MARCH **2024**

THE FOCUS

CYBER SECURITY

Use this guide *to protect yourself and ICASA against cyber crime. Make sure you know what to do when you recognise a red flag*

www.icasa.org.za

BEWARE!

THE CRIMINAL HAS ALSO GONE DIGITAL

You rely on digital technologies to do your work. Criminals rely on digital technologies to steal your information.

To a digital criminal, information is more valuable than a TV or jewellery.

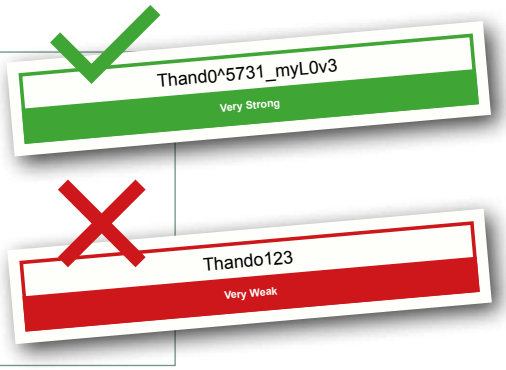
If you suspect that you are being targeted by cyber criminals, please contact **helpdesk@icasa.org.za** as soon as possible.

PROTECT YOUR PASSWORDS

Passwords provide a simple and effective way of protecting unauthorised access to data and systems.

Research has shown that most people use the same simple password for everything. **Don't be one of those people!** This can make you a target for cyber crime.

- Follow the organisational guidelines and procedures when you create your passwords.
- Try to make your passwords as complicated as possible.
- Never share your login and password with anyone.
- Change your password regularly.
- If you suspect that your password has been compromised, change it immediately.



PROTECT YOURSELF FROM PHISHING SCAMS

Phishing is the most prevalent form of cyber attack.

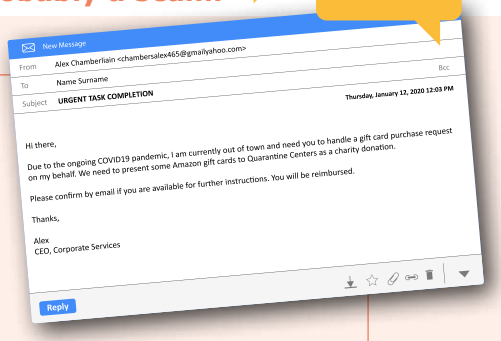
Attackers will try to send an email, SMS or whatsapp, or even try to call you from an obscure telephone number, to fool you into revealing sensitive information or giving them access to your computer.

- Never click on links or attachments from suspicious senders.
- Beware of common phishing language like "verify your account", "update your details", "claim your prize".
- Avoid sharing personal information before you are able to verify the identity of the person requesting it.
- When in doubt, ask someone who works in the IT department to help you identify fraudulent emails, messages and phone calls.

PROTECT YOURSELF FROM SPOOFING

In spoofing, which is also known as impersonation, cyber criminals pretend to be one of your work colleagues, or an official from a government authority like SARS. They try to trick you into initiating fraudulent payments or providing sensitive information that they can use to steal directly from company accounts.

When the request is urgent and is written in a threatening tone, insists on confidentiality and comes from an email address that is slightly different from the expected address, **it is probably a scam.**

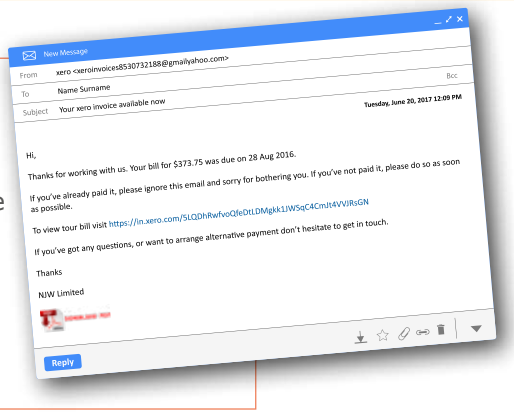


- Always follow the organisation's processes for authenticating payment requests and making payments.
- Be suspicious of urgent or unusual payment requests that are made at a time when it may be harder to confirm them.
- Double check banking details if the person who has contacted you gives you alternative banking details for a deposit.
- If the email has been sent from a free email address like SARS@gmail.com or accounts.icasa@yahoo.com, immediately treat it with suspicion.

ALWAYS VERIFY INVOICES BEFORE MAKING PAYMENTS

With invoice fraud, criminals rely on your trusting nature to try to fool you to pay fake supplier invoices.

This enables the criminal to **steal money from the organisation you work for**, and they involve you in the crime.



- Scrutinise the details of every invoice you receive to check if any of the details looks suspicious.
- Some suspicious details to look out for include figures in foreign currencies, incorrect reference numbers and typing mistakes.
- Never pay any invoice that does not have a corresponding purchase order issued by your organisation.
- When in doubt, query suspicious requests with your manager or the CFO.

AVOID CONNECTING YOUR WORK DEVICES TO PUBLIC WIFI HOTSPOTS

Open, unsecured public WiFi networks like those offered by restaurants, cafés and libraries can be dangerous because criminals can set up routers to provide free WiFi in public areas.

Once you connect, **they can intercept, capture, and divert all your communications.** That means criminals can access everything from your logins and company email attachments to the credit card information you enter on websites.

- Avoid public WiFi networks that don't require passwords.
- Pay attention to computer warnings that you are connecting to a network that hasn't been secured.
- If relaying sensitive information, consider using your mobile data network (dongle, portable modem or smartphone) instead of unsecured WiFi.
- Pay attention to who is around you when you need to key in passwords in public places.

WATCH OUT FOR SMS CONFIRMATION THAT YOUR NUMBER HAS BEEN PORTED

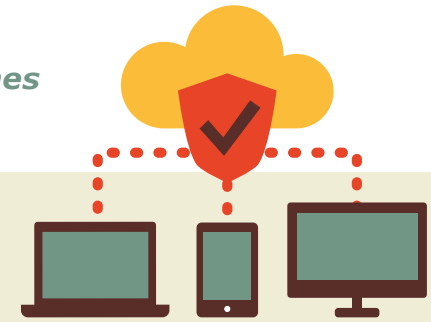
Cellphone companies will send out a notification, by SMS, before doing a sim swap. If you receive an SMS that warns your number is to be ported, do not ignore it.

It means that a **criminal is attempting to hack your number** in order to ask for money from your whatsapp contacts.

- If your phone suddenly won't connect to your mobile network and you are not in the middle of nowhere (or in an area being load-shed), assume your number is being hacked, and get in touch with your network service provider as soon as possible.
- Activate your whatsapp's security notifications, so that you receive a warning when a contact's security code has changed.
- If a "friend" asks for money shortly after their security code changes, be extremely suspicious.
- The best way to prevent your whatsapp number from being hacked is to enable two-step verification. This will require both a PIN and email confirmation before any changes can be made to your settings and so that no number-porting scam or other mechanisms will let someone steal your identity

PROTECT YOUR WORK DEVICES FROM CYBER ATTACKS

Confidential data is often lost or exposed through negligence or by accident. Sometimes a single click is all that is needed.



Security breaches caused by cyber attacks cost organisations millions of rands annually, and a significant percentage of those breaches involve human errors.

There are several different ways that a cyber criminal can gain access to your computer. One of the most common methods is through unsolicited email that might include attachments, or contain links to malicious websites.

- When browsing the internet, avoid accepting pop-up messages or prompts without reading them first.
- Never believe messages that tell you that you have won a prize.
- Avoid downloading "free" movies, games or music. These usually contain spyware that can give criminals access to your devices.
- Never download software from unknown sources.
- When in doubt, ask your IT support team whether it is safe to do so.
- Always follow the organisation's policy and procedures for handling data and using devices.
- In email, be cautious about using CC; BCC; Reply All and Forward.
- Never click on any links contained in an email if the sender is from outside your organisation or uses a free email address.
- Immediately report the loss of any device that might contain or can access the organisation's data to the IT department.

CYBER CRIME:

is the crime that involves the use of digital devices and computer networks (like your company network or the internet).

CYBER SECURITY:

is the practice of protecting digital devices, networks and important information from cyber crime attacks. It requires the people who use these technologies to be vigilant at all times and to report any suspicious that they might encounter.