# دليل وارشادات امن المعلومات

إن المحافظة على سرية وأمن المعلومات الشخصية الخاصة بك هي من أهم أولوياتنا

هذه النشرة التعريفية تقدم مبادئ توجيهية عامة بشأن كيفية حماية المعلومات والتي تبدأ "بك"، من حيث اتباعك لأفضل الممارسات في العمل والمنزل

## كيف يمكن أن تحمي نفسك؟

لحمايتك من محاولات الاحتيال أو الوصول غير المصرّح به إلى بياناتك، نرجو منك الالتزام بالتعليمات التالية عند التعامل مع شركة إيلاف الأردنية للحلول المتكاملة:

- لا تشارك أي معلومات شخصية أو مالية إلا من خلال الوسائل الرسمية المعتمدة من الشركة، مثل:
  - التطبيق الرسمي
  - الموقع الإلكتروني
  - الاتصال الهاتفي من الأرقام المعتمدة والمعلنة على موقعنا
- في حال تلقيت اتصالًا أو رسالة مشبوهة، ننصحك بعدم التفاعل معها، والاتصال فورًا بخدمة العملاء للتحقّق من صحتها
- موظفو شركة إيلاف الأردنية للحلول المتكاملة لن يطلبوا منك أبدًا:
  - كلمة المرور
  - رمز التحقق (OTP)
  - بيانات البطاقة أو الحساب البنكي كاملة
- إذا كان إن هناك شيء غريب أو غير مريح، قم بأنهاء المكالمة مباشرة وتواصل معنا عبر القنوات الرسمية للتأكد من صحة الطلب

## ما هي الهندسة الاجتماعية (Social Engineering)

الهندسة الاجتماعية هي أسلوب يُستخدم لخداع الأشخاص بهدف الحصول على معلومات شخصية أو سرية، مثل كلمات المرور أو أرقام الحسابات البنكية، دون الحاجة إلى اختراق الأنظمة التقنية.
يقوم المحتال في هذه الحالة بالتظاهر بأنه جهة موثوقة، مثل موظف شركة أو مؤسسة رسمية، ليكسب ثقة الضحية ويدفعها إلى كشف معلوماتها الخاصة دون أن تشعر بالخطر. تتعدد طرق الهندسة الإجتماعيةو ومنها:

- المكالمات الهاتفية
- الرسائل النصية القصيرة
- البريد الإلكتروني
- الرسائل عبر وسائل التواصل الاجتماعي أو حتى الرسائل الورقية أو الفاكس

**نصيحة مهمة:** لا تشارك معلوماتك الشخصية أو السرية مع أي جهة ما لم تكن متأكدًا من هويتها، واحرص دائمًا على استخدام القنوات الرسمية المعتمدة من شركة إيلاف الأردنية للحلول المتكاملة

## ما هو خداع البريد الإلكتروني (E-mail Spoofing)

خداع البريد الإلكتروني هو أسلوب يستخدمه المحتالون لإرسال رسائل بريد إلكتروني تظهر وكأنها من جهة موثوقة بينما في الحقيقة تكون من مصدر مختلف تمامًا.
الهدف من هذا النوع من الخداع هو كسب ثقتك ودفعك للقيام بإجراء معين، مثل تحويل الأموال أو تزويدهم بمعلومات حساسة مثال على ذلك:
قد يصلك بريد إلكتروني يبدو مطابقًا للبريد الذي تتعامل معه عادة، ويطلب منك تحويل مبلغ مالي إلى حساب جديد
في الواقع، هذا البريد مرسل من محتال، وليس من الجهة الحقيقية التي تتعامل معها

**نصيحة مهمة:** تحقّق دائمًا من عنوان البريد الإلكتروني بدقة، ولا تتخذ أي إجراء مالي أو تشارك معلوماتك إلا بعد التأكد من أن الرسالة وصلت من جهة رسمية ومعروفة، وباستخدام القنوات المعتمدة من شركة إيلاف الأردنية للحلول المتكاملة.

## هجمات التصيّد والاحتيال (Phishing)

هجمات التصيّد هي أحد أساليب الهندسة الاجتماعية، حيث يقوم المحتالون بخداعك بهدف سرقة معلوماتك الشخصية مثل أرقام بطاقات الائتمان، كلمات المرور، بيانات الحسابات البنكية، وغيرها من المعلومات الحساسة
في هذا النوع من الهجمات، يُرسل المحتالون رسائل بريد إلكتروني أو رسائل نصية مزيفة المصدر، تبدو وكأنها صادرة من جهة موثوقة، مثل البنك أو شركة معروفة
تطلب هذه الرسائل منك إدخال معلوماتك الشخصية، أو الضغط على رابط يؤدي إلى موقع إلكتروني مزيف صُمّم ليبدو كالموقع الحقيقي

+962 (6) 200 4717
info@gatetopay.com
www.gatetopay.com
King Hussein Business Park - Building No. 23

تشمل طرق التصيّد المستخدمة ما يلي :

- رسائل البريد الإلكتروني
- الرسائل النصية القصيرة (SMS)
- المكالمات الهاتفية
- الرسائل عبر وسائل التواصل الاجتماعي

**نصيحة مهمة:** لا تضغط على أي رابط أو تشارك معلوماتك إلا بعد التأكد من مصدر الرسالة. وكن حذرًا من أي رسالة تطلب منك تحديث بياناتك أو التحقق من حسابك بشكل مفاجئ. لمزيد من الأمان، تعامل دائمًا مع شركة إيلاف الأردنية للحلول المتكاملة من خلال القنوات الرسمية فقط

## نصائح إضافية لحماية معلوماتك الشخصية

- لا تُدخل معلوماتك الشخصية أو بيانات بطاقتك الائتمانية إلا على مواقع إلكترونية موثوقة وآمنة
- تأكّد دائمًا من أن الموقع الذي تستخدمه يحتوي على علامة القفل في شريط العنوان ويبدأ بـ https://
- احرص على تحديث البرامج والتطبيقات بشكل دوري، وخاصة :
  - نظام التشغيل على جهاز الكمبيوتر أو الهاتف المحمول
  - تطبيقات الخدمات المصرفية
  - برامج مكافحة الفيروسات
- تأكّد من تثبيت برنامج حماية من الفيروسات، وابقِه محدّثًا باستمرار
- أغلق جهازك (الكمبيوتر أو الهاتف) في حال عدم استخدامه، لتقليل فرص الوصول غير المصرّح به
- لا تقم بتثبيت التطبيقات من مصادر غير موثوقة أو غير معروفة
- إنشاء واستخدام كلمات مرور قوية

كلمة المرور القوية هي خط الدفاع الأول لحماية حساباتك, تأكّد من أن

- لا تقل عن ٨ أحرف
- تحتوي على أحرف كبيرة وصغيرة
- تشمل أرقامًا ورموزًا
- لا تستخدم معلومات سهلة التخمين مثل اسمك أو تاريخ ميلادك
- لا تشارك كلمة المرور مع أي شخص، ولا تستخدم نفس الكلمة في أكثر من حساب

+962 (6) 200 4717
info@gatetopay.com
www.gatetopay.com
King Hussein Business Park - Building No. 23