



What is Phishing?

Phishing is a common cybercrime where fraudsters attempt to trick individuals into revealing sensitive information by posing as trusted organizations. These frauds typically appear as emails, messages, or web-sites that look legitimate but are designed to steal confidential data such as login credentials, personal information, or financial details.

How Does the Fraud Work?

Fraudsters often:

- Send emails, SMS messages, or links that appear to come from banks, government authorities, or well-known companies.
- Direct victims to fake websites that closely resemble legitimate platforms.
- Encourage users to click on links or download attachments to "verify" their accounts or resolve urgent issues.
- Capture login credentials, banking information, or personal data entered on the fake websites.
- In some cases, install malicious software (malware) that allows criminals to gain unauthorized access to devices and accounts.

How Can You Protect Yourself?

- Be cautious of unsolicited emails, messages, or links requesting personal or financial information.
- Always verify website addresses before entering login credentials or sensitive data.
- Avoid clicking on suspicious links or downloading attachments from unknown sources.
- Never share passwords, PINs, OTPs, or banking details through email or messaging platforms.
- Access banking or financial services only through official websites or trusted mobile applications.

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

ما هو التصيد الاحتيالي؟

يعدّ التصيد الاحتيالي أحد أكثر الجرائم الإلكترونية شيوعاً، حيث يحاول المحتالون خداع الأفراد للكشف عن معلومات حساسة من خلال انتحال صفة جهات موثوقة. وعادةً ما تأتي هذه المحاولات عبر رسائل البريد الإلكتروني أو الرسائل النصية أو المواقع الإلكترونية التي تبدو شرعية، لكنها مصممة لسرقة بيانات سرية مثل بيانات تسجيل الدخول أو المعلومات الشخصية أو التفاصيل المالية.

كيف تتم عملية الاحتيال؟

غالبًا ما يقوم المحتالون بما يلي:

- إرسال رسائل بريد إلكتروني أو رسائل نصية أو روابط تبدو وكأنها صادرة عن بنوك أو جهات حكومية أو شركات معروفة.
- توجيه الضحايا إلى مواقع إلكترونية مزيفة تشابه بشكل كبير المواقع الرسمية والشرعية.
- حث المستخدمين على النقر على الروابط أو تنزيل المرفقات بحجة "التحقق" من حساباتهم أو معالجة أمور عاجلة.
- الاستيلاء على بيانات تسجيل الدخول أو المعلومات المصرفية أو البيانات الشخصية التي يتم إدخالها عبر المواقع المزيفة.
- في بعض الحالات، تثبيت برامج خبيثة تمكن المجرمين من الوصول غير المصرح به إلى الأجهزة والحسابات.

كيف يمكنك حماية نفسك؟

- توخّ الحذر عند تلقي رسائل أو روابط غير متوقعة تطلب منك مشاركة معلومات شخصية أو مالية.
- تحقق دائماً من عنوان الموقع الإلكتروني قبل إدخال بيانات تسجيل الدخول أو أي معلومات حساسة.
- تجنب النقر على الروابط المشبوهة أو تنزيل المرفقات من مصادر غير معروفة.
- لا تشارك أبداً كلمات المرور أو الأرقام السرية أو رموز التحقق لمرة واحدة (OTP) أو البيانات المصرفية عبر البريد الإلكتروني أو تطبيقات المراسلة.
- استخدم الخدمات المصرفية أو المالية فقط من خلال المواقع الإلكترونية الرسمية أو التطبيقات الموثوقة.

وتفضلوا بقبول فائق الاحترام والتقدير،
البنك العربي المتحد (ش.م.ع.)

If you suspect any fraud or suspicious activity, please report it to us immediately on **800474** or **info@uab.ae**.

إذا كنت تشك في أي عملية احتيال أو نشاط مشبوه، فيرجى إبلاغنا بذلك فوراً على الرقم **800474** أو البريد الإلكتروني **info@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.