Republic of Namibia

Financial Intelligence Centre

**P.O.BOX 2882, Windhoek**

**Tel: + 264 61 2835100, Fax +264 61 2835259**

**Web address: www.fic.na**

**E-mail address: helpdesk@fic.na**

# CYBERCRIME FOREWARNING

**ISSUED: APRIL 2023**

## 1. Background

Over the years, people have lost substantial funds owing to cybercrime. Criminals who are involved in cybercrime continue to increase significantly and their methods of operation become more complex, affecting essential services such as businesses and private individuals. Cybercriminals may pursue exploiting members of the public or security vulnerabilities in order to steal their essential information such as passwords, data or funds.

There can be many definitions for cybercrimes but a suitable one within the context of this report is that cybercrimes target or use a computer network or a networked device. In other words, it refers to a variety of crimes carried out online, using the internet through computers, laptops, tablets, internet-enabled televisions, game consoles, and smartphones. Cybercrime may be carried out by individuals or organizations. Most cybercrimes are committed by cybercriminals or hackers who want to illicitly defraud people of their money. However, occasionally cybercrimes also damage computers or networks for reasons other than profit such as political or personal. This is not the context of this report. Some cybercriminals are organized to use advanced techniques and are highly technically skilled[1].

Criminals abuse networked devices as a way of illicitly soliciting funds from members of the public through deceptive, dishonest, and fraudulent means. These crimes often result in huge financial losses for victims. Other than the obvious financial losses, the proceeds from such activities are often laundered. Money Laundering (ML) activities undermine the integrity of our financial system. The FIC is sharing this publication to help contribute to efforts geared toward combatting such activities.

## 2. How do these crimes operate?

Cybercriminals are increasingly enhancing the sophistication and complexity of their methods. There are constantly new innovative ways employed to advance cybercrime and associated fraud. At times, criminals that target computers may infect them with malware to damage devices or stop them from operating. Such criminals may also use malware to delete or steal data. Below are some common techniques of cybercrime[2]:

[1] https://www.kaspersky.com/resource-center/threats/what-is-cybercrime; and
[2] https://krazytech.com/technical-papers/cyber-crime.

**Hacking:** It is a simple term that defines sending illegal instructions to any other computer or network. In this case, a person's computer is hacked so that his/her personal or sensitive information can be accessed. The criminals use a variety of software to crack a person's computer and the person may not be aware that his/her computer has been accessed from a remote location;

**Identity Theft:** This has become a major problem with people using the internet for cash transactions and banking services. In this type of cybercrime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card, and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history;

**Malicious Software:** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or cause damage to software present in the system; and

**Fraud Calls/eMails:** the criminals may contact a potential victim through false messages, calls, or emails in which they misreporesent to be employees of financial institutions such as banks. They may have information related to the victim's bank account or cards. Such criminals may request personal details like ATM card information, password or may request that the victim clicks on the link sent by themselves. If one mistakenly trusts them and gives them the details, they can use such to defraud the victim.

## 3. How do you protect yourself from these crimes?

**Use strong passwords:** Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods;

**Be social media savvy:** Be sure to keep your social networking profiles (Facebook, Twitter, YouTube, etc.) set to private. Be sure to check your security settings. Be careful of what information you post online. Once it is on the internet it is there forever;

**Secure your mobile devices:** Many people are not aware that their mobile devices are also vulnerable to malicious software, such as computer viruses and hackers. Be sure to download applications only from trusted sources. It is also crucial that you keep your operating system up-to-date. Be sure to install anti-virus software and use a secure lock screen as well;

**Protect your computer with security software:** Several types of security software are necessary for basic online security. Security software essentials include firewalls and antivirus programs. A firewall is usually your device's first line of defense. It controls who and what can communicate with your computer online;

**Protect your identity online:** When it comes to protecting your identity online it is better to be too cautious than not cautious enough. It is critical that you be cautious when giving out personal information such as your name, address, phone number, and/or financial information on the Internet; and

Carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary.

## REMEMBER

If you become a victim of a cybercrime or any other fraudulent activity, immediately file a Suspicious Transaction or Activity Report with the FIC at the Bank of Namibia. Alternatively, you may contact the nearest police station to initiate a criminal investigation.