إرشادات وتوعية بأمن المعلومات

مقدمة:

لطالما كانت الإدارة الفعالة للأمن السيبراني / أمن المعلومات من أولويات بنك الأردن سورية لإدارة المخاطر والحفاظ على سمعتها في السوق.

توفر سياسة أمن المعلومات مجموعة متكاملة من تدابير الحماية التي يجب تطبيقها بشكل موحد عبر بنك الأردن سورية لضمان بيئة تشغيل آمنة لعملياتها التجارية.

تُعتبر معلومات العملاء والمعلومات التنظيمية وأنظمة تكنولوجيا المعلومات الداعمة والعمليات والأشخاص الذين يقومون بإنشاء المعلومات وتخزينها واستردادها من الأصول المهمة للبنك.

يُعد توافر المعلومات وسلامتها وسريتها أمرًا ضروريًا لبناء والحفاظ على ميزتنا التنافسية، والتدفقات النقدية، والربحية، والامتثال القانوني، وصورة البنك المرموقة.

إنّ حماية بياناتك الشخصية والمالية في البنك هي أولى أولوياتنا.

نحن ملتزمون باعتماد وسائل الأمان الفعّالة عند جمع بياناتك ومعالجتها و نقلها و ضمن أفضل الممارسات العالمية و بما يلبي متطلبات السلطات الرقابية.

نصائح حول كيفية تلافي التصيّد الإلكتروني:

سعياً من بنك الأردن - سورية للحفاظ على السرّية المصرفية لعملائه الكرام، وبعد أن لوحظ التزايد في عمليات التصيّد الإلكتروني (Phishing) على بعض المواقع الإلكترونية أو عبر الرسائل القصيرة، نورد لكم نشرة توعوية حول كيفية تلافي التصيّد الإلكتروني.

ما هي رسائل التصيّد الإلكتروني (Phishing)؟

وسيلة من وسائل الاحتيال الإلكتروني والتي تكون على شكل رسائل بريد إلكترونية (E-MAIL) أو رسائل نصية قصيرة (SMS) تهدف إلى حث المتلقي لتلك الرسائل على الكشف عن المعلومات الخاصة به، مثل رقم بطاقة الائتمان ورقم الحساب أو كلمة السر أو غيرها، وترد تلك الرسائل عبر مواقع تبدو في ظاهرها معروفة للجميع، وتحظى بالمصداقية العالية، وفي الحقيقة إنها ليست كذلك.

كيف نميز رسائل التصيّد الإلكتروني (Phishing Messages) عن غيرها من الرسائل الأخرى ؟

عادة، تطلب منك تلك الرسائل الإدلاء بمعلومات خاصة بك، في حين أن الرسائل الواردة إليك من مواقع تمثل جهات معروفة مثل Bank Of Jordan Syria، eBay، Amazon أو غيرها لا يمكنها أن تطلب منك تقديم معلومات حول كلمة السر أو أية معلومات خاصة.

كيف تبدو رسالة التصيّد الإلكتروني؟

تبدو وكأنها واردة من موقع بنك الأردن - سورية الأصلي أو أي موقع آخر، وتطلب منك تحديث حسابك أو ما شابه، وهنا عليك ألا تستجيب لمثل تلك الرسائل، والتي يمكن أن تأخذ الأشكال التالية:

- الطلبات العاجلة حول تقديم المعلومات الشخصية.
- العبارات التي تطلب منك اتخاذ خطوات سريعة وعاجلة.
- الطلبات التي تدعوك إلى تقديم معلومات حول اسم المستخدم وكلمة السر وأرقام الحسابات...إلخ.

يمكن أن تتخذ رسائل التصيّد الإلكتروني شكل الرسائل ذات العنوان الغريب، وأن تكون على شكل رد غير عادي على عنوان.

تأكد من أن بنك الأردن - سورية لا يمكنه أن يطلب من عملائه الإدلاء بمعلومات حول اسم المستخدم أو كلمة السر عبر البريد الإلكتروني أو الهاتف أو أية وسيلة أخرى.

ماذا لو تلقيت أياً من رسائل التصيّد الإلكتروني (Phishing)؟

يرجى اتباع الخطوات التالية:

- عدم الرد عليها.
- عدم الاتصال برقم الهاتف الوارد في الرسالة.
- التبليغ عن الرسالة بالاتصال بمركز الخدمة الهاتفية لبنك الأردن - سورية على مدار الساعة.

ماذا لو تلقيت مكالمة هاتفية تطلب مني الإدلاء بمعلومات خاصة؟

امتنع عن تقديم أي معلومات بنكية خاصة بك ويجب عليك الاتصال فوراً بفرعك.

ما هي المعلومات البنكية الخاصة بي والتي يجب علي عدم الإفشاء بها للغير أياً كان، حتى لو كان موظف البنك؟

- الرقم السري الخاص ببطاقة الصراف الآلي أو البطاقة الائتمانية.
- اسم المستخدم والرقم السري الخاص بخدمة الإنترنت البنكية.
- الرقم السري أو اسم مستخدم الذي تقوم بإدخاله لكي تستخدم أياً من خدمات البنك الإلكترونية مثل (الصراف الآلي، خدمة الإنترنت البنكي، الموبايل البنكي).

ماذا يجب أن أفعل إن قمت بإدخال أية معلومات مالية أو شخصية ضمن مواقع التصيّد الإلكتروني (Phishing Website) أو إن كنت أحد ضحاياها؟

في مثل هذه الحالات، يرجى اتباع التعليمات التالية:

- الاتصال بالفرع، والإبلاغ عن البريد الوارد إليك، ونوع المعلومات التي قمت بإعطائها.
- اتباع تعليمات الفرع.
- تغيير كلمات السر الخاصة بكل الحسابات المصرفية الإلكترونية بشكل فوري.

كيف يحصل محتالوا التصيّد الإلكتروني على عنوان بريدي أو رقم هاتفي؟

عادة، لا يهاجم محتالوا التصيّد الإلكتروني الأفراد، بل يقومون بإرسال آلاف من رسائل البريد الإلكتروني (E-mail) أو الرسائل النصية القصيرة (SMS) إلى العديد من عناوين البريد الإلكترونية أو أرقام الهواتف بصورة عشوائية للحصول على بضع ضحايا.

كيف أحمي نفسي من رسائل التصيّد الإلكتروني؟

حافظ على معلوماتك الخاصة، ولا تُدل بها لأي أحد كان، وكذلك احذر من تقديم أية معلومات خاصة بك عبر رسائل البريد الإلكتروني أو الرسائل النصية القصيرة (SMS) أو النوافذ المنبثقة عن الروابط الإلكترونية (Pop-up) .

إن كنت بصدد زيارة موقع إلكتروني، قم بطباعة عنوان ذلك الموقع مباشرة في شريط العنوان في المستعرض (Internet Browser)، وليس الضغط على الرابط الإلكتروني الذي يمثله والموجود ضمن رسالة البريد الإلكتروني الواردة إليك للتأكد من أنك تزور موقعاً حقيقياً وليس مجرد موقع زائف أو مشبوه.

هل يمكن لبنك الأردن – سورية أن يطلب من المستخدمين تقديم معلومات حول كلمات السر أو اسم المستخدم؟

لا، إلا أنه يمكن له أن يتصل بك مباشرة عبر الهاتف أو عن طريق رسالة عادية أو غيرها من الطرق الأخرى لطلب معلومات عامة لا تتعلق بكلمات السر أو ما شابه، عليك عدم الإفشاء بهذه المعلومات (اسم المستخدم او كلمة السر) تحت أي ظرف من الظروف.

كيف يقوم بنك الأردن – سورية بالتواصل مع عملائه بشكل رسمي ومباشر للإفادة حول معاملاتهم؟

- من خلال تسجيلك في خدمة الرسائل النصية القصيرة أو على عنوان البريد الإلكتروني المزود مسبقاً من قبلك.
- نصائح حول كيفية تفادي الاحتيال الآلي (ATM Skimming).
- الاحتيال الآلي (ATM Skimming) وكيفية حدوثه.
- قيام الفاعل بمحاولة بتثبيت معدات وادوات مزيفة على أجهزة الصراف الالي، لجمع البيانات (رقم البطاقة والرمز السري) عن بطاقات الصرافة الآلية.

عزيزنا العميل، يرجى مراجعة النقاط التالية للتأكد من سلامة جهاز الصراف الآلي قبل القيام بعمل سحب او إيداع للنقود لتفادي الوقوع بمصيدة الاحتيال الآلي (ATM Skimming):

- عدم اخذ المساعده من اشخاص مجهولين عند استخدام الصراف الالي .
- قم بتغير كلمة المرور لبطاقة الصراف الالي من فتره الى أخرى .
- تحريك قارئ البطاقة، للتأكد من أن القارئ غير مزيف.
- التأكد من عدم وجود طبقة لوحة المفاتيح مزيفة فوق لوحة المفاتيح الاصلية.
- التأكد من عدم وجود طبقة لاصقة على لوحة المفاتيح حتى لا يتم نسخ الرمز السري.
- التأكد من عدم وجود كاميرا موجهة على لوحة المفاتيح، التي قد تتيح للسارق تسجيل الرمز السري.
- التأكد من إغلاق غطاء لوحة المفاتيح أثناء إدخال الرمز السري.

عزيزنا العميل، في حال العثور على أي من الأدوات المشتبه بها كما في النقاط السابقة، يرجى الاتصال فورا مع فرعك .

الهندسة الاجتماعية:

ما هي الهندسة الاجتماعية او الاحتيال الالكتروني عبر الانترنت (Social Engineering)

الهندسة الاجتماعية

هو أسلوب من أساليب الاختراق والاحتيال التي تعتمد على العنصر البشري حيث يستخدم المهاجم مهاراته في الاتصال مع الآخرين ويستخدم أساليب الخداع والحيل النفسية ليحصل منهم على المعلومات المطلوبة ليتمكن بواسطتها من القيام بعملية الاختراق او الاحتيال.

انتحال الهوية:

تتطلب الهندسة الاجتماعية عادة بعض أشكال انتحال الهوية من أجل كسب ثقة الضحية فمثلاً من الممكن أن ينتحل المهاجم صفة موظف لدى شركة او مسؤول علاقة عملاء من خلال احد صفحات التواصل الاجتماعي حيث يقوم المحتال بالتواصل مع الضحية، و غالباً ما يكون لديهم بعض المعلومات المتعلقة بها، وقد يتظاهرون بأنهم من موظفي البنك، أو غيرهم من الموظفين لدى مؤسسات تحظى بالثقة، ومن ثم يحاولون إقناع الضحية بتحويل المال أو سحب النقد وتسليمه والإفصاح عن معلومات أو بيانات خاصة (رقم الحساب ، اسم المستخدم، كلمات السر (PIN code ,OTP) ، رقم بطاقة الائتمان، رقم الهاتف).

علماً بأن المؤسسات المالية لا تقوم بطلب مثل هذه المعلومات التي قد يتم استخدامها للوصول إلى الموارد المالية أو المعلومات الحساسة.

أنواع الهندسة الاجتماعية:

1. هندسة قائمة على أساس بشري وهي جرائم تعتمد على الإنسان دون تدخل التقنية ومن أمثلة ذلك:

- **الإقناع**

هي هجمات تحدث من خلال التواصل مع الضحية عن طريق الهاتف او مواقع التواصل الاجتماعي، حيث يقوم المهاجم بالتواصل مُدعياً بأنه شخص ذو منصب أو مسؤولية وله صلاحيات ويقوم تدريجياً بسحب المعلومات من الضحية حتى يتمكن من الوصول لهدفه الرئيسي وهو الاحتيال أو الاختراق.

- **التجسس والتنصت**

يمكن سرقة كلمة المرور ومعلومات مهمة عن طريق مراقبة الضحية حين كتابتها أو التنصت والاستماع لمحادثة هاتفية لذلك يُنصح دائماً بتجنب كتابة كلمات السر والمعلومات الهامة على اوراق او أن يتم تبادلها مع اشخاص آخرين.

- **الاحتيال الصوتي (vising)**

هي من أكثر هجمات الهندسة الاجتماعية تحدث من خلال الهاتف، حيث يقوم المهاجم بالاتصال مُدعياً بأنه شخص ذو منصب وله صلاحيات ويقوم تدريجياً بسحب المعلومات من الضحية.

2. هندسة قائمة على أساس تقني وهي برامج وتقنيات تساعد المهاجم للوصول للمعلومة ومن أمثلة ذلك:

- **التصيد الإلكتروني (Phishing)**

يُعد أحد أهم طرق الهندسة الاجتماعية، وهو عبارة عن رسالة الكترونية تصل للضحية وتحتوي على Link لصفحة وهمية تظهر مشابهة تماماً للموقع الرسمي ومن الممكن ان تطلب من الضحية ادخال كلمة السر واسم المستخدم ومن ثم توجهه للصفحة الصحيحة بعد أن حصلت على البيانات السرية للضحية.

- **الرسائل المزعجة (spam)**

وهي عبارة عن كمية كبيرة من الرسائل الالكترونية يتم ارسالها بعناوين جذابة ويوجد بداخلها ما يسبب توقف الخدمة و/ أو سرقة المعلومات.

كيف تحمي نفسك؟

- لا تثق بأي عملية تواصل إن كانت عن طريق مكالمة هاتفية أو بريد الكتروني أو رسالة عن طريق مواقع التواصل الاجتماعي من أي شخص يطلب منك معلومات شخصية أو بنكية ويجب التأكد من هوية هذا الشخص من خلال الاتصال بالمصدر الطالب للمعلومات قبل مشاركة أي معلومة.
- تجنب وضع المعلومات الشخصية على الإنترنت قدر الإمكان.
- لا تشارك بياناتك الشخصية حتى مع أقرب الأشخاص إليك حمايةً لك ولهم.
- عدم الاحتفاظ بالأوراق والمستندات المهمة في أماكن غير آمنة.
- تجنب التفاعل مع الرسائل الإلكترونية أو الرسائل النصية أو رسائل مواقع التواصل الاجتماعي التي تحتوي على روابط مشبوهة.
- استخدم كلمة مرور قوية للخدمات المصرفية عبر الإنترنت واعمل على تغييرها باستمرار.

يجب أن تكون كلمة المرور قوية وألا تتضمن في تركيبها الكلمات التي يسهل على الأخرين إيجادها، وذلك وفق الآتي:

- يجب أن تتكون كلمة السر من الأحرف الكبيرة و الصغيرة، مع أرقام، و رموز (*،@ ، + ،.....).

- يجب عدم استخدام كلمات سر معروفة والتي يمكن معرفتها بسهولة، كالأسماء وتاريخ الميلاد أو أرقام الهواتف.
- يجب ألا يقل عدد محارف كلمة السر عن 8 خانات الى 20 خانة، تحتوي على رموز و ارقام و احرف
- يجب عدم استخدام أرقاماً أو حروف متكررة مثل (3333 أو AAAA).
- يجب عدم مشاركة كلمة السر مع اي شخص او كتابتها في مكان ظاهر.
- يجب تغيير كلمة السر باستمرار.