

Play Smart, Stay Safe: Spotting Online Gaming Scams

العب بذكاء، ولا تقع في الفخ: اكتشف احتيال الألعاب الإلكترونية.



What is Online Gaming Fraud?

Online gaming fraud happens when scammers target you through games, platforms, or player communities to steal your money, personal information, or account access. They usually exploit in-game purchases, reward offers, or direct messages to catch you off guard.



How the Scams Work ?

Fraudsters generally rely on a few common tricks:

- **Tempting Bait:** Promising free in-game currency, rewards, or upgrades to pull you in.
- **Fake Links:** Sharing malicious links disguised as giveaways, special deals, or account verification.
- **Deceptive Trust:** Posing as fellow players or game admins to trick you into sharing your login or personal details.
- **Account Hijacking:** Hacking gaming accounts to buy unauthorized purchases or target other players.

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



How You Can Protect Yourself?

Protecting your gaming identity comes down to a few core habits:

- **Lock Down Credentials:** Never share your login details or personal information to anyone.
- **Question "Free" Deals:** Avoid links offering rewards or deals that seem too good to be true.
- **Level Up Security:** Use strong, unique passwords and turn on two-factor authentication (2FA) where available.
- **Stick to Official Sources:** Only download games and updates directly from verified, official platforms.
- **Track Account Activity:** Regularly check your accounts for any unexpected charges, logins or activity.

Important Note: Legitimate gaming platforms will NEVER ask for your password or personal details through unofficial links or private messages.

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

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



ما هو الاحتيال في الألعاب الإلكترونية؟

يتم الاحتيال في الألعاب الإلكترونية عادةً عندما يستهدفك المحتالون عبر منصات الألعاب أو مجتمعات اللاعبين، بهدف سرقة أموالك أو معلوماتك الشخصية أو الوصول إلى حسابك. حيث يستغل المحتالون عمليات الشراء داخل اللعبة، أو عروض المكافآت، أو الرسائل المباشرة للإيقاع بك دون أن تشعر.



كيف تتم عملية الاحتيال؟

يلجأ المحتال عادةً إلى الأساليب التالية:

- **العروض المفترية:** وعود زائفة بتوفير عملات مجانية للألعاب أو مكافآت أو ترقية.
- **الروابط الوهمية:** إرسال روابط مشبوهة تبدو وكأنها هدايا مجانية أو عروض خاصة أو طلبات للتحقق من الحساب.
- **انتحال الشخصية:** انتحال صفة لاعبين آخرين أو مشرفي اللعبة لكسب ثقتك ومشاركة بياناتك أو معلوماتك الشخصية.
- **اختراق الحساب:** اختراق حسابات اللاعبين لإجراء عمليات شراء غير مصرح بها أو استهداف لاعبين آخرين.

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



كيف تحمي نفسك؟

لحماية حسابك وهويتك، يجب اتباع الخطوات التالية:

- **احم بياناتك:** لا تشارك أبداً بيانات تسجيل الدخول أو معلوماتك الشخصية مع أي شخص.
- **لا تثق بالمعروض المجانية:** تجنّب الضغط على الروابط التي توفر مكافآت أو أي عروض قد تبدو حقيقية.
- **ارفع مستوى الأمان:** استخدم كلمات مرور قوية وفريدة، وفعل خاصية المصادقة الثنائية (2FA) إذا كانت متوفرة.
- **التزم بالمصادر الرسمية:** حمل الألعاب والتحديثات فقط من المنصات الرسمية والموثوقة.
- **راقب نشاط حسابك:** تحقق بانتظام من حسابك لرصد أي عمليات شراء غير شرعية أو عمليات تسجيل دخول أو أنشطة مشبوهة.

من المهم أن تعلم: منصات الألعاب الموثوقة لن تطلب منك أبداً كلمة المرور أو بياناتك الشخصية عبر روابط غير رسمية أو رسائل خاصة.

مع فائق التقدير،
البنك العربي المتحد

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.