

CEDISPAY DIGITAL ADVICE AND WAYS FOR CLIENTS TO BE EFFICIENT

CedisPay is a "no paperwork" financial institutions: Photos of KYC documents can be uploaded via mobile app or website, customers sign their documents through their online account and guarantors sign documents through DocuSign. Our "no paperwork" for clients activities include:

- Automated workflows
- 2. Making payment online or mobile phone
- 3. Scanning paper document into a digital document format such as PDF
- 4. Using Google forms to complete loan application
- 5. Apply for a loan through our website on a computer or Smart phone
- 6. Using Doc sign to sign facility letter
- 7. Email communication & WhatsApp communication
- 8. Converting your signature to an electronic format for signing documents online
- 9. Using online system to score customers
- 10. Determine loan eligible amount
- 11. Loan pricing
- 12. Loan evaluation
- 13. Automated ID verification
- 14. Credit burau integration.

Please apply the following digital advice for to be efficient

- 1. Digitize your document creations and storage methods -Take pictures of their receipts and save on their phone
- 2. Digitize evidence to support business income and expenses either put your income and expenses as when on mobile money account /bank

account or book them into mobile money account /bank account on weekly basis

- 3. Digital payments—for instance, by mobile phone or app for suppliers
- 4. Have Savings habits
- 5. Have Insurance habits
- 6. Have Bills paying habits

Our advice for you to be efficient include

- 1. Delegate the small things
- 2. Automate processes and workflows
- 3. Consolidate tasks and remain focused
- 4. Welcome change
- 5. Use available tools- Calendly to streamline meetings, QuickBooks for your financials

How To Avoid Sending Money to a Scammer

Mobile payment apps can be a convenient way to send and receive money with your smartphone. These apps have become very popular — and scammers may try to use them to steal your money.

Some scammers may try to trick you into sending them money through a mobile payment app. That's because they know once you do, it's hard for you to get your money back.

Scammers might pretend to be a loved one who's in trouble and ask you for money to deal with an emergency. Others might say you won a prize or a sweepstakes but need to pay some fees to collect it.

Keep this advice in mind if you send money through a mobile payment

- 1. app:
- 2. Don't send a payment to claim a prize or collect sweepstakes winnings.
- 3. Don't give your account credentials to anyone that contacts you.

- 4. Protect your account with multi-factor authentication or a PIN.

 Before you submit any payment, double-check the recipient's information
- 5. to make sure you're sending money to the right person.
 If you get an unexpected request for money from someone you do recognize, speak with them to make sure the request really is from them and not a hacker who got access to their account.

Ways to Guard Against Mobile Money Fraud

Savvy cyber criminals have developed sophisticated means to rob unsuspecting users of the mobile money service as well as users of other electronic payment services. If you have not yet been targeted, good on you. But just like any other crime, you are not totally insulated unless you take extra precaution. We belief that these five measures can help guard against Mobile Money fraudsters.

PROTECT YOUR PERSONAL IDENTIFICATION NUMBER

In what is called "Cash Out" fraud, subscribers to the Mobile Money service are pushed payment approval prompt and lured to enter their PIN Code in order to receive a price won or for a particular service say (phone book backup or job alerts) to be enabled on their phone. This action authorises payment of money from the consumers' wallet to the fraudster's wallet. At all cost protect your personal information from unknown sources. If for any reason you suspect that your personal identification number is in the wrong hands, change it quickly and report to your network provider or the police.

BEWARE OF UNSOLICITED MESSAGES (SCAMS)

Fraudsters invent convincing messages to get your attention and then your money. Mostly these messages come promising some unexpected money that you have won or are likely to win or some imported goods sent by a relative which you have to pay in order to redeem. Know this,

mana doesn't fall from the sky anymore. Think twice before you give out your personal information in response to these messages. You will not get any money you are not expecting and you are most likely not going to win any lottery by giving out your pin or sending mobile money. You are only going to be defrauded.

CHECK THE AUTHENTICITY OF PAYMENT APPS BEFORE USING THEM

Cyber crooks create mobile applications that mimic the original ones that banks and other financial institutions develop in order to phish relevant personal information and to steal your money. Other payment service providers also have apps to enable transactions from banks to mobile wallets and vice versa. To avoid being a victim, always check the authenticity or the originality of these apps before downloading and installing them. When in doubt always verify from the service provider for specific security features and links to the original apps. When you are certain you have the original application, don't hesitate to enable the two factor verification functions on these apps to secure your personal information and money.

DON'T TRUST ANONYMOUS CALLS WHEN MONEY IS INVOLVED

One of the many tricks that these crooks use is to call unsuspecting subscribers to the mobile money service and ask them to revert money sent to them by mistake. First, they send you a message saying you have received X amount of money from Kofi. Then they follow up immediately with a call saying it's a wrong transaction and ask that you send the money back to them. A mobile money alert will always come from your service provider and not any other person's number.

Nevertheless, always check your balance to see if it tallies with the amount they are asking you to resend. Even if it does, call your service provider first for assistance before you proceed.