ADAMS FRAUD PREVENTION SERIES

This booklet is made to support you in identifying potential fraud activities you may encounter. We strongly advise you to thoroughly review the bookelt to be aware of the proactive measures outlined to safeguard yourself from falling victim to fraud.

PHISHING EMAILS

- Beware of deals that sound too good to be true
- Do not click on links received via emails/social media from unknown sources
- Always verify offers through merchant official website rather than relying on unsolicited email communications

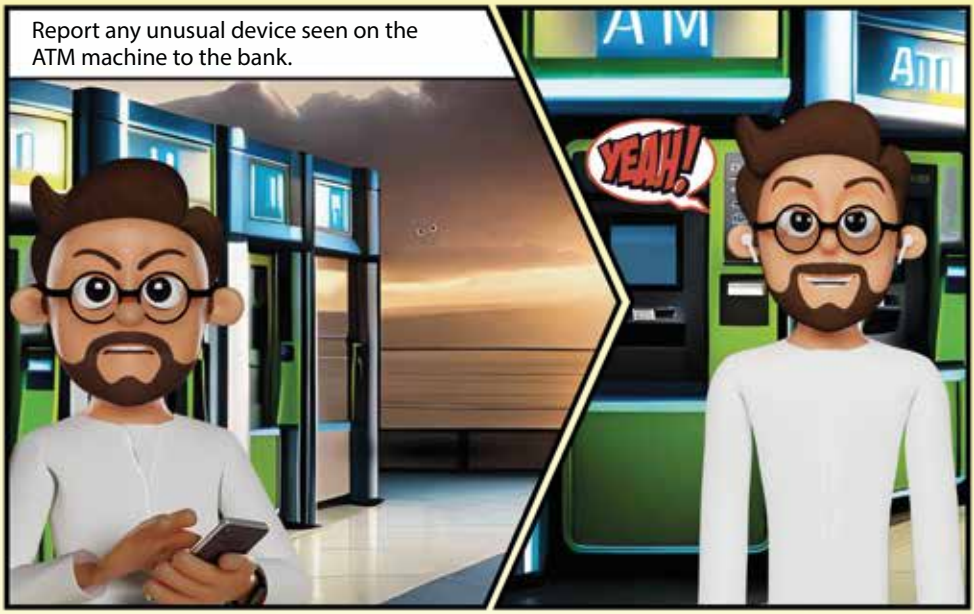
VISHING (SUSPICIOUS CALLS)

- Never share your (card number, expiry date or CVV number) or bank account details (account name and account number) with anyone pretending to be calling you from the bank/authorities/police
- Report fraud calls to authorities immediately
- Banks or authorities will never ask for your sensitive information over the phone

SMISHING (SUSPICIOUS SMS)

- Be careful when clicking on any link you receive especially when they request any financial transactions or personal details
- Report fraud cases to authorities and verify offers directly with your bank
- Always verify offers on banks official website

ATM CARD SKIMMING



- Always stay vigilant while using ATMs and report any suspicious devices
- Make sure no one sees your pin
- Never accept help from strangers at ATMs

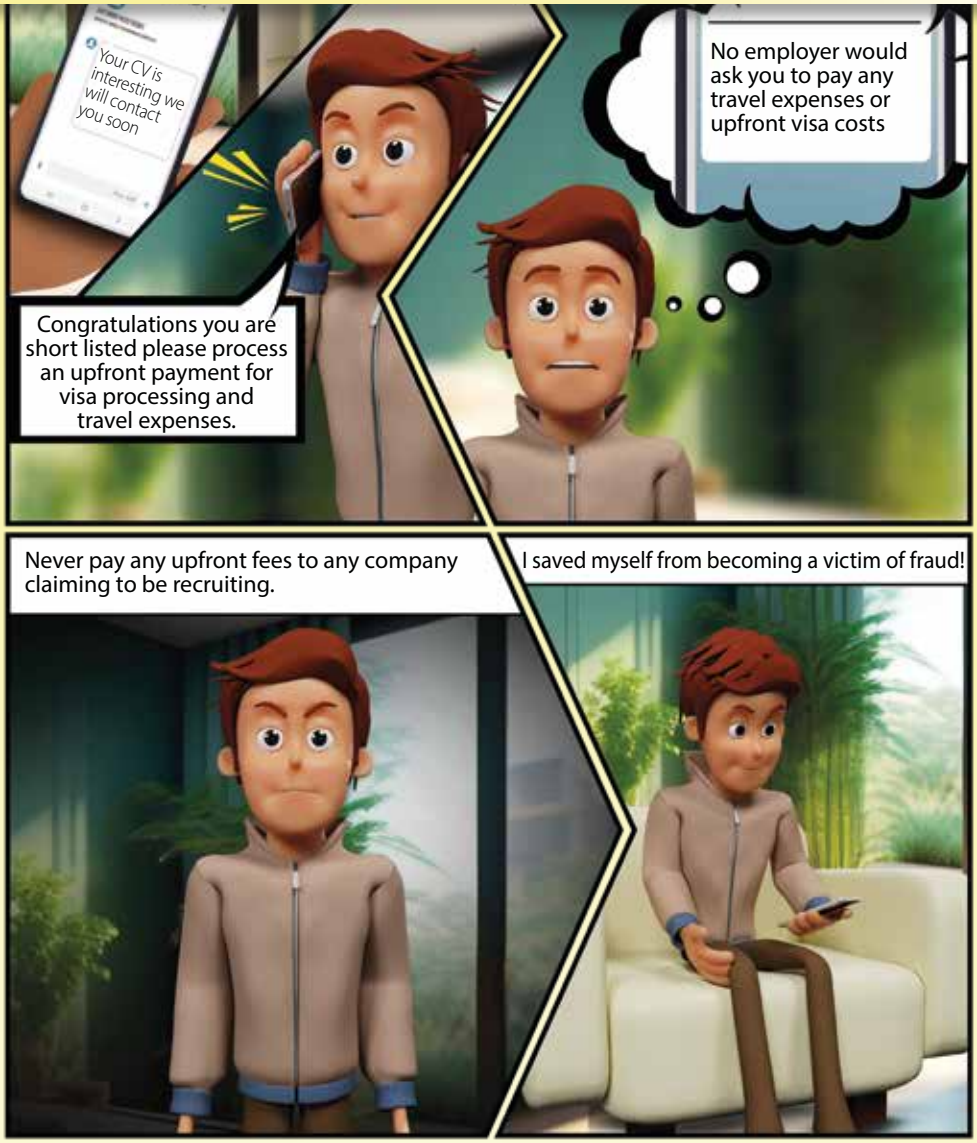
JUICE JACKING

- Avoid public charging stations and opt for your own USB power adapter to plug into electrical outlets.
- Keep a portable power bank with you for on-the-go charging without relying on public outlets.

IMPERSONATION THROUGH SOCIAL MEDIA

- Refrain from sharing card details on social media, emails, or messaging apps
- Remember the importance of cross-checking urgent requests received through social media or emails with a direct phone call

ONLINE JOB SCAMS



- Online job opportunities could also be a potential fraud
- Job seekers should be cautious when asked to make upfront payments or provide personal information as a part of a job application
- It's essential to verify the legitimacy of the job offer by checking for the job posters profile and official online pages

اتحاد مصارف الإمارات

UAE BANKS FEDERATION

PRODUCT PROMOTION FRAUD

- Stay cautious when confronted with seemingly incredible offers
- Reviewing and understanding contracts protects you from potential fraud
- Always be cautious when considering offers and promotions

FAKE ADVERTISEMENTS

- Contact merchants through local and official numbers
- Validate the authenticity of advertisement on social media especially the ones that are "too good to be true"
- Remain vigilant and avoid falling victim to fake advertisements

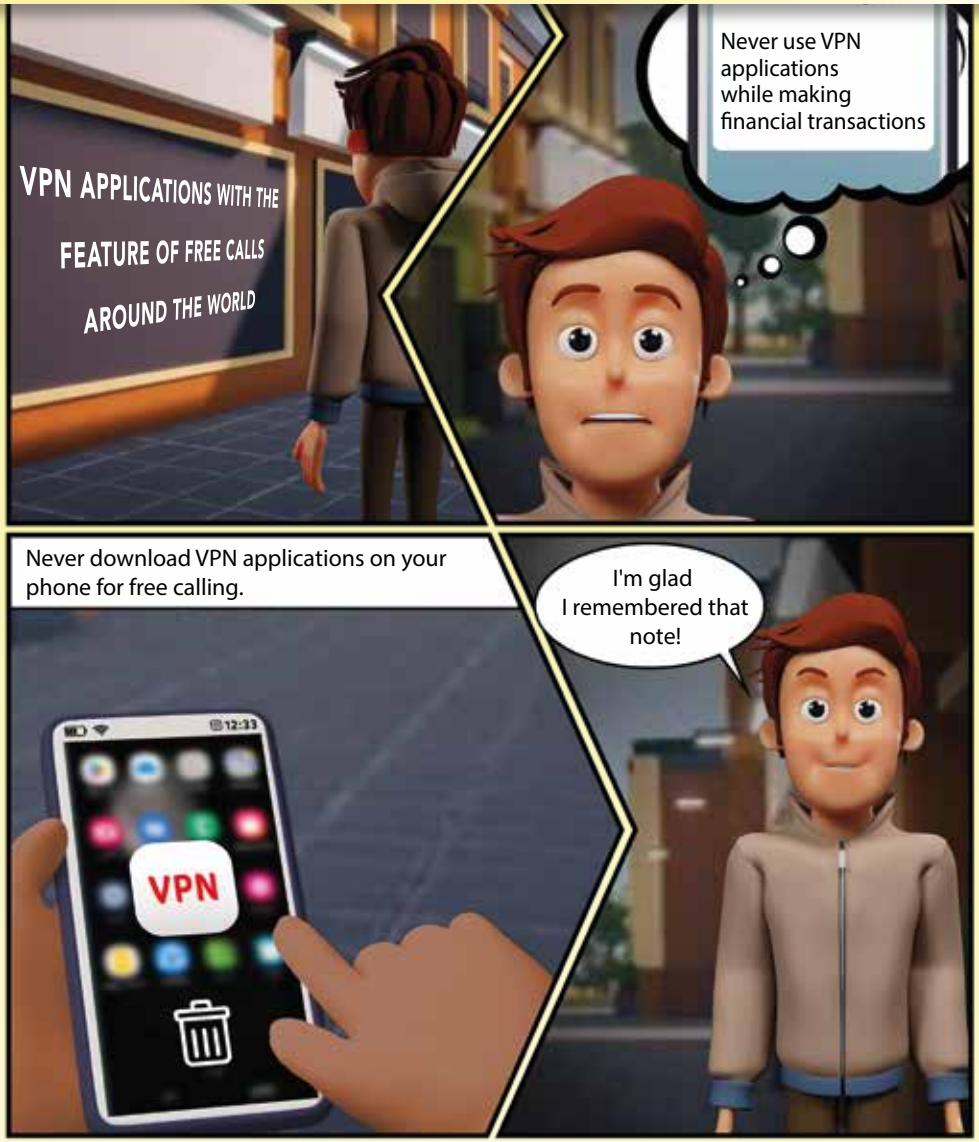
GAMING FRAUD

- Be cautious about sharing personal information or screen access with unknown individuals online
- Do not click on suspicious links sent by unknown individuals
- Educate yourself and people around you on online safety measures

PUBLIC WIFI AWARENESS
(FRAUD USING PUBLIC WI-FI)

- There are many risks associated with using public Wi-Fi
- Fraudsters could be able to hack your account through public Wi-Fi
- Connecting to public networks could also allow access to personal accounts

FRAUD USING VPN



- Be aware of downloading VPN applications for free calling, as they might compromise your privacy and security
- Contact your bank directly to block your card in case of any suspicious transactions
- To avoid being hacked, do not use the same email address for your bank statements and online platform registration

CHARITY FRAUD

Do not share your card details or bank account details on unknown websites.

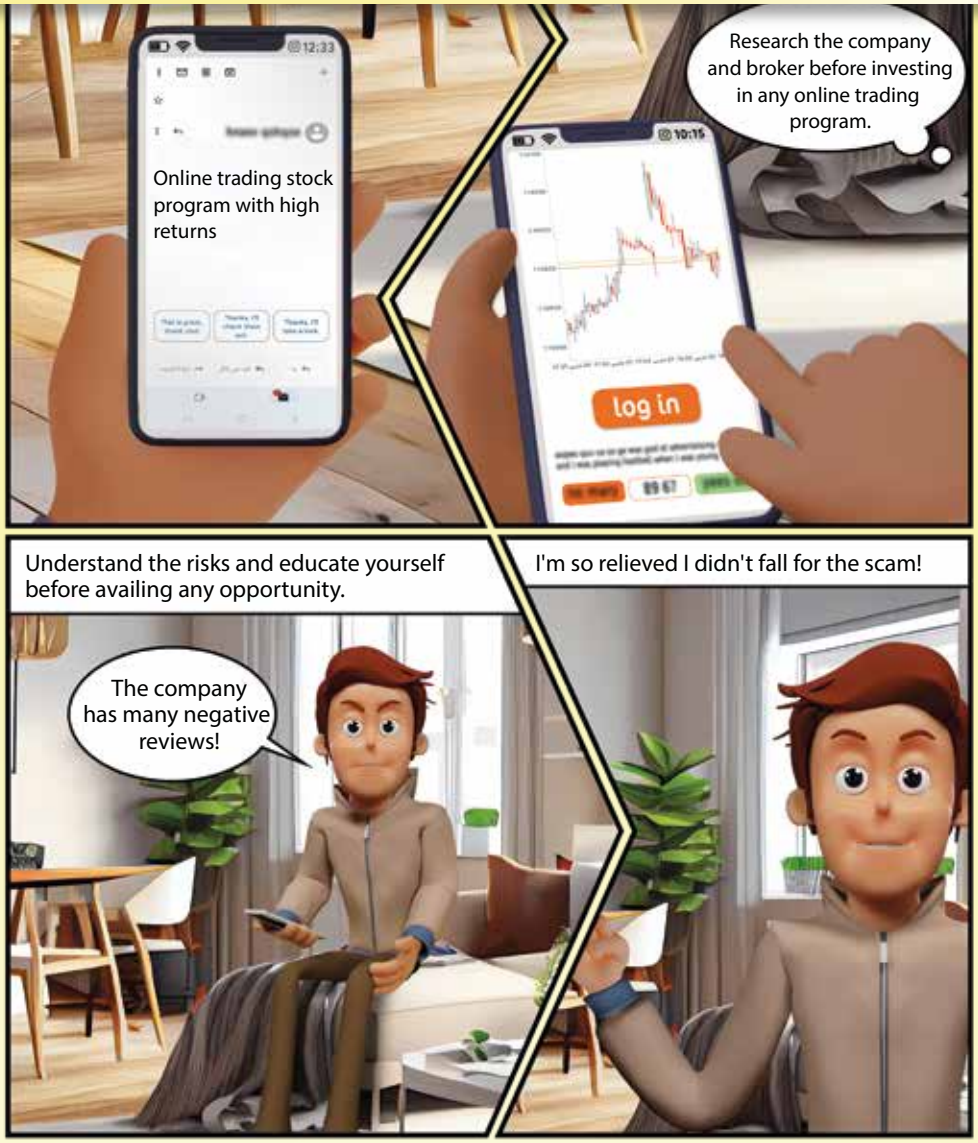
I'm happy i didn't make a donation on a fake website

- It is important to check if the charity organization is registered
- Asses the authenticity of advertisements by checking the organization's link to verify
- Refrain from sharing your card and bank account details on unverified websites, or using auto-save options to save your information

IDENTITY THEFT

- Changing the SIM card and cloning it are methods used by fraudsters to hack into your mobile phone and gain control over your number
- Do not provide any electronic authorization that could enable fraudsters to clone your SIM card
- If you notice any discrepancies in your account, report them to the bank you deal with immediately.

ONLINE TRADING SCAM (FOREX)



- Always research both the company and the assigned broker before engaging into any onine trading program
- Be wary of promises of guaranteed profits, such claims often mask fraudulent schemes
- Refrain from sharing your account details with anyone to protect your financial security

INVESTMENT PORTFOLIO FRAUD

- Verify credentials and licensing before engaging with any financial advisor or investment firm
- Check if they are registered with relevant regulatory authorities and if their licenses are up to date
- Understand the investment strategy and risks

CRYPTOCURRENCY FRAUD SCAM

- This experience underscored the importance of caution in the face of excessive marketing and offers that seem too good to be true
- It is necessary to conduct thorough research before investing in cryptocurrency platforms
- Be aware of sharing sensitive information with anyone and keep crypto and bank accounts separate

SPOOFED EMAILS

- Always verify payment instructions received via email or phone call
- Cross-check such instructions with involved parties, particularly for changes in beneficiary details callback
- Remain vigilant for even the slightest variation in spelling within email addresses or domain names

MAGIC INK FRAUD

Always use your own pen to fill any documents applications and cheques.

I refused the request from the agent and avoided the fraud attempt.

- Individual vigilance is very important in such situations
- Caution is required when dealing with unfamiliar agents
- There are many risks associated with fraudulent practices like magic ink fraud

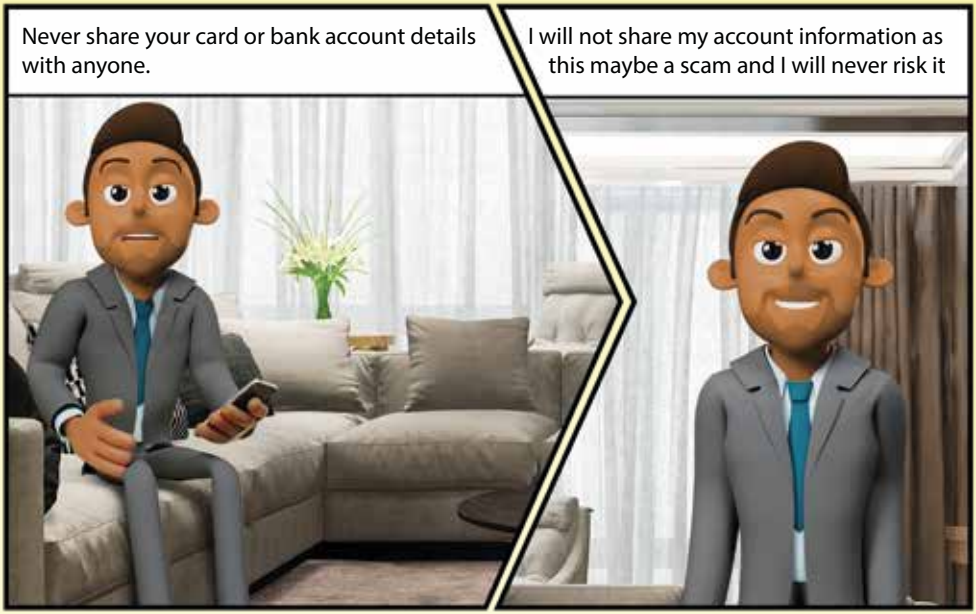
PAYMENT REQUEST FRAUD

- Always double-check the displayed KYC name after the QR code is scanned before authorizing the payment
- Always verify the displayed KYC name (the name retrieved from the bank records of a Request-to-Pay) before accepting payment request

QR CODE FRAUD

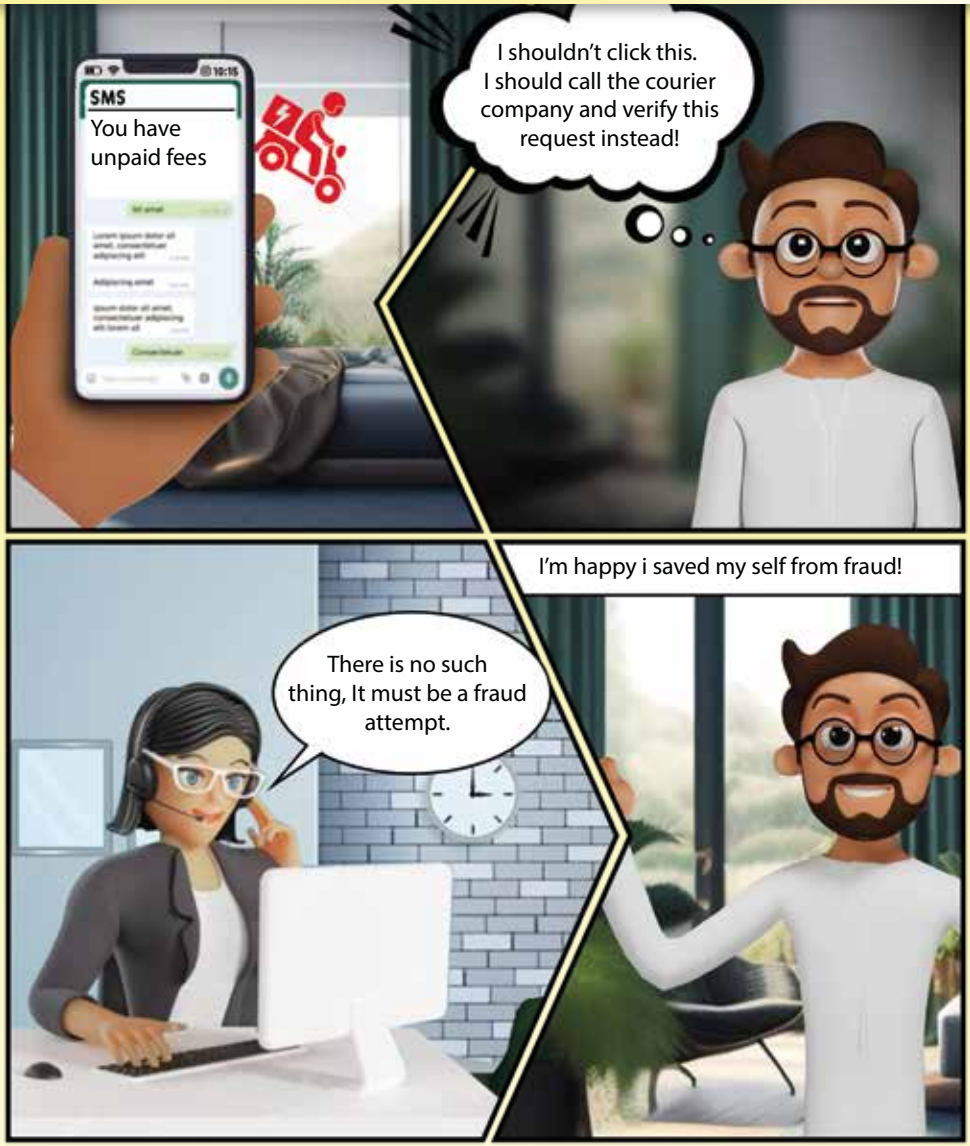
- Always check and verify the retail name after you scan the QR code to avoid falling for fraud

PRIZE SCAM FRAUD



- Never share your (card number, expiry date or CVV number) or bank account details (account name and account number) with anyone
- Report calls from unknown sources informing you of prizes, raffles and competitions to the authorities

COURIER DELIVERY FRAUD



- Never click on suspicious links, especially those that include financial details
- Always report such situations with the relevant authorities

اتحاد مصارف الإمارات

UAE BANKS FEDERATION