iTOO™

[MY]CYLUTION

INCIDENT RESPONSE GUIDE

We have compiled this guide to assist you in managing incidents covered by your **[MY]CY**lution policy.

Please keep this document in a safe place as it includes a range of scenarios, actions required by you and recommendations.

Not all modules listed below are universally included in every policy – always refer to your Policy Schedule to ascertain the specific package and modules featured in your policy.

This guide does not constitute legal advice.

INCIDENT RESPONSE LINE: 0861 555 771

Think Expert. Think iTOO

THEFT OF FUNDS

ACTIONS TO TAKE:

Report the incident to:

- iTOO on 0861 555 771
- Your bank or mobile wallet company within 48 hours of discovery of the incident. We will require written evidence that the bank and/or mobile wallet company is not reimbursing you for the Theft of Funds.
- The Police within 72 hours of discovery and obtain an A-1 statement and crime reference number.

Coverage offered by the [MY]CYlution policy (if applicable):

- Theft of funds resulting from unauthorised access due to hacking of your online bank account, credit/debit card or hacking of your mobile wallet by a third party.
- Direct and pure financial loss of your funds resulting from you being an innocent victim of phishing or email spoofing.

Recommendations:

- **Document collection for investigation:**
  - Gather relevant documents and information, including dates and times of the fraud.
  - Collect all correspondence, such as names, phone numbers, social media profiles, chats, or online interactions with the fraudsters.
  - Save website addresses and screenshots as well as any emails and email addresses, including full header information. (your specific email provider or a web search can describe how to capture header information.)
  - If credit cards were involved, include receipts or statements.
  - Record all forms of payment, including transfers, wire transfers, money orders, and relevant account information.
  - Safeguard your identity by changing passwords and blocking compromised cards or accounts.
- **Device security:**
  - Equip all devices with the latest antivirus and antispyware software from a reputable vendor.
  - Register for cell phone notifications from your bank to receive real-time alerts on account activities.
- **Cell phone security:**
  - Monitor cell phone reception loss which could indicate an illegal SIM swap. If suspected, promptly notify your bank.
- **Password protection:**
  - Ensure your PINs and passwords are entered discreetly to prevent unauthorized viewing.
  - If compromised, change your PIN and password promptly, either online or at a branch.
- **Secure banking environment:**
  - Refrain from conducting banking on public or unfamiliar computers at libraries, cafes, or hotels.
  - Avoid using unsecured Wi-Fi hotspots, ensuring your wireless network is encrypted before performing transactions on your private device.
- **Online banking safety:**
  - Do not access Online Banking through email links; type the address or use bookmarks.
  - Prevent illegal software downloads by setting up administrative rights.
- **Password confidentiality:**
  - Memorize your PINs and passwords; never share or write them down, not even with bank officials.
- **Software and email caution:**
  - Steer clear of downloading pirated software due to potential malware.
  - Log off immediately after online banking
  - Secure your PC against unauthorized access.
- **Email vigilance:**
  - Avoid clicking links or attachments in unsolicited or suspicious emails, which could contain viruses, spyware, or trojans.
  - Install a personal firewall on your PC to enhance security.
- **External device care:**
  - Be cautious with external storage devices like memory sticks and portable hard drives; consider password protection.
- **Personal information protection:**
  - Refrain from sending emails containing personal information like card numbers and expiry dates.
  - Install a spam blocker to deter phishing emails.
- **Software updates:**
  - Keep your operating system, browser patches, and antivirus software up to date on personal devices to detect phishing sites and malware effectively.
- **Phishing response:**
  - If you have responded to a phishing email, change your internet banking credentials promptly and inform your bank.

By adhering to these comprehensive security measures, you can significantly reduce the risk of online fraud and protect your personal and financial information.

IDENTITY THEFT

ACTIONS TO TAKE:

Report the incident to:

- iTOO on 0861 555 771
- The Police within 72 hours of discovery and obtain an A-1 statement and crime reference number.

Identity Theft happens when a person other than your Partner or Children illegally use your identity document or confidential information relating to your identity.

Coverage offered by the [MY]CYlution policy (if applicable):

- Costs to reapply for loan or credit applications which the credit provider rejected due to a bad credit rating.
- Costs to certify documents for law enforcement agencies, financial institutions, or credit agencies.
- Telephone calls and postage to amend your records and to reflect your true name or identity.
- Credit monitoring with identity theft education and assistance from established providers for up to six months.
- Costs to reissue the identity document which was used for the Identity Theft.
- Your expenses and Lost Income for time you take off from work to sort out the Identity Theft incident.

Recommendations:

- **Notify relevant parties:** Inform your bank, employer, and any other applicable entities about the identity theft incident.
- **Monitor financial statements:** Scrutinize your credit card and bank statements for any unauthorized charges and continuously check your bank statements for any signs of suspicious activity.
- **Inspect social media profiles:** Thoroughly review your social media profiles to identify any potential compromises.
- **Implement two-factor authentication**: Enhance security by implementing two-factor authentication on all accounts, especially for financial services.
- **Activate SMS notifications:** Register for SMS notifications to receive alerts when your accounts are accessed.
- **Conduct regular credit checks:** Routinely perform credit checks to verify if someone has attempted to obtain credit using your personal details. If detected, promptly inform the relevant credit provider.

By following these steps, you can effectively manage the aftermath of identity theft and mitigate further risks to your personal information and financial security.

The Protection of Personal Information Act, 2013 (POPI Act) aims to promote the protection of personal information processed by public and private bodies by, among others, introducing certain conditions for the lawful processing of personal information. Should you suspect that there has been interference with the protection of your personal information, you may lodge a complaint with the Information Regulator at complaints.IR@justice.gov.za.

DATA RESTORATION /MALWARE DECONTAMINATION

ACTIONS TO TAKE:

Report the incident to iTOO on 0861 555 771 so that we can engage our experts to:

- restore your data and software to its pre-incident state, or
- clean and restore your computer system, data, and electronic media affected by malware.

Examples include scenarios like unknowingly downloading a malicious programme while browsing the internet, resulting in your personal files, photos, and software becoming encrypted, or infecting your personally owned device with malware from a borrowed memory stick or hard drive, necessitating a reformat of your hard drive, and the reinstallation of your operating system.

Coverage offered by the [MY]CYlution policy (if applicable):

Costs of an IT expert to decontaminate, clean and restore your data and software, as well as the costs to replace parts of the computer should it be necessary.

Recommendations:

- **Document malware details:** Record specifics about the malicious program or malware involved, including its entry point if known, and the extent of damage inflicted on your files, software, and system.

Smartphone Security:

- **Secure lock screen:** Activate lock screen and security features on your smartphone, such as pattern passwords or fingerprint locks.
- **Avoid saving sensitive data:** Refrain from storing sensitive personal information or bank account details on your electronic devices.
- **Use VPN on public Wi-Fi:** When using public Wi-Fi, always use a Virtual Private Network (VPN) for added security.
- **Maintain built-in security measures:** Do not bypass or disable the built-in security features of your devices.
- **Safe app downloads:** Only download mobile apps from reputable and secure sources.
- **Install security software:** Install trusted mobile security and antivirus software from reliable security vendors.
- **Regular software updates:** Keep your mobile device and antivirus software up to date with the latest security patches.
- **Remote device management:** Enable settings for remote locating and restoring factory defaults on your electronic devices.
- **Data encryption:** Whenever possible, encrypt the data on your device.

For Securing Email and PC:

- **Check email settings:** Log into your email account on a secure PC and verify if any settings have been tampered with. Delete unauthorized changes.
- **Update passwords:** After fixing settings, create a new password and set your secondary email as the alternative address.
- **Disable unused wireless connections:** Turn off unused wireless connections like Bluetooth, Wi-Fi, and NFC when not in use.
- **Sign out and clear cache:** After transactions, sign out of your Online Banking session, close the browser, and regularly clear your browser cache on both PC and mobile devices.
- **Secure Wi-Fi networks:** Ensure your personal Wi-Fi networks are password protected with proper security settings.
- **Change router password:** Replace the default router password from your ISP with a strong, unique password.
- **Strong passwords:** Utilize strong passwords for all your accounts.

For Online Presence:

- **Privacy settings:** Set the privacy settings on your social media profiles to the highest possible level.
- **Two-factor authentication:** Enable two-factor authentication for public webmail services like Yahoo and Gmail.
- **Mysterious emails:** Take instances or reports from friends of strange or unusual emails from your accounts seriously.
- **Check outgoing email:** Monitor your “sent items” or “outgoing” emails for unknown messages, as this could signal that your device has been compromised.

By following these guidelines, you can significantly enhance your online security and protect your personal and financial information.

CYBER BULLYING & CYBER STALKING

ACTIONS TO TAKE:

Report the incident to:

- iTOO on 0861 555 771
- Provide written evidence stating the nature of events; where the content was posted; list of recipients and
- An A-1 statement from the police and obtain a crime reference number within 7 days of discovery by you.

Cyberbullying is the repeated, intentional use of electronic communications used to humiliate, intimidate or threaten you and can result in your wrongful termination of employment, false arrest, disciplinary action, or shock and mental injury as diagnosed by a medical practitioner.

Cyberstalking involves the use of electronic devices or the Internet to repeatedly harass or frighten you.

Coverage offered by the [MY]CYlution policy (if applicable):

- costs to remove the relevant online material,
- your lost income,
- legal costs to prosecute the third party,
- costs to manage and protect your reputation,
- trauma counselling and expenses to move your child to a different school if required.

Recommendations:

- **Stay calm:** Do not respond or retaliate to cyberbullying.
- **Block and report:** Swiftly block the perpetrator across all profiles, such as Facebook, Instagram, WhatsApp, etc. Also, report any abusive comments to the social media platform administrators.
- **Preserve content:** Avoid deleting any content involved in the incident, as it is crucial for investigation and evidence purposes. Our experts will conduct a forensic examination of the information from the device as soon as possible.
- **Guard personal information:** Refrain from posting or sharing personal information online, including full names, addresses, phone numbers, school details, parental information, credit card numbers, and friends' personal data.
- **Internet passwords:** Never share your internet passwords with anyone.

Tips for Parents:

- **Monitor computer use:** Place the computer in a high-traffic area of your home to easily oversee its use, rather than allowing private use in bedrooms.
- **Use filters:** Set up filters on your child's device to block inappropriate online content and enable you to monitor their online activities.
- **Encourage communication:** Urge your child to confide in you or another trusted adult if they encounter threatening messages or become targets of cyberbullying.
- **Establish clear rules:** Ensure your child understands the risks and rules for online activities, including computers, tablets, smartphones, email, and text messaging, along with the consequences for any violations.

By adhering to these measures, you can effectively respond to cyberbullying incidents and provide a safer online environment for yourself and your children.

Help centers are as follows:

- Childline: Call 116 or visit www.childlinesa.org.za
- South African Federation For Mental Health Helpline: Call 011 781 1852 or https://www.safmh.org/

The Cybercrimes Act 19 of 2020 provides that a person who lays charges at the police for these types of cybercrimes can also apply at a Magistrate's Court for a protection order. In respect of children, this cybercrime will also form part of the Child Justice Act 75 of 2008, which regulates how children will be dealt with when they are accused of committing crimes and what consequences they will face.

CYBER EXTORTION

ACTIONS TO TAKE:

- Report the incident to iTOO on 0861 555 771 – the ransom payment must be lawful and subject to prior written consent.
- You must notify the relevant law enforcement authorities of the Cyber Extortion incident.

Cyber extortion is a form of cybercrime where an individual or a group threatens to cause harm to a person, their reputation, or their computer systems unless certain demands, often monetary, are met. This form of digital threat has become increasingly common, with ransomware attacks topping the list.

Coverage offered by the [MY]CYlution policy (if applicable):

- The costs for IT experts to confirm the validity of the demand and as appropriate try restore your systems and data.
- If required, we will cover the ransom demand as well as other reasonable costs that may be incurred by you to resolve the incident.

Recommendations:

- **Preserve content:** Refrain from deleting any content, as it will be crucial for investigation and evidence purposes. Our experts will meticulously gather information from the device for analysis.
- **Backup critical data:** Always create backups of essential data, ensuring they are free from ransomware to prevent re-infection of your device.
- **Note file extensions:** If ransomware has altered the file extensions, document the new extensions.
- **Record ransom note:** Capture a screenshot or record the ransom note and the associated demand.
- **Disconnect from the internet:** Immediately sever incoming and outgoing connections. Disconnect your device from the internet by turning off Wi-Fi. Turn off the device to halt further damage by the malware.
- **Network isolation:** Since ransomware can propagate rapidly, consider turning off other devices on your network to prevent it spreading to more devices.
- **Change passwords:** As certain ransomware can steal passwords, take precautionary steps by changing your account passwords. Begin with the most vital accounts first, such as cloud storage, email, and bank accounts.

By adhering to these measures, you enhance your chances of mitigating the damage caused by ransomware and safeguarding your data.

NETWORK SECURITY LIABILITY (INCLUDING IOT)

ACTIONS TO TAKE:

- Report the incident to iTOO on 0861 555 771 and provide any pertinent details and reference numbers.

You can be held legally liable for damages to a third party due to the failure to prevent a Cyber Incident on your computer system or other Internet-connected components. An example of this might be when your device is hacked or infected with malware, causing damage to another person's device or data. The affected party may take legal action against you for the damages they have suffered.

Coverage offered by the [MY]CYlution policy (if applicable):

Costs for an IT expert to investigate what happened. We will also cover your ensuing legal costs and any settlements that may be awarded or agreed upon.

Recommendations:

- **Compile pertinent data:** Collate all relevant information concerning the Cyber Incident, including the type of breach, the attack's entry point, and the extent of the resulting damage.
- **Key documents and information to collect and retain:**
  - **Technical aspects**: Gather technical specifics about the breach, including timestamps, log files, and any digital footprints left by the perpetrator.
  - **Pre-breach security records**: Maintain an all-encompassing account of your computer system's security measures that were in place prior to the breach.
  - **Evidence of damage:** Preserve documentation that verifies the extent of harm sustained by the third party's computer system. This can include emails, invoices, or any other relevant forms of communication.
  - **Legal documentation:** Retain any legal documents linked to the incident, such as legal claims, communication exchanged with legal professionals, or official court records.

In the aftermath of a Cyber Incident, it's crucial to have an organized and comprehensive collection of information. This documentation can be invaluable for investigation, assessment, and potential legal proceedings.

PRIVACY & DATA BREACH LIABILITY

ACTIONS TO TAKE:

- Report the incident to iTOO on 0861 555 771 and provide any pertinent details and reference numbers.

You can be held legally liable for damages to a third party due to the failure to prevent a Cyber Incident on your computer system or other Internet-connected components. An example of this might be when your device is hacked or infected with malware, causing damage to another person's device or data. The affected party may take legal action against you for the damages they have suffered.

Coverage offered by the [MY]CYlution policy (if applicable):

Costs for an IT expert to investigate what happened. We will also cover your ensuing legal costs and any settlements that may be awarded or agreed upon.

Recommendations:

- **Compile pertinent data:** Collate all relevant information concerning the Cyber Incident, including the type of breach, the attack's entry point, and the extent of the resulting damage.
- **Key documents and information to collect and retain:**
  - **Technical aspects**: Gather technical specifics about the breach, including timestamps, log files, and any digital footprints left by the perpetrator.
  - **Pre-breach security records**: Maintain an all-encompassing account of your computer system's security measures that were in place prior to the breach.
  - **Evidence of damage:** Preserve documentation that verifies the extent of harm sustained by the third party's computer system. This can include emails, invoices, or any other relevant forms of communication.
  - **Legal documentation:** Retain any legal documents linked to the incident, such as legal claims, communication exchanged with legal professionals, or official court records.

In the aftermath of a Cyber Incident, it's crucial to have an organized and comprehensive collection of information. This documentation can be invaluable for investigation, assessment, and potential legal proceedings.

PRIVACY & DATA BREACH BY A THIRD PARTY

ACTIONS TO TAKE:

- Report the incident to iTOO on 0861 555 771 and provide any pertinent details and reference numbers related to the liability claim.

Privacy breaches occur when a company storing your personal information is hacked, resulting in your personal information being stolen and used to commit identity theft against you. In South Africa, the Protection of Personal Information Act (POPIA) says all businesses must protect the integrity of all personal information in their possession and under their control.

Coverage offered by the [MY]CYlution policy (if applicable):

Your legal costs to seek damages against the company your personal information was stolen from.

Recommendations:

- **Collect pertinent details:** Compile all pertinent information regarding the incident, including the breach's scope, the compromised data type, and any public acknowledgment or communication from the third party.
- **Gather and retain documents:** Ensure you gather and retain the following documents and information:
  - Evidence showcasing the impact of the data breach on you, such as emails, invoices, or other relevant communications.
  - Any legal documentation connected to the incident, including legal claims, lawyer correspondence, or court papers.
  - Written acknowledgments or communications from the third party acknowledging their responsibility for the data breach.

By diligently collecting and preserving these documents, you can build a comprehensive record of the breach's effects and any relevant legal actions or acknowledgments by the involved parties.

ONLINE SHOPPING

ACTIONS TO TAKE:

- Report the incident to iTOO on 0861 555 771
- Provide evidence that you have made reasonable attempts to resolve the issue with the Third Party and/or seller of the goods and services either by seeking performance of the sale or requesting a refund.
- The fraud event is reported by you to your card issuer, payment service provider, bank or other relevant entity within 48 hours of discovery by you.
- You provide written evidence that the card issuer, payment service provider, bank or other relevant entity is not reimbursing you.
- You report the incident and obtain an A-1 statement and crime reference number from the police within 72 hours of discovery by you.

You purchase an item online for your personal use and later discover that you have been scammed – you do not receive the goods or services ordered.

Coverage offered by the [MY]CYlution policy (if applicable):

- Your financial loss for non-delivery or non-rendering of goods or services that were ordered online specifically for your personal use.

Recommendations:

- **Direct navigation:** Always type the online store's web address directly into your browser instead of clicking on links from emails or social media.
- **Read reviews:** Check comments and reviews on the store's social media ads and do a Google search to find reviews and feedback from other customers.
- **Google search:** Search for the merchant, store, and products to verify their reputation and authenticity. Look for any Facebook groups where customers share their experiences.
  - Do an online search for "brand x + reviews"
  - Search "brand x + scam" or "brand x + fraud"
- **Secure website:** When making transactions, ensure the website starts with 'https' and has a closed padlock icon in the address bar. This indicates secure encryption.
- **Avoid storing information:** Don't store credit card details or personal information on online store accounts to prevent potential data breaches.
- **Watch for suspicious messages**: Be cautious of suspicious emails or SMS messages, especially those offering deals that seem too good to be true.
- **Strong passwords:** Use strong, unique passwords for online store accounts, and consider using two-factor authentication for added security.
- **Check prices:** Be wary if a product's price seems unrealistically low compared to similar items elsewhere.
- **Website age:** Be cautious of new websites, as they might be set up for fraudulent purposes.
- **Contact information:** Ensure the retailer provides genuine contact details like phone number, address, and email.
- **Payment security:** Use credit cards or secure payment platforms like PayPal for added protection.
- **Monitor statements:** Regularly review your credit card and bank statements for any unauthorized transactions.
- **Check for leaked account details:** Use tools to check if your account details have been leaked in data breaches.
- **Device security:** Secure your devices with reputable antivirus software to prevent malware and hacking attempts.

EXPRESS KIDNAPPING

ACTIONS TO TAKE:

- Report the incident to iTOO on 0861 555 771
- The Insured must at all times use best efforts to ensure that knowledge of the existence of this insurance is restricted as far as possible.
- You must provide proof of cash withdrawal.
- You report the incident and obtain an A-1 statement and crime reference number from the police within 72 hours of release.
- We will not be liable for an amount exceeding the actual value of money or assets that is surrendered.
- We will only be liable for an amount equal to the foreign currency equivalent based on the exchange rate set by the central bank on the day the money is surrendered.

Express kidnapping is when someone is taken and held against their will. The victim is forced to withdraw cash from an ATM or transfer money from their bank account until their funds are depleted or they are released.

Coverage offered by the [MY]CYlution policy (if applicable):

- The value of the funds and/or value of the property surrendered by the victim in exchange for their release.

Recommendations:

- **ATM safety:**
  - Use ATMs located within banks, hotels, and shopping centers during daylight hours to minimize risk.
- **Personal information protection:**
  - Be cautious about sharing sensitive information in public places or on mobile phones to avoid becoming a target.
  - Review and limit the personal information you share on social media to prevent making yourself vulnerable.
- **Taxi safety:**
  - Beware of criminals posing as unlicensed taxi drivers. Opt for licensed and reputable taxi services to ensure your safety.
- **Vary your routine:**
  - Prevent predictability, which can make you an easy target.
  - Change your daily routine by altering departure and return times, taking different routes, varying parking locations, and modifying activity schedules.

By adopting these precautions, you can significantly enhance your personal safety and reduce the risk of becoming a target.

iTOO™

INCIDENT RESPONSE LINE: 0861 555 771

Remember your policy includes access to the Cyber+ contact centre, who will assist and guide you following a personal cyber incident.

For more information visit the **[MY]CYlution** site

For all your queries please send an email to **cyber@itoo.co.za**

itoo.co.za

Think Expert. Think iTOO