Online Safety

SmartCash PSB has a strong commitment to information security. To meet our high level of security standards as well as those of the legal bodies regulating our business sector, SmartCash PSB places a strong emphasis on making the platforms that our customer use safe and secure. Even with these diligent efforts in place, customers must be aware of what they can do to maintain and increase the security of their system.

We also request that our customers, for any responsible disclosure of a security vulnerability in our website, mobile application, or our services, contact us at customerservice@smartcashpsb.ng

Protection against online fraud

To protect your account and personal information from fake emails, SMS and websites, follow a few simple steps:

- Delete suspicious emails without opening them. If you do open a suspicious email, do not respond to online solicitations for personal information
- Do not open any attachments or click on any links it may contain
- Never provide sensitive account or personal information in response to an email

How to identify a fake email, SMS or website

1. **Email:**

- Check the sender's address: Look at the email address carefully to identify addresses that are like legitimate ones but may have slight misspellings or added characters
- Look for generic greetings: Fake emails usually use generic names to address the recipient. Emails that start with "Dear Customer" or "Dear User" could be suspicious.
- Check for urgent language or use of threats: Fake emails often try to create a sense of urgency, claiming that your account will be suspended or compromised unless you act immediately.
- Hover over links: Hovering over links in an email (without clicking) can reveal the actual URL.
- Poor grammar and spelling: Many scam emails contain obvious grammar or spelling errors, which is uncommon in legitimate corporate communications.

- Unexpected attachments: Be careful of emails with unexpected attachments. These attachments could contain malware.

2. SMS (Text Messages):

- Unknown sender: Be cautious if you receive a message from an unknown number, especially if it claims to be from a company or government agency.
- Shortened or suspicious links: Scammers often use shortened URLs (e.g., bit.ly) in SMS to hide the real destination. Avoid clicking on any links unless you're sure they're legitimate.
- Urgent or alarming messages: Just like in emails, scammers try to create urgency. Messages that threaten immediate action if you don't respond quickly are often fake.
- Requests for personal information: Legitimate companies won't ask for sensitive information (like passwords or credit card details) via SMS.

3. Website:

- Check the URL: Ensure the website's URL starts with "https" (not just "http") and includes a padlock icon.
- Look for misspellings or extra characters in the URL: Fake websites often use URLs that are close to the legitimate site but may include extra characters or slight misspellings.
- Search for reviews or warnings: Before interacting with a website you're unsure of, search for reviews or check for any warnings about the site being a scam.

Tips for safe internet use for customers

Trust your instincts: If something feels off, it's better to be cautious and investigate further.

Don't share personal information: Be wary of any unsolicited request for personal or financial information.

Verify with the source: If you receive a suspicious message or email claiming to be from a company, contact the company directly using official contact information (not the info provided in the message).

By being vigilant and following these guidelines, you can protect yourself from falling victim to scams