## 1.Critical Issues relating to Electronic Payment Systems

Electronic payments (E-payments) are transactions conducted through automated networks rather than use of physical cash, cheque or any other physical instrument. Changes in technology have brought about more payment options for the transacting public with increased efficiency and convenience. Access devices such as Automated Teller Machines (ATMs), Point of Sale(POS), Internet and mobile devices can be accessed using credit cards, debit cards, mobile, bank transfers, internet payments among others. Customer education and awareness should continue to be heightened to ensure safety of funds and the transacting individuals. Fortunately, there are many safeguards available to protect your sensitive personal information from falling into the wrong hands.


***Bank cards for transacting on POS and ATM***

## 2. ATM Security Tips

- Individuals must think about personal safety when using an ATM. It is best to be alert and aware of your surroundings no matter where or when you use it.
- It is best to use ATMs in public areas.
- Firstly, look at the ATM to check for any suspicious signs. Do not use an ATM that appears unusual or offers options which you are not familiar or comfortable with.
- If it looks like the device has been tampered with, do not use it as this could possibly mean that someone has attached a “skimmer” to the ATM to steal your financial information. Report such discoveries to the police and or your bankers immediately.
- Be wary of people trying to help you with ATM transactions. Do not accept assistance from or offer your personal identification number to seemingly well-meaning strangers, even security guards manning the ATM, and never allow yourself to be distracted.
- Always verify that the amount you withdrew or deposited matches the amount on your transaction confirmation.
- Secure your cash and card in a safe place after your transaction whilst still at the ATM.
- If your card is stuck in the machine, report it immediately to your bank before leaving the machine.
- Do not leave your card unattended.
- If your access device (card) is lost or stolen, if you can block it from unauthorised use then immediatley contact your bank.

***ATM (Automated Teller Machines)***

## 3.PIN Security Tips

- Never write down your personal identification number (PIN) where it can be accessed by someone, especially on the back of your card, or save it in your phone but rather, memorize it.
- For security reasons, avoid sharing your PIN with other people including family members.
- When selecting a PIN, avoid picking a number that is easy for others to guess - for example, 0000,1234, your name, telephone number, year of birth, or any simple combination of these.
- Choose a strong password, one that is not easily replicated by anyone.
- When typing in your PIN at the ATM cover the number pad when inputting the digits so that no one near you can see your PIN.
- Change your current PIN from time to time at least once every 90 days to make it more difficult for fraudsters to predict.

## 4. Online shopping tips


- Ensure you are on a secure website before entering payment details. The web address should begin with ‘https://’ (hypertext transfer protocol secure). The ‘s’ stands for ‘secure ‘and also an icon of a locked key ensures that the site is secure.
- Double check all details of your payment before confirming transaction.
- Before entering payment details on a website, ensure that the link is secure, which can be done in the following ways;
  i) There should be a padlock symbol in the browser window frame, which appears when you attempt to log in or register.
  ii) Be sure that the padlock is not on the page itself this will probably indicate a fraudulent site.
- Ensure you have effective and updated antivirus/antispyware software and firewall running on your machine before you go online.

## 5.Security Tips For Safe Internet Banking


- Avoid storing passwords in a file on any computer system (including mobile or similar devices) without encryption.
- Do not let your computer remember your password. Never accept auto complete option provided by your computer/ browser.
- Change passwords frequently.
- User-id and passwords should not be stored on any page that appears when you click on a hyperlink received through email.
- Avoid accessing Internet banking accounts from public wifi or shared personal computers (PCs).Make sure you have a secure internet connection shown by a small padlock icon somewhere on your browser and check if the address bar – the universal resource locator (URL) of the site you are begins with ‘https’.
- Install a personal firewall on your computer system. This will provide added level of security. Always check your last log-in date and time in the post login page.
- After you have logged in, you will not be asked to provide your username and login password again. Also, you will not be asked to provide your CREDIT or DEBIT CARD details while using internet banking. If you get a message (such as through a pop-up) asking for such information, please do not provide this information no matter how 'genuine' the page appears.
- It is good and recommended practice to always log out of your online banking session when not in use. This will lessen the chances of falling prey to session hijacking and cross-site scripting exploits.
- Run an antivirus software on your computer. This will ensure you are protected from Trojans and other forms of viruses that could be used to gain access to your personal and financial data.
- Try to get a bank account that offers some form of two or three factor authentication for online banking.
- Check your statement regularly for unauthorised transactions.

- Try to get a bank account that offers some form of two or three factor authentication for online banking.
- Check your statement regularly for unauthorised transactions.

## 6.Security Tips on POS for Retailers

- Regularly inspect the POS equipment, terminals, and PIN-entry devices for any signs of tampering which may include broken seals, missing screws, inessential wiring, or additio nal labels that might hide signs that the device has been altered, worn out or there are disconnected cables.
- Invest in surveillance systems. Consider installing surveillance cameras in the stores or places of business. Doing so will allow you to monitor instore activities 24-7 and will give you recordings you can revisit if necessary.
- Ensure POS devices meet the requisite standards.
- Software and technology on the device should be consciously updated, encrypted and serviced.

## 7.Customers

- Keep important information away from prying eyes by ensuring that POS, card terminals, and screens are positioned for maximum privacy.
- When typing in your PIN for a point-of-sale (POS) purchase, cover the number pad so that no one near you can see your PIN.
- Avoid giving your card or pin number to the merchant staff or anyone for assistance.

80 Samora Machel Avenue
P. O. Box 1283. Harare Zimbabwe
Telephone +263 0242 703 000, +263 867 700 0477.

## 8.Mobile Banking Security Tips

Mobile banking, or m-banking, enables mobile phone users to access financial services even when they are miles away from their nearest branch or home computer.

- Protect your personal information by ensuring your mobile device maintains a PIN, fingerprint authentication, or strong password or other forms which allow access to the device.

**When your device is not in use, enable automatic screen lock.**

- Once your session is complete, log out of mobile banking session before closing the application.
- Do not share personal and financial information via email, text or phone.
- Delete security codes and message alerts you may receive via text from your financial institution. If you change your mobile phone number, be sure to update your online banking profile to protect sensitive message alerts.
- Report a lost or stolen mobile device. Contact your financial institution immediately to update your information. You can also login and remove the old device from your online banking profile.
- Switch on your GPS mobile tracker as this will assist you to quickly locate your device when lost or stolen.
- Use caution when downloading banking apps. Only install apps from reputable and trusted sources such as a direct link from your financial institution's website. Never enter your login details on a website or in a mobile application that doesn't come directly from a trusted company.
- Keep your mobile operating system up-to-date by installing the latest updates as prompted by your device to ensure maximum security, but the same may not be true of some-such as your banking and payment application.
- Avoid the use public Wi-Fi hotspots. Unsecure networks can expose sensitive data, making it vulnerable to hackers.
- Do not root or jailbreak your device. This practice weakens device security.
- Ensure that your mobile device has remote wipe installed or enabled. This helps in the event that you lose your phone, you can delete all information you had stored on your phone. Notify your bank so that no texts or mails will be sent to your mobile device.


NATIONAL PAYMENT SYSTEMS DEPARTMENT

# SECURITY TIPS
## WHEN USING
## ELECTRONIC PAYMENTS