

Social Media Impersonation: Know the Signs

تعرف على علامات انتحال الشخصية عبر وسائل التواصل



What is Social Media Impersonation?

Social media impersonation is a type of fraud where scammers create fake profiles or hack existing accounts to pose as trusted individuals, brands, or organizations. Their goal is to gain your trust and trick you into sharing your personal information, make payments, or disclose sensitive banking details.



How Does the Fraud Work?

Fraudsters typically:

- Create fake social media accounts using stolen names, photos, or company branding to appear legitimate.
- Hack genuine accounts and use them to contact friends, followers, or customers.
- Send messages requesting urgent financial help, payments, or donations.
- Share suspicious links disguised as promotions, giveaways, or account verification requests.
- Impersonate banks or service providers to collect personal, banking, or security information.

Even if a request appears to come from someone you know, always verify its authenticity before taking any action.



How Can You Protect Yourself?

- Verify social media profiles before responding to messages or requests.
- Be cautious of urgent or unusual requests, even if they appear to come from someone you know.
- Avoid clicking on suspicious links shared through social media.
- Never share your personal information, banking details, passwords, or login details through social platforms.
- Report and block suspicious or impersonating accounts immediately.

Important Note: Banks and trusted organizations will NEVER ask for your passwords, OTPs, or banking details through social media.

**Best Regards,
United Arab Bank (P.J.S.C.)**



ما هو انتحال الشخصيات عبر وسائل التواصل الاجتماعي؟

يعتبر انتحال الشخصيات عبر وسائل التواصل الاجتماعي أحد أساليب الاحتيال التي يعتمد بها المحتالون على إنشاء حسابات وهمية أو يخترقون حسابات أخرى، ليتظاهروا بأنهم أشخاص أو علامات تجارية أو مؤسسات موثوقة بهدف كسب ثقتك ثم استدراجك لمشاركة معلوماتك الشخصية، أو إجراء دفعات، أو الإفصاح عن بياناتك المصرفية الحساسة.



كيف تتم عملية الاحتيال؟

يلجأ المحتال عادةً إلى الأساليب التالية:

- إنشاء حسابات وهمية على مواقع التواصل الاجتماعي باستخدام أسماء أو صور أو علامة تجارية لشركة لتبدو الحسابات موثوقة.
- اختراق حسابات حقيقية واستخدامها للتواصل مع الأصدقاء أو المتابعين أو العملاء.
- إرسال رسائل تطلب مساعدة مالية عاجلة أو إجراء دفعات أو تبرعات.
- مشاركة روابط تبدو كأنها عروض ترويجية أو جوائز أو طلبات للتحقق الحساب.
- انتحال صفة بنك أو جهة موثوقة للحصول على بياناتك الشخصية أو المصرفية أو الإفصاح عن الرموز السرية.

لذلك، احرص دائماً على التحقق وعدم القيام بأي إجراء حتى لو بدا لك الطلب من شخص تعرفه.



كيف تحمي نفسك؟

- تحقق من حسابات التواصل الاجتماعي قبل التجاوب مع أي رسالة أو طلب.
- احذر من الطلبات العاجلة أو غير المعتادة حتى لو كان الطلب من شخص تعرفه.
- لا تضغط على الروابط المشبوهة التي تصلك عبر وسائل التواصل الاجتماعي.
- لا تشارك بياناتك الشخصية أو المصرفية أو كلمات المرور أو معلومات تسجيل الدخول عبر منصات التواصل الاجتماعي.
- أبلغ عن الحسابات المشبوهة أو المزيفة واحظرها فوراً.

معلومة مهمة: البنوك والجهات والمؤسسات الموثوقة لن تطلب منك أبداً مشاركة كلمات المرور أو رموز OTP أو بياناتك المصرفية عبر وسائل التواصل الاجتماعي.

**مع فائق التقدير،
البنك العربي المتحد**

If you suspect any fraud or suspicious activity,
please report it to us immediately at **09Fraud@uab.ae**.

إذا ساورك شك بوجود عملية احتيال أو نشاط غير معتاد،
بادر إلى إبلاغنا فوراً عبر البريد الإلكتروني: **09Fraud@uab.ae**.

Download the UAB Mobile App
حمل تطبيق الهاتف المتحرك للبنك العربي المتحد



United Arab Bank (P.J.S.C) is licensed and regulated by the Central Bank of the UAE.

Connect with UAB
تواصل مع البنك العربي المتحد



البنك العربي المتحد (ش.م.ع) مرخص ومنظم من قبل المصرف المركزي لدولة الإمارات العربية المتحدة.