Let's Talk Fraud

SMS Fraud

Cell Phone Fraud

Cell Phone Notification Fraud

Online & Mobile Banking Fraud

Social Media Fraud

Email Fraud

Identity Theft

FISH HOEK

 **Email Fraud (Phishing)**
Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider or a bank, for example. It asks the consumer to provide personal identifying information.

SMS Fraud (Smishing)
Smishing (a combination of the words SMS (text message) and Phishing it is a scam where fraudsters send text messages to random cell phones. Scammers use email or text messages to try to steal your passwords, account numbers, or ID numbers. If they get this information, they could get access to your email, bank, or other accounts or they could sell your information to other scammers.

 **Phone or Voice Fraud (Vishing)**
Vishing (a combination of the words Voice and Phishing) is a phone scam where fraudsters target you by phone and try to trick you into divulging personal, financial or security information.

 **Computer Fraud (Technical Support Scam)**
With this type of scam the fraudster rings you unexpectedly telling you that there is a problem with your computer, modem or internet connection. They may indicate that there is virus on your computer or a problem with the internet connection or modem. In order to “fix this” they say they need to gain access to the computer and talk you through steps that will fix the problem. Criminals often use familiar names such as “Microsoft”, “Windows” or “Apple” to make them sound more credible.

 **Identity Theft**
Identity theft occurs when your personal details such as your Identity number, driving licence and banking details are compromised or stolen allowing fraudsters to pose as you. This allows fraudsters to use your information to obtain credit or to purchase goods or services in your name, take over your bank account or to make applications in your name for new bank accounts, cards or loans. One of the biggest problems with identity theft is that the crimes committed by the fraudster can often be attributed to you.

 **Social Media Fraud**
Be very cautious about what information you post on social media. Think of security questions e.g. mothers maiden name, where you work, where you went to school, birthday messages = date of birth. The fraudster can build up a profile through various social media channels to build a picture of your identity.

- **Keep important personal documents secure,** including your passport, birth certificate, credit or debit cards.
- **Limit or restrict how much personal information** you share on social network sites.
- **Shred or destroy** any documents containing personal information before disposing of them.
- **Regularly check your bank** and credit card statements. If you find an unfamiliar or unusual card payment or bank transaction, contact your card issuer or bank immediately.
- **Report lost and stolen cards** or suspected fraudulent use of your account to your bank or financial institution immediately.
- **When receiving new cards confirm** that all your personal limits are set correctly, they may have been set to default ie. No limits New Features may have been added eg. The TAP function
- **When using online or mobile banking**, choose, use and protect passwords with great care.
- **Make sure your smartphone or tablet** is always protected with a PIN and set the device to automatically lock.
- **Do not store your banking PINs or passwords** on your smartphone or tablet.
- **Only download mobile apps from official App stores**, such as the Apple App Store or Google Play Store.
- **Update banking and other apps** on your device regularly.
- **Always log out of your banking app** when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.
- **Regularly clear your browser's cache.** Some mobile phones and tablets store copies of web pages that may contain your banking information.
- **Always update your mobile phone's operating system**. Older software may have vulnerabilities that could expose you to security and fraud risks.
- **Do not use unsecured public Wi-Fi networks** or hotspots for internet banking.
- **Use a reputable brand of antivirus software** on your mobile phone and check your device's security settings to ensure maximum protection.
- **Don't feel pressured or rushed**. Fraudsters may try to make you feel foolish, stupid or negligent if you don't follow their instructions.
- **Contact your bank immediately** if you have given a caller any bank details.

Important telephone numbers

Bank	Fraud Line
ABSA Bank	0860 557 557
Capitec Bank	0860 102 043
First National Bank	0875 759 444
Nedbank	0800 110 929
Standard Bank	0800 020 600
Discovery bank	011 324 4444

Please report all crimes to the police at Fish Hoek Police Station

Fish Hoek Police Station contact numbers:

Contact number	021 784 2700
During Load shedding	082 522 2745 & 082 522 2053

Please note:
If we do not report crime we do not receive the resources to fight crime.

Fish Hoek Community Police Forum Website

https://fishhoekcpf.co.za

The Fish Hoek Community Police Forum is in the process of updating their website and will contain Emergency Contact Numbers and will continually be updated with useful and relevant information pertaining to our community.

Fish Hoek Community Police Forum Facebook

https://www.facebook.com/fhcpf/