multinet trust exchange
exchanging trust since 1994

Licensed by Central Bank of the UAE

Fraud Awareness and Reporting:

To report any fraudulent activities please contact:

Dubai Police	Toll Free 901 **dubaipolice.gov.ae**	**Sharjah Police**	Call Center 901 **shjpolice.gov.ae**	**AbuDhabi Police**	Hotline 800-2626 **adpolice.gov.ae**

You can also report it to **Multinet Trust Exchange**
Customer Happiness Center: +971 4 2555685 Ext-101
Email: complaint@multinettrust.com

Customer Awareness and Fraud Techniques:

Multinet Trust Exchange is committed to utilizing all of our resources to fight against fraud and prevent criminals from victimizing our customers.
We use the latest technology and train our staff and valued customers to fight against fraud together.

Protect yourself:

You are advised to adhere the below guidelines.

1. Don’t click on suspicious links.
2. Never send money to unverified sources.
3. Report suspicious activities to the relevant authorities immediately.
4. Do not share personal details with unknown.

Fraud Techniques

Fraud Awareness

multinet trust exchange
exchanging trust since 1994
Licensed by Central Bank of the UAE

Fraudsters try to stole the money by using below methods.

1.WhatsApp/ Botim	2. Phone calls	3. SMS	4.Facebook/ Social Media		

They ask for their victims' data and bank account information, claiming that they need these details to receive their prize money. They use these details to gain access to the victims' accounts and steal their money.

Other scammers will also instruct their targets to send money to a certain address or bank accounts before they can claim their cash prize.

Types of Fraud:

1. **Phone:**
   Fraudsters will pose as bank employees. They will claim that your account is frozen. They will ask for personal information. They will connect you to an automated system that will ask for your card details and security code.
   Fraudster also pose that they are calling from Police/CID/Dubai courts department and will shout to provide Emirates ID number or Provide mobile OTP immediately.

2. **Lottery:**
   Fake message claiming that a person has won a certain promotion. Fraudster will require some information which they will use to access to accounts.

3. **Email:**
   Fake email from bank claiming that the account is frozen for security reasons and that the customer should call a number found

in the email. The person picking up the phone will grab the customer's details giving the fraudsters access to the customer's bank account/details.

4. **Fund-Transfer:**
   Businesses deal with suppliers and clients from all over the world, primarily via email. Fraudsters will send links via copycat emails. when the victim clicks on the link it gives the fraudster access to their computer or smartphone.

5. **ATM-BANK:**
   Small camera placed above the keypad to gain access to a user's PIN.
   Fake keypad placed above the actual keypad of the ATM to get user's PIN.
   Device placed above the card reader in the ATM that will scan the front and back of the card, giving the fraudster access to the card number and 3-digit security code.

6. **Sim-Swap**
   Fraudsters will gather information on a certain person, either from social media or other sources. They will contact service providers to gain access to a new SIM card.
   They will make payments using the victim's card and use the new SIM to gain access to the One Time Password (OTP) sent through SMS to authenticate the transaction.
   They can also use the OTP to access social media or bank accounts.

7. **Data-Privacy:**
   Emirates ID number, date of birth, bank account details and much more can be breached by fraudsters. They will use this information to hack into your bank accounts, social media accounts etc.