



FRAUD AWARENESS AND REPORTING

Al Fuad Exchange – Consumer Awareness Hub

At Al Fuad Exchange, we want to help you make safe financial choices. Our Awareness Hub gives you simple tips, alerts, and advice to protect yourself from fraud, scams, and other risks.

1. How Fraudsters May Contact You

Scammers can reach you in different ways:

- **Phone calls** – Pretending to be from banks, police, companies, or even family members using AI voice cloning. Fraudsters can record a small sample of someone's voice (sometimes from social media) and use AI to mimic it. Victims may receive calls requesting urgent money transfers or confidential information.
- **SMS / WhatsApp** – Fake urgent messages or links.
- **Email** – Fake notices, phishing links, or harmful attachments.
- **Social media** – Fake accounts pretending to be official.

Tip: Real companies will never ask for your PIN, password, or OTP through phone, email, or social media. Always verify requests through a trusted secondary channel before taking action.

2. Common Scam Situations

1. Phishing Email

- **What happens:** You get an email saying your card is blocked and must click a link or call a number.
- **Warning signs:** Urgent tone, links asking for personal info.
- **What to do:** Don't click. Check directly with Al Fuad Exchange.

2. Fake Lottery or Prize

- **What happens:** A message says you won a prize but need to give details or pay a fee.
- **Warning signs:** Asking for money or personal information.
- **What to do:** Al Fuad Exchange never asks for fees. Always confirm with us.

3. Phone Call Asking for OTP

- **What happens:** Caller pretends to be from your bank, police, or even a family member using AI voice cloning and asks for OTP or card details.
- **Warning signs:** Pressure to act fast, request for secret info.
- **What to do:** Never share OTP or PIN. Hang up and report.

4. Fake Social Media Accounts

- **What happens:** You get a friend request or message from a fake AI Fud account.
- **Warning signs:** Few followers, strange usernames, prize claims.
- **What to do:** Don't reply. Report the account.

5. ATM Skimming

- **What happens:** Fake devices or cameras steal your card info at an ATM.
- **Warning signs:** Loose devices, strange screens or errors.
- **What to do:** Cover your PIN. Report suspicious ATMs.

6. SIM Swap Fraud

- **What happens:** Your mobile network stops working. Scammers try to get your OTPs.
- **Warning signs:** Sudden loss of service, calls asking to confirm details.
- **What to do:** Call your mobile provider. Never share OTPs.

7. Business Email Scam

- **What happens:** You get an email from a "supplier" asking you to pay to a new account.
- **Warning signs:** Urgent payments, email address looks slightly different.
- **What to do:** Call your supplier on their real number. Don't click links.

8. Identity Theft

- **What happens:** Your Emirates ID, birth date, or bank info is stolen.
- **Warning signs:** Strange account activity, unknown requests for info.
- **What to do:** Watch your accounts closely. Report any issue quickly.

3. General Safety Tips

- Always check messages and calls before responding.
- Don't share your PIN, password, or OTP.
- Use safe internet connections.

- Don't send money to unknown people.
- Teach family and friends about scams.
- Be extra cautious of AI-generated voices pretending to be someone you trust. Verify all urgent requests through another trusted channel.

4. Points to take considering

- Scammers use urgency, secrecy, and lies.
- Stay alert and verify before acting.
- Never share secret information.
- Report suspicious cases quickly.

5. Report Fraud

Al Fuad Exchange:

- Landline: +971 (4) 221 1117
- Mobile: +971-505364545
- Email: customerservice@alfuadexchange.com

Authorities:



DUBAI POLICE

- Toll Free number 901
- E-Crime Online Platform



ABU DHABI POLICE

- "Aman" service hotline at 800-2626
- adpolice.gov.ae



MINISTRY OF INTERIOR

- 800500
- moi@moi.gov.ae

Knowledge is your best protection. Stay aware, stay safe with Al Fuad Exchange.

التوعية بالاحتيال والإبلاغ عنه

مركز التوعية للمستهلكين – شركة الفؤاد للصرافة

في الفؤاد للصرافة، نحرص على مساعدتك لاتخاذ خيارات مالية آمنة. يقدم مركز التوعية لدينا نصائح وإشعارات وإرشادات بسيطة لحماية نفسك من الاحتيال، والعمليات الاحتيالية، والمخاطر الأخرى.

1- كيف يمكن للمحتالين الاتصال بك

يمكن للمحتالين الوصول إليك بعدة طرق:

- **المكالمات الهاتفية** – يدعون أنهم من البنوك أو الشرطة أو شركات، أو حتى أفراد عائلتك باستخدام تقنيات نسخ الصوت بالذكاء الاصطناعي. قد يقوم المحتالون بتسجيل عينة قصيرة من صوت شخص ما (أحياناً من وسائل التواصل الاجتماعي) واستخدام الذكاء الاصطناعي لتقليده. قد يتلقى الضحايا مكالمات تطلب تحويل أموال عاجلة أو معلومات سرية.
- **الرسائل القصيرة / واتساب** – رسائل عاجلة مزيفة أو روابط خبيثة.
- **البريد الإلكتروني** – إشعارات مزيفة، روابط تصيد احتيالي، أو مرفقات ضارة.
- **وسائل التواصل الاجتماعي** – حسابات مزيفة تدعي أنها رسمية.

نصيحة: لن تطلب منك الشركات الحقيقية أبداً مشاركة رقم التعريف الشخصي (PIN)، كلمة المرور، أو رمز التحقق (OTP) عبر الهاتف، البريد الإلكتروني، أو وسائل التواصل الاجتماعي. تحقق دائماً من الطلبات عبر قناة موثوقة ثانية قبل اتخاذ أي إجراء.

2- المواقف الشائعة للاحتيال

1. **البريد الإلكتروني الاحتيالي (Phishing Email)**
 - ما يحدث: تتلقى بريداً إلكترونياً يفيد بأن بطاقتك محظورة ويجب النقر على رابط أو الاتصال برقم معين.
 - علامات التحذير: نبرة عاجلة، روابط تطلب معلومات شخصية.
 - ما يجب فعله: لا تنقر على الرابط. تحقق مباشرة مع الفؤاد للصرافة.
2. **اليانصيب أو الجوائز المزيفة**
 - ما يحدث: رسالة تقول أنك فزت بجائزة وتطلب منك تقديم بيانات أو دفع رسوم.
 - علامات التحذير: طلب المال أو المعلومات الشخصية.
 - ما يجب فعله: الفؤاد للصرافة لا تطلب أبداً رسوماً. تحقق دائماً معنا.

3. مكالمة هاتفية تطلب رمز التحقق (OTP)
- ما يحدث: المتصل يدّعي أنه من البنك، الشرطة، أو حتى أحد أفراد العائلة باستخدام نسخ الصوت بالذكاء الاصطناعي ويطلب رمز التحقق أو بيانات البطاقة.
 - علامات التحذير: الضغط على الاستجابة بسرعة، طلب معلومات سرية.
 - ما يجب فعله: لا تشارك OTP أو PIN. أغلق المكالمة وأبلغ عن الحادثة.

4. حسابات وهمية على وسائل التواصل الاجتماعي
- ما يحدث: تتلقى طلب صداقة أو رسالة من حساب مزيف باسم الفؤاد.
 - علامات التحذير: عدد قليل من المتابعين، أسماء مستخدمين غريبة، أو ادعاءات بالجوائز.
 - ما يجب فعله: لا ترد. أبلغ عن الحساب.

5. سرقة بيانات أجهزة الصراف الآلي (ATM Skimming)
- ما يحدث: أجهزة أو كاميرات مزيفة تسرق بيانات بطاقتك عند استخدام الصراف الآلي.
 - علامات التحذير: أجهزة مفكوكة، شاشات غريبة أو أخطاء غير مألوفة.
 - ما يجب فعله: غطّ إدخال الرقم السري. أبلغ عن أي أجهزة مشبوهة.

6. احتيال تبديل بطاقة (SIM Swap Fraud)
- ما يحدث: يتوقف عمل شبكة هاتفك. يحاول المحتالون الحصول على رموز التحقق الخاصة بك.
 - علامات التحذير: فقدان الخدمة فجأة، مكالمات تطلب تأكيد البيانات.
 - ما يجب فعله: اتصل بمزود الخدمة. لا تشارك OTP أبدًا.

7. احتيال البريد الإلكتروني التجاري (Business Email Scam)
- ما يحدث: تتلقى بريدًا إلكترونيًا من "مورد" يطلب تحويل أموال إلى حساب جديد.
 - علامات التحذير: طلبات دفع عاجلة، عنوان البريد الإلكتروني مختلف قليلاً عن المعتاد.
 - ما يجب فعله: اتصل بالمورد على الرقم الحقيقي. لا تنقر على الروابط.

8. سرقة الهوية (Identity Theft)
- ما يحدث: يتم سرقة بطاقة الهوية الإماراتية، تاريخ الميلاد، أو معلومات البنك الخاصة بك.
 - علامات التحذير: نشاط غريب في الحسابات، طلبات غير معروفة للمعلومات.
 - ما يجب فعله: راقب حساباتك عن كثب. أبلغ عن أي مشكلة بسرعة.

3- نصائح السلامة العامة

- تحقق دائمًا من الرسائل والمكالمات قبل الرد.
- لا تشارك رقم التعريف الشخصي (PIN) ، كلمة المرور، أو رمز التحقق (OTP).
- استخدم اتصالات إنترنت آمنة.
- لا ترسل أموالاً لأشخاص مجهولين.
- قم بتعليم عائلتك وأصدقائك حول عمليات الاحتيال.
- كن حذرًا بشكل خاص من الأصوات المزيفة التي يتم إنشاؤها بالذكاء الاصطناعي والتي تدّعي أنها من شخص تثق به. تحقق من جميع الطلبات العاجلة عبر قناة موثوقة ثانية.

4- نقاط هامة يجب مراعاتها

- يستخدم المحتالون العجلة، السرية، والأكاذيب.
- كن يقظًا وتحقق قبل اتخاذ أي إجراء.
- لا تشارك المعلومات السرية أبدًا.
- أبلغ عن أي حالات مشبوهة بسرعة.

5- الإبلاغ عن الاحتيال

الفؤاد للصرافة:

- الهاتف الأرضي: +971 4 2211117
- الهاتف المحمول: +971 505364545
- البريد الإلكتروني: customerservice@alfuadexchange.com

الجهات الرسمية:

شرطة دبي



- رقم الهاتف المجاني 901
- E-Crime Online Platform
- **شرطة دبي**
DUBAI POLICE

شرطة أبوظبي



- الخط الساخن لخدمة "أمان" 800-2626
- adpolice.gov.ae
- شرطة أبوظبي
ABU DHABI POLICE

وزارة الداخلية



- 800500
- moi@moi.gov.ae
- UNITED ARAB EMIRATES
MINISTRY OF INTERIOR

المعرفة هي أفضل حماية لك. كن واعيًا، واحم نفسك مع الفؤاد للصرافة.