**Stay Safe: How to Outsmart Latest Scams and Protect Your Money**


In this digital era, one can lose money at a click as scammers continue devising sophisticated ways to lure potential victims.

Cybercriminals are even targeting employees' email accounts within organizations, using fake messages disguised as workplace policy updates. This marks a new variation in their constantly evolving tactics amid the rise of digital interactions.

Consider David, a young professional, who received a text message at work asking him to provide his bank account details for a reward program between his company and bank. The message included a link where he could "provide details."

David, instead of clicking the link, remembered his bank's consistent warnings about avoiding suspicious messages and links. Acting cautiously, he visited his HR and also contacted the bank directly.

The bank confirmed the message was a scam and emphasized that they never send reward links via text, urging verification through official channels.

**#KataaUtapeli #KaaChonjo**

Scammers exploit emotions like fear, urgency, and trust to trick people into sharing sensitive information or transferring money. They use tactics such as phishing messages with fake links posing as trusted institutions and social engineering to manipulate victims

For instance, they may call pretending to be bank representatives, asking for personal information under the guise of "verifying your account." Others may claim to have accidentally sent you money and ask you to return it, only for you to later discover that the original transfer was fraudulent.

Scammers exploit carelessness in public spaces by offering unsolicited help at ATMs to steal PINs or swap cards. On public Wi-Fi, hackers can intercept data and access banking accounts unnoticed.

They also use lost IDs or passports to impersonate victims and open fake accounts. They also monitor social media for financial clues to take advantage of opportunities.

Some use fake emergencies like relatives asking for money and school fees and rent scams asking you to deposit money to new account numbers linked to your landlord or schools.

**Essential Security Tips to Protect Yourself**

- Avoid clicking on links in unsolicited messages; verify directly with your bank.
- Use strong passwords and verify passwords with authentication apps.
- Avoid saving your banking passwords on your phone or browser, especially on shared devices.
- Never share a password reset code.

Equity Bank is committed to safeguarding its customers' accounts. If you're an Equity customer, keep these essential security measures in mind:

- Never share your ATM's CVV (three-digit CVV code at the back of your card), PIN, password, or OTP; banks won't ask for your PIN or password.
- Use different passwords for banking and social media accounts.
- If your card gets stuck at an ATM, don't leave or accept help; call your bank immediately.
- Use mobile data, avoid using public Wi-Fi for online banking.
- Confirm payment instructions before transferring money.
- Download banking apps only from official stores and enable 2-factor authentication.
- Memorize your PIN, keep it private, and cover the keypad when entering your pin while in public.
- Report lost IDs or passports to your bank immediately and other relevant authorities.
- Don't accept help from strangers at ATMs; call your bank if your card is stuck.
- Monitor your accounts regularly and report suspicious activity promptly.
- Report any suspicious numbers or SMS lines to **333** for FREE.
- Be wary of calls or messages from unknown numbers. All official calls from Equity Bank will originate from **0763 000 000**.

**Be Vigilant**: Take control of your financial security now, protect yourself from fraudsters and ensure your hard-earned money stays safe! To learn more visit: Secure Banking Tips | Equity Bank Kenya.

**#KataaUtapeli #KaaChonjo**