Banking Channels Security: Internet, Mobile and ATM Security

1. How we're protecting you.

Our Commitment to You
Stanbic Bank understands that your trust in us depends on how well we keep your personal, business and account information secure. Our Corporate Information Security Program is comprehensive and proactive to ensure your information is secure whether you choose to bank with us through banking offices, ATMs, telephone or the Internet.

Stanbic Bank utilizes industry-accepted security practices that are appropriate for the way you choose to bank with us. For your protection, no matter which channel you choose, we verify you are who you say you are before granting you access to your accounts. Additionally, our systems use firewalls and encryption to protect your information from others.

We will never send e-mails asking you to provide, update or verify personal or account information such as passwords, Social Security Numbers, PINs, credit or debit card numbers, or other confidential information.

We have put the following measures in place to keep you and all your Online Banking information safe.

- **Secure sign in –** At minimum, you will always have to enter your User ID, password and other credentials to access your account(s).
- **Automatic sign out -** We will automatically sign you out after several minutes of inactivity in case you forget to sign out or leave your device unattended.
- **Fraud detection systems -** We monitor your account(s) for any unusual behaviour.
- **Suspend account -** We will temporarily disable your account(s) after a number of incorrect sign in attempts in case fraudsters are trying to guess your details.

2. Protect yourself

You can maximize the security of your online and mobile activities and protect yourself against identity theft and other online and mobile fraud by adopting safe online and mobile usage and practices

A. Keeping your online identity secure

1. **Don’t tell them everything**
   Identity thieves gather small pieces of information published online to build a profile of their victim. If you allow it, people can see your date of birth, mobile number, address and information on your family. Instead try to limit how much personal info you give away online, for example on Facebook and Twitter, but also when registering information on gaming sites or forums.
2. **Password security. Use a strong password for example:**

    - At least 8 characters consisting of letters (upper and lower case), numbers and Use
    - Don't use your names, birth dates or pet names
    - Never write down or share your password
    - Regularly change your password, at least every 90 days is recommended
    - Use different passwords for each site you use.

3. **Account Usage**

- Do not use your online banking password for other applications
- Never access bank, brokerage or other financial services information at public locations such as Internet cafes, public libraries, etc.
- Prohibit the use of "shared" usernames and passwords for online banking systems
- Avoid using automatic login features which save usernames and passwords for online banking
- Never leave a logged on computer unattended

4. **Watch out for email scams**
   If you get any emails or text messages you don't recognise or you're not sure about asking you for personal details, don't provide them or click on any links they give you. Be especially cautious if they threaten to suspend or limit access to your account.

B. Surf safely

Whether you're new to using the Internet or a seasoned surfer, it's worth considering these solutions in place to keep you and your personal information safe online.

Use anti-virus software - Running anti-virus software can help you prevent infection from viruses, Trojans and many other nasty 'bugs'. Anti-virus isn't just for computers, so make sure your other devices are protected by downloading appropriate software.

Use a firewall - Once set up, it can help prevent potential intruders from accessing your device. Most modern operating systems come with built in firewalls. To make sure it provides an effective barrier between your device and the Internet, it's important to set up your firewall appropriately by following vendor instructions.

Prevent spyware - Spyware is a form of online spying. You can help prevent it from getting onto your device by using up to date anti-spyware software and surfing with caution.

Secure your wireless connection - Without a secure wireless network, anyone can use your connection. Securing your wireless connection can be as simple as setting up a password. Your Internet service provider or wireless router manufacturer should provide instructions on how to do this.

C. Beware of Keystroke Logging or Keylogging

Keylogging is a method by which fraudsters record your actual keystrokes and mouse clicks. Keyloggers are "Trojan" software programs that target your computer's operating system (Windows, Mac OS, etc.) and are "installed" via a virus. These can be particularly dangerous because the fraudster has captured your user ID and password, account number, ID Number - and anything else you have typed. If you are like most other users and have the same ID and PIN/Password for many different online accounts, you've essentially granted the fraudster access to any bank or company with whom you conduct business. After all, they've got your login credentials so they appear to be a valid user.

Here are some ways you can prevent yourself from being a victim of keystroke logging:

- Use Anti-Virus Software. This is the single most important thing you can do to protect your computer from viruses. There are many on the market today – some cost money while others are free. If you opt to use a free version, make sure it is being offered by a reputable company and do research on the company and its product before installing.
- Keep your Operating System up-to-date with the latest security patches.

D. Use ATM's securely

1. Do not share your card or Pin with anyone.
2. Observe your surroundings before using an ATM. If the machine is obstructed from view or poorly lit, visit another ATM
3. Shield the screen and keyboard so anyone waiting to use the ATM cannot see you enter your PIN or transaction amount
4. Put your cash, card and receipt away immediately. Count your money later, and always keep your receipt
5. If you see anyone or anything suspicious, cancel your transaction and leave immediately
6. If anyone follows you after making a transaction, go to a crowded well-lit area and call the Police

Look out for unfamiliar fixtures on ATMs. These fixtures will not appear to be part of the normal ATM, or are attached to the slot where you insert your card. If you notice something suspicious don't use it and report it to the Bank immediately

E. Suspicious Websites, Emails, Advertisements or Pop-up Windows

- **Email security -** Occasionally, bogus emails are used by fraudsters in an attempt to extract your personal banking details. It is important to remember, Stanbic Bank **will never ask you to update any information by email**. Neither we nor any bank agent will ever contact you and ask for your personal banking details, PIN or passwords. If you do receive an email that seems to have been sent from the bank asking for your personal banking details, pin, passwords, or you are suspicious in any way, please delete it immediately. Do not call any telephone number or respond to the email, genuine emails can always be re-sent.
- If you accidentally open a suspicious email, do not click on any of the links within the email.
- If a suspicious email is opened and/or the links within the email are clicked, immediately contact our contact Center.

F. Phishing

Don't get caught through phishing
We're all used to getting some pretty strange emails in our inboxes asking us to "click here" or send information about ourselves, or even making promises of great wins. While Internet offers convenient access to services such as shopping and banking, it also holds risks to the security of your personal information and money. One such risk is "phishing", used by criminals in ever–changing ways to ultimately take your money.

What is phishing?
Criminals use phishing to try to get you to give them your banking and other personal information.

How is it done?
Usually, you will receive an email from the fraudsters that appears to be from us with a link to a site that is very similar to ours. In most cases you would find it very difficult to tell that the site is not ours. The email will ask you to provide your customer selected username and password, card details or account numbers.

Another way criminals use is to send you an email claiming to be from your Internet service provider (ISP) that includes links to their genuine site. Once you are linked to the site a pop–up window appears requesting your credit card information.

What we are doing to protect you
We are committed to protecting the confidentiality of your banking details. We are always looking out for sites that pretend to represent Standard Bank or any of our subsidiaries. When we find one we take measures to close them down as soon as we can. We also do our best to make sure our

customers are told of new ways criminals may try get information out of you.

To make online transacting safer, you should make use of our security and authentication services. These include

- One–time password is a unique, compulsory and time–sensitive password used as added security on selected Internet banking transactions. The password will be sent to you by SMS and is valid for one Internet banking session. This service is free.
- Payment confirmation is a message that informs the person you are paying that a transfer or payment has been successfully completed.

How you can protect yourself
Never give your personal details to anyone without making sure that they are who they say they are. A Stanbic Bank representative will never ask you for personal or banking information in an email.

You should view emails and pop–up windows asking for your personal information with the same amount of suspicion you would the person behind you in an ATM queue.

- Treat emails that appear to be from us asking for personal details with suspicion
- Never reply to their email or get into a conversation with them
- Never provide your personal details, for example, your PIN or account details by email
- Do not follow any links in emails to reach our Internet banking website. Always enter our website address manually into your Internet Browser to connect to our Internet banking site.

What you can do if you suspect phishing

Call your nearest branch if you think you have in one way or another given your banking details to a criminal.
Let us know if you are not sure about an email or website saying it Standard Bank's. We will ask you to please forward the email to us and we'll investigate.

Do **not** respond to that email.

By sending it to us you may help us close down an illegal site and help save others from falling victim to these criminals.

If you've given out your details
Call your nearest branch if you think you have in one way or another given your banking details to a criminal.

G. Securing your Desktop or Laptop PC

- Install, update and run reliable commercial anti-virus and anti-spyware software
- Install an actively managed firewall on your computer and/or network
- Ensure that your computers are patched (updated) regularly – particularly the operating system and key applications
- Implement any automatic updates for the operating system, anti-virus and anti-spyware applications
- Limit administrative rights on your computer and network to prevent the inadvertent downloading and installation of malware or viruses
- Completely close and exit all web browsers before and after an online banking session to lessen the risk of certain types of sophisticated malware attacks
- For even better protection, consider rebooting your computer before and after an online banking session

- Disconnect your computer from the Internet (both wired and wireless connections) when Internet access is not being used for an extended period (e.g., unplug from the Internet each evening when your work is done and reconnect in the morning)

H. Antivirus Software

What is anti-virus software? - Anti-virus software is a computer program that searches your hard disk for viruses and removes any that are found. It only protects against what it already knows about. New viruses spread very quickly so you must update your anti-virus software regularly, on a weekly basis at the very minimum.

What anti-virus products are available? - There are many anti-virus products to choose from so it's best to do your research. Most anti-virus suppliers also offer a firewall product at little or no extra cost, and these can be set up at the same time. You'll need to ensure your chosen product is set up to check for updates every time your computer is switched on, and runs a weekly scan. Typically updates take a couple of minutes and will happen in the background. Ideally it should also be set up to perform a full scan of the computer once a week.

What is spyware / adware and how to prevent it - Spyware is a program that secretly gathers information about what you do on your computer and quite often it does this without your knowledge. In its least dangerous forms it is known as adware. Adware collects information about your internet habits on behalf of companies and can occasionally pops up adverts as you surf.

How does it work? - In its more dangerous form, it can act like a Trojan virus which is installed on your computer without you realising. You do not have to be connected to the internet to be spied upon, but once on the internet, any information gathered can be sent to the fraudsters spying on you.

How can I prevent it? - Spyware removers, search out these programs in the same way as anti-virus and can also block those annoying pop-up adverts. There are many free anti-spyware programs which can be downloaded and used to scan your computer for spyware and adware, like Ad-aware.

Signs of infection

If you keep getting pop up windows all over your screen, you may have been infected with spyware or adware. You should run a scan like Ad-Aware or Windows Defender to detect and to remove it.

I. The Top 10 security tips for your Online and Mobile Banking:

- Protect your computer and mobile devices with up-to-date security software and install regular security and software updates.
- Only use official mobile banking apps provided by your bank, e.g. Stanbic Bank Mobile Banking Apps, and only download apps from an official app store.
- Never log in to Online Banking through a link in an email. Either type the address into your browser or use your bookmarks.
- Use PINs or passwords that are hard for someone to guess. For example, use a mix of letters, numbers and symbols for passwords. Change your PIN or password immediately if you think someone may have discovered it.
- Don't give anyone your security details or information and never write them down or store them on your mobile device in a way that might be recognised by someone else.
- Never give your PIN, password or full security details to anyone who calls you or in an email or text message.
- Be wary of opening attachments or clicking on links in emails or texts that you weren’t expecting or are unsure about.

- Our Bank will never call you and ask you to transfer money to a new account, so ignore such calls. Ensure we have your up-to-date mobile number so we can contact you if we spot unusual or suspicious activity on your account.

If your phone is lost or stolen, call us straight away so we can disable your mobile banking apps as a precaution. Give Call details.

J: What to Do If You Suspect Online Fraud

If you suspect or detect online fraudulent activity, it is vital that you report it to us. Your immediate action may prevent further theft or compromise. The sooner you act, the sooner we can help.

1. Contact TD Bank immediately to report fraud.
    - Customer Service
        - Tel.
        - Email:
    - Be prepared with all details of the incident, including transaction information, timing, and the manner in which the compromise was identified. You may be asked for information, including the following:
        - Did you receive a suspicious e-mail?
        - Did your online banking site look or act differently than normal in any way?
        - Did a fraudulent transaction post to your TD Bank account?
2. Shut down your web browser and computer, and disconnect your Internet connection and wireless capability.
    - If a computer is compromised, any continuing activity or operation could expose additional sensitive information to criminals.
    - A computer that is turned off and disconnected from the Internet cannot transmit data to the Internet.
    - Some malware may exist only in a computer's temporary memory; shutting down the computer might prevent permanent or further infection.
    - Contact your competent technical support person to scan and remove any malware from the computer, workstation or network before using your computer or network to access any sensitive information.
    - Change your password and any answers to security questions after the computer has been cleaned.

K: Contacts

1. Our contact Center
2. Report Fraud
3. Lost and Stolen Cards
4. Suspicious emails or contacts by suspicious people