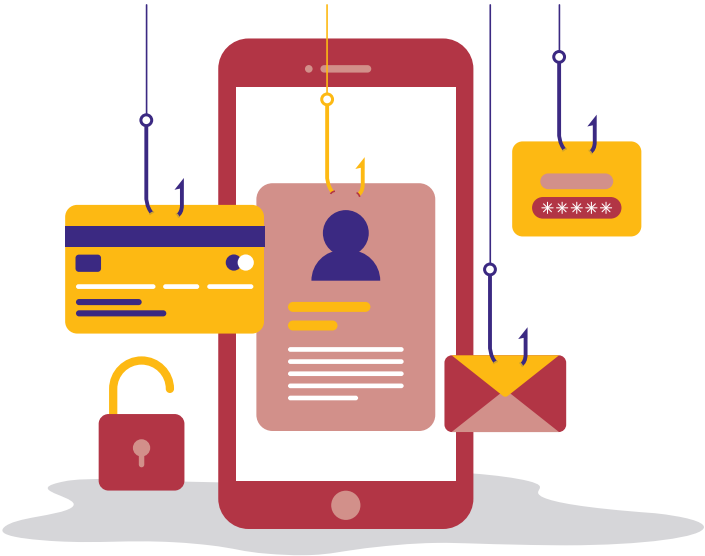


PHISHING

Phishing is the name of a particular type of email scam. Phishing is so popular with criminals that everyone with an email address will probably at some point be subjected to it.

The scam entails an email sent by a criminal to your email address, pretending to be from your bank, SARS or any other credible agency. The message is always urgent, often written in poor English, and includes a link for you to click on and follow instructions.

The link goes to a website that looks very much like the real thing, yet it is not. As soon as victims enter their usernames/passwords, their information is stolen, giving the criminals free access to log in as they please. Although many people still fall prey to this practice, it is easy to avoid.



How to protect yourself from a phishing scam

- If you are concerned about an email message, pick up the phone and call the service provider to verify.
- Do not click on web links in suspicious-looking messages.
- Verify the legitimacy of the website:
  - Do some research on the website by searching for it on Google, checking reviews and looking at the English grammar used.
  - Suspicious websites will often contain advertisements that take up the entire page, require that you take a survey or redirect you to another page, or even show explicit or suggestive ads.
  - Secure websites will have 'https' in the URL bar.
  - Avoid giving permissions to the website for notification, location, etc. unless really required.

SCAMS

Scams are when criminals or people with bad intentions try to trick you into sharing information that would enable them to gain access to your money and other property.

There are generally two types of scams, namely online scams and offline scams.

Online scams occur through emails, WhatsApp messages and websites. They are designed to grab your attention, such as a message that appears to be from SARS e-filing, or from a prince requiring a nominal amount of money to release a fortune.

Offline scams are more difficult to detect. They are often perpetrated by criminals pretending to be regular workers, business people in fancy suits, or just regular folk with the gift of the gab. These scams are often a bit more sophisticated, with criminals gathering intelligence, carefully selecting their target and using a specific attack technique.

Techniques include the following:

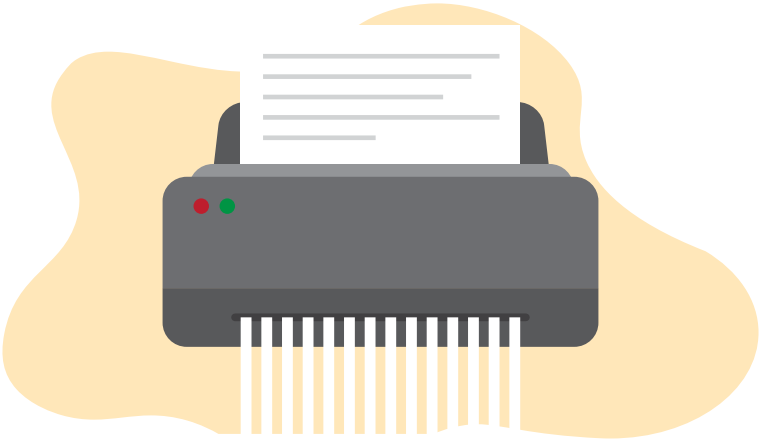
- **Baiting** (such as offering users free music or movie downloads if they provide their information).
- **Pretexting** (where attackers create a good pretext or false motive that they can use to steal their victims' personal information).

- **Sympathy attacks** (where the attacker pretends to need assistance to stay out of trouble or avoid losing their job, thereby playing on the victim's empathy and sympathy).

- **Ego attacks** (where the attacker appeals to the vanity or ego of the victim, who wants to prove how smart or knowledgeable they are, and then provides sensitive information in the process).

- **Intimidation attacks** (where the attacker pretends to be someone influential, using authority to coerce the victim into cooperation).

- **Quid pro quo** (promising a benefit in exchange for information, with the benefit usually taking the form of a service, whereas baiting uses goods).



So-called 'dumpster diving' is another common method of gathering people's information. Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network or on a person. People will search your trash to find information about you or even a company.

Therefore, always properly shred or destroy personal paper documents that you wish to dispose of. Do not simply throw them away as is – they may contain personal information about you and your family.

ONLINE BANKING

South African banks have evolved in terms of technology, and now offer their customers the convenience of transferring money, making payments and viewing their account balances online.

More and more people make use of this technology, conducting their financial affairs on the internet. Generally speaking, the systems are secure and use encryption. Encryption makes it extremely difficult for criminals to spy on you or steal your information. The only potential weakness is your username, password or PIN. These are the 'keys to the kingdom'.

The following tips will help make your online banking and ATM experience more secure:

- Enable SMS notifications on all your bank accounts. Set strict daily limits on transfers and withdrawals.
- Review your statements at least once a month.
- Block accounts if you suspect fraud, card theft or card cloning.
- When card machines mysteriously disconnect after you have entered your PIN, beware. Always ask for the slip and check for duplicate transactions, in which case vendors must reimburse you.
- Never let your card out of your sight.
- Shield the keypad when entering your PIN.
- Never accept assistance from strangers at ATMs.

Only use online retailers that you trust.

CYBERCRIME

Cybercrime is crime that is carried out by means of a computer. While most of the internet can be searched using search engines such as Google, there is a part of the worldwide web that these engines cannot access. This is called the dark web, where organised crime, syndicates and illegal activity thrive.

Common types of cybercrime include:

- Hacking
- Piracy
- Child pornography
- Drug trafficking
- Online casinos
- Phishing and other scams
- Online prostitution
- Crimen injuria and cyberbullying
- Cyberterrorism
- Human trafficking

These crimes are all committed using the internet and occur on a massive scale in certain countries and circles.

How to protect yourself from cybercrime

- Always add extra security to your internet experience on sites such as Facebook and Gmail (e.g. two-factor authentication).
- Do not infringe, or encourage the infringement, of copyright on movies, games and TV shows.
- Do not get involved in illegal activities online or offline.
- Do not click on links in emails from people you do not know – these emails may be a phishing scam.
- Do not open attachments in emails from people you do not know – this could result in ransomware downloads.
- Do not participate in racist, hateful or discriminatory speech or messaging.

How to report cybercrime

Should a crime be committed at your place of work, consider contacting your human resources department. Some companies also have a whistleblowing system that allows you to report a crime while remaining anonymous.

Contact the South African Police Service (SAPS) Crime Stop (tip-off line) on 0860 010 111.

CYBERBULLYING

Gone are the days when bullying only happened on the playground during school hours. Today, bullying can occur 24/7 on the internet. This means non-stop harassment, name-calling, degrading comments and insults. Statistics show that children as young as ten commit suicide due to cyberbullying.

The situation is dire, and many schools now actively raise cyberbullying awareness and have customised programmes to assist learners.

Cyberbullying also affects college and university students, as they increasingly use social media.

But this phenomenon is not limited to school learners and students. Everyone is in danger of being intimidated, harassed, defamed or threatened online. When involving adults, cyberbullying evolves into what is known as crimen injuria – unlawfully, intentionally and seriously impairing another person's dignity.

Remember that nobody should tolerate bullying, intimidation or harassment of any kind.

Examples of online bullying and harassment include:

- Spreading degrading rumours about someone online.
- Sending constant emails to a female colleague about her body.
- Intimidating a colleague to obey your instructions.
- Blackmailing people by sharing nude photos of ex-partners with a threat to post online if they do not pay.

Computer viruses have been around since the beginning of computers. A computer virus is any software with malicious, or bad, intent and is often called malware. The range of viruses that exist is vast, but the most common types are listed below.

Common types of viruses

- **Virus:** Often infects programs and executes when a user launches an infected program.
- **Worm:** A very common type of malicious software that can spread through computer networks without any user interaction.
- **Ransomware:** This encrypts your data until you pay up to get the unlock key.
- **Trojan horse:** A type of malicious software that disguises itself as a normal file or program to trick users into downloading and installing it.
- **Rootkit:** A type of malicious software that is designed to remotely access or control a computer without being detected by users or security programs.

- **Bot:** A software program with built-in intelligence that can operate autonomously and automatically. A 'botnet' is a network of bots working together, and can be very dangerous for computer networks and systems.

- **Adware:** These are automatic adverts that pop up on your internet screen and may contain spyware.

- **Spyware:** This is a type of malware that functions by spying on the activity of users without their knowledge. It can monitor activity, record screen videos, collect keystrokes and harvest data such as account information, logins and financial details. Spyware can also modify the security settings of software.

How to protect yourself from viruses

Install antivirus software

It is easier than you may initially think, and does not have to cost you hundreds of rands. Free software is available and does a very good job.

Examples of free antivirus software are:

- AVG
- Avast
- Microsoft Defender
- Microsoft Security Essentials

Update your device

Criminals never quit and continuously try to find loopholes to enter computer systems. These loopholes are called vulnerabilities, and creators of computer software such as Microsoft are hard at work to plug these vulnerabilities with patches.

Certain software creators regularly release patches and security updates. When they are released, it is important to install them to stay protected against viruses.

At your place of work, your computers are most likely patched automatically. At home, you are responsible to ensure that your devices are kept up to date in terms of patches and security updates.

Remember, criminals are on the lookout for loopholes or vulnerabilities to get into computer systems and devices – do not let it be yours. Stay protected.

Ransomware is a type of computer virus and is so dangerous that it deserves its own chapter.

What is ransomware, and how does it work?

Ransomware is any software that tricks someone into encrypting their own device, which criminals will then unlock in return for large sums of money. Criminals usually send ransomware using email attachments.

The email subject is normally designed to entice people into opening the attachment. Some examples of subject lines include:

- 'Delivery pending'
- 'Invoice attached'
- 'Your package is waiting'

These emails almost always contain an attachment, which may be a simple text document. This, however, is the trick – the attachment is ransomware, and opening it will launch a program that immediately encrypts your entire device.

Encryption scrambles all the information on your device, holding it 'ransom' by making it unreadable to anyone without the unlock key. In this case, only the criminals have the key, and to get it, you will have to pay.

How not to fall victim to ransomware

It is simple. Never open attachments from people you do not know, or messages you were not expecting. Fight the urge to click and open suspicious attachments. Remember, for the trick to work, criminals rely on your curiosity.

Criminals never go on holiday – always remain vigilant!

Ten computer ethics guidelines

Using the Computer Ethics Institute's publications (Ten Commandments of Computer Ethics – COMPUTER ETHICS INSTITUTE) as a guideline, we explain the ten rules of computer ethics in more detail below.

1. Do not use a computer to harm other people.

If you use your computer to cyberbully, harass and attack people's characters through emails, online chats and/or social networks, your computer use is harmful to others. Computers also control many mechanical devices, and manipulating this equipment may lead to physical injury or death.

2. Do not interfere with other people's computer work.

It is unethical to generate or consciously spread programs designed to disrupt other people's computer work by destroying files, taking up huge amounts of computer time or memory, displaying annoying messages or stealing information (through malware).

3. Do not snoop around in other people's files.

Reading other people's email or text messages is as bad as opening and reading their snail mail. This is an invasion of privacy. Obtaining other people's non-public files should be judged in the same way as breaking into their homes and stealing their documents. If your colleagues do not lock their workstations, do not regard this as an invitation to meddle with their computer files.

4. Do not use a computer to steal.

Using a computer to break into the accounts of a company or bank, to transfer money, is robbery. Stealing money, identities, information or software is not only unethical, but also illegal, and is a form of computer crime. Theft is theft, whether in the physical or digital world. While bank robbers of yesteryear are still around, many nowadays find it far easier to use computers rather than guns and masks.

5. Do not use a computer to spread lies.

Spreading lies, rumours and hoaxes via the internet is extremely easy. Yet spreading false information about people, events, groups or anything else is wrong. Lying about yourself in an online chat is unethical. In general, this rule ties in with the principle of being honest at all times.

6. Do not copy or use proprietary software for which you have not paid.

Just as photocopying a copyrighted book is wrong, so too is copying copyrighted information in a digital format. Software is an intellectual product. Software piracy in the form of illegally copied software, games, movies and music amounts to billions every year.
Piracy is unethical and a form of computer crime.

7. Do not use other people's computer resources without authorisation or proper compensation.

Cracking a system is wrong, unethical and illegal. Just as breaking off the lock to a gate is wrong, so is bypassing authorisation, cracking passwords and circumventing security controls on a computer.

8. Do not misuse other people's intellectual output.

An intellectual output could be defined as any piece of work, whether text, data, images, sound or performance. It would be wrong and unethical to take a colleague or friend's work and pass it off as your own. Just because the material is not copyrighted, does not make it right to do so. This is called plagiarism. Just as plagiarism is wrong, so is using another person's intellectual property as if it is yours. When using images, written works and the creative outputs of others, give credit where credit is due by referencing their work appropriately. Consider the time and effort it takes to develop a piece of work. And violating the copyright on material such as games, music, movies and software is of course an offence.

9. **Think about the social consequences of the program you are writing or the system you are designing.**

This rule focuses specifically on software development. Writing software with harmful intent is unethical (malware). Developing software to control the timing of an explosive or changing traffic light signals with the intent to cause injury is wrong.

10. **Ensure that your computer use always shows consideration and respect for your fellow human beings.**

Just be nice! The fact that you cannot see the people you are interacting with does not mean that you can disrespect and be rude to them. Having respect for your fellow human beings is the right thing to do.

The principles:

1. **Lawfulness, fairness and transparency:** You should always process personal data in this manner. There must be full transparency in the collection and processing of data and it must be used only for the purpose that the user agreed to.

2. **Purpose limitation:** Data should only be collected and processed for a specific and lawful purpose.

3. **Data minimisation:** It must be ensured that only the minimal amount of data that is truly needed is collected and processed, and nothing more.

4. **Accuracy:** All personal data must be kept up to date and measures should be in place for correcting and updating any inaccurate data. If you are not keeping, or it is not necessary to keep, your database up to date, you should delete outdated and inaccurate data promptly.

5. **Storage limitation:** Data must not be kept for longer than needed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest or for scientific, historical research or statistical purposes.

6. **Integrity and confidentiality:** Adequate security controls must be in place to ensure that the data are protected against loss, destruction or damage.

7. **Accountability:** Appropriate measures and records must be in place to prove compliance.

This booklet is available online.
Scan the QR code below:

www.capetown.gov.za

CITY OF CAPE TOWN
ISIXEKO SASEKAPA
STAD KAAPSTAD

Making progress possible. Together.