Security Information

Safeguard Your Account

Nobody knows your account better than you. That is why you should never share your card details, internet banking log in and token with anyone over the phone, SMS, or email.

NPF Microfinance Bank is continuously developing and implementing security enhancements to ensure the integrity of our Online Banking platform. Our goal is to protect your online safety, the confidentiality of our customer account and personal data.

Learn more about protecting yourself online, how to spot fraudulent e-mails and Web sites.

Security Tips

- Giving away your Internet Banking login, card details, PIN, and codes from your token device, gives anyone total access to your account. NPF Microfinance Bank will never ask for any of these details via any form of communication.
- Keep your ATM cards safe and do not share your personal identity number (PIN) with anyone. Do not keep any written copy of your PIN with your card. Memorize it.
- Seeing a phone number or email address you recognize does not mean it is genuine. Always give cold callers a cold reception
- Use your hand or body to shield your PIN when you are conducting transactions at the Automated Teller Machine (ATM) or when making Point of Sale (POS) transactions at retail stores.
- Create strong passwords for your Internet Banking login and card details. Change them often.
- Check your bank account statements and card transactions regularly to make sure these only reflect transactions you have made. If you see a transaction you cannot explain, report it to the bank.
- Subscribe to SMS alerts to be delivered to your cell phone or email, so you can stay updated on your account activity.
- Always log on to our internet banking service via our website – http://www.npfmicrofinancebankplc.ng or https://ibank.npfmicrofinancebankplc.ng
- Watch out for copycat websites. Don't fall prey to any website that looks like NPF Microfinance Bank 's website. Check the URL carefully. (https://)

Recognizing Fraud

You are the first and best layer of defense in combating online fraud. Learning to properly detect and avoid online scams is the ultimate protection against fraud. Read the tips below to help you spot potential scams.

Online fraud typically takes the form of fraudulent e-mails and Web sites. These forged means of communication often use corporate logos, colors, and legal disclaimers to make them appear authentic.

Fraudulent Emails

Fraudulent e-mails are the most common avenue of online scams. A "spoofed" e-mail is one that purports to be from a reputable source to trick you into divulging personal or account information, sending payment, or otherwise taking an action that will result in fraud. These attacks are common because they are low-tech and can be easily deployed on a massive scale. Even though the warning signs are there, "phishing" and scam e-mails continue to fool people. Some of these mails also request that customers update their account records by clicking on links to fake Internet banking and Interswitch websites.

Spoofed Websites

Spoofed Web sites, like phishing e-mails, are used by fraudsters who build fake websites that look very similar to NPF Microfinance Bank's website to lure unsuspecting customers into submitting their online banking log-in information and card details which are later used to access such accounts. Spoof Web sites allow fraudsters to collect such sensitive information as Internet Banking Account and ATM Card Details.

NPF Microfinance Bank will never ask a customer to provide, verify or update their personal, account or financial information via email or pop-up windows. This includes: Passwords, Personal Identification Numbers (PIN), or ATM, Credit or Debit Card numbers. If you receive an email requesting such information, do not respond and never click on a link contained in a suspicious email.

Phishing

Phishing involves the use of fraudulent email or browser pop-up messages that appear to be from a legitimate source, often using a company name, logo and/or graphic. A typical scam consists of:

- Receipt of an email message stating you need to update or validate your account information.
- The message suggests a dire consequence, such as your online access expiring or being suspended, if you do not respond.
- Via a link in the message, it directs you to a Web site that looks legitimate but is not.

The intent is to trick you into divulging personal information, such as your account number, User ID or Password so they can commit crimes of a monetary nature or identity theft. It may also be an attempt to deliver and install malicious code (malware) that can harm your computer.

How to avoid falling for Phishing Scams

Never open any email unless you know who the sender is. The very act of opening an email can infect your computer with malware. Be skeptical of every email you get, and never click on suspicious links, or download suspicious attachments. If all else fails, call your bank.

Pharming

Occurs when you enter a Web address but are redirected, without your consent or knowledge, to a fraudulent site that looks like a legitimate site. The intent of the fraudulent site is to capture confidential information.

- If your card is lost or stolen, contact us Card Services immediately using the following telephone numbers:
- Debit Cards: +234-8074550514
- Credit Cards: +234-8074550514
- You will never be contacted on phone to verify personal or card information, your PIN or to request that you transfer funds or process transactions to protect your account
- Memorize your Personal Identification Number (PIN). Never write it on the card or anywhere else it could be compromised.

Skimming

“Skimming“ is a method by which thieves capture the magnetic stripe data from your card and use it to create a new, counterfeit card. These counterfeit cards are then used to process unauthorized transactions against your account. There are two main methods of skimming card information:

A small device that appears to be a part of the machine is placed over the card insertion slot of an ATM, gas pump, or other self-service kiosk. As you slide your card into the ATM, this device “reads” the data on the stripe and either stores it or transmits it to a nearby location. Often, there is also a small, hidden camera that captures your keystrokes as you input your PIN into the machine.

How to protect yourself

- If you see an attachment on an ATM that looks suspicious, do not use the ATM. Notify the institution that owns the machine as soon as possible.
- Never give your PIN to anyone or write it on your card.
- Review your monthly statements immediately and notify your bank of any discrepancy.

Your Responsibility

NPF Microfinance Bank, its staff or agents will never call or send you an email with a link, asking you to update your Internet Banking profile or request your passwords, token generated codes, card details or PIN. Anyone that asks for any of these details is a fraudster.

If you receive or have received an email fitting this description or a suspicious telephone call from someone claiming to be from NPF Microfinance Bank, please report such to any of the NPF Microfinance Bank numbers on: **0700CALLNPFMFB, 08008008008, 08074550514, 08074550522** and forward such emails to info@npfmicrofinancebankplc.ng **or** fraudalert@npfmicrofinancebankplc.ng

NPF Microfinance Bank's Policy

NPF Microfinance Bank is continuously developing and implementing security enhancements to ensure the integrity of our Online Banking platform. Our goal is to protect the confidentiality of our customer account and personal data. While we work to ensure that a secure environment is provided for Online Banking, there are steps that Online Banking clients should follow to protect confidential information while performing financial transactions online:

- Create a strong unique Online Banking password. Select a password that is hard to guess by using random letters, numbers, and symbols. Do not use readily identifiable information such as your name, birth date, or child's name.
- Do not share your password with anyone else. Keep your password secure.
- Do not use the Save Password option on your computer.
- Change your password regularly. We recommend changing your password at least every 40 to 90 days.
- Signoff when you have finished your online banking session.