البنك العربي
ARAB BANK

١. توخ الحذر عند استخدام الإنترنت

- تصفح المواقع غير المعروفة يزيد من خطورة التعرض للفيروسات والشيفرات الضارة الأخرى.
- لا تقم بتحميل البرامج عن الإنترنت إلا إذا دعت الحاجة لذلك ومن المصادر الموثوقة فقط.
- تأكد من هوية الشخص المستلم للمعلومات الشخصية أو السرية الخاصة بك وكن متيقنا من حاجته للمعلومات ذات العلاقة.
- واذا تيقنت من شخصية الطرف الذي تتعامل معه، لا تطلعه أبدا على المعلومات الحساسة مثل الرقم السري وكلمات السر. ولا تقبل أبدا أي تواصل من شبكات لاسلكية مجاورة غير معروفة.

٢. احذر من عمليات الاحتيال على الإنترنت

- عمليات الاحتيال على الإنترنت (phishing) هي نوع من الخداع للحصول على بياناتك الشخصية (مثل أرقام البطاقات الائتمانية وكلمات السر وبيانات الحسابات البنكية...الخ) لغايات الاحتيال.
- قد يرسل محترفو الاحتيال آلاف الرسائل الإلكترونية (وحتى رسائل خلوية قصيرة) تبدو أنها من مواقع إلكترونية أو مصادر تثق بها، مثل البنك الذي تتعامل معه أو الشركة التي تصدر البطاقات الائتمانية، ويطلبون منك تزويدهم بالبيانات الشخصية عبر البريد الإلكتروني أو على موقع غير شرعي على الشبكة أسسوه لهذه الغاية.
- في حال وصلتك رسائل بريدية أو خلوية مشبوهة تبدو في ظاهرها أنها مرسلة من البنك الذي تتعامل معه، الرجاء القيام بما يلي:
  - لا ترد على الرسالة ولا تضغط أي رابط فيها أو تغير البريد الإلكتروني في أي حال.
  - اتصل بنا فورا.
- لا تقم بإدخال رقم البطاقة الائتمانية أو المعلومات الشخصية إلا في حالة أن تكون أنت المبادر بالتعامل مع الموقع أو أن تكون المواقع التي تتعامل معها موثوقة.
- راقب حركات حسابك المصرفي بشكل منتظم بحثا عن أية حركات مالية غير معروفة لديك، وإن كنت ترغب في أن نطلعك على كل حركة أجريت على حسابك البنكي أو بطاقتك الائتمانية، بادر بالتسجيل لخدمة الرسائل القصيرة التي نقدمها.
- لا تستخدم الخدمات المصرفية الإلكترونية في الأماكن العامة المفتوحة مثل مقاهي الإنترنت.
- إذا كنت تستخدم المودم الموصول بالكوابل أو DSL عندما تشبك على الإنترنت، لا تبق الاتصال فعالا عندما لا تحتاج لاستخدامه، ولا بأس في تثبيت برمجيات جدار ناري شخصية.

٣. حافظ على أمن جهاز الكمبيوتر الخاص بك

- قم بتفقد الحالة الأمنية لجهاز الكمبيوتر الخاص بك بشكل دوري ونفذ الإصلاحات المطلوبة والتحديثات والتبديلات.
- استخدم منتجات حديثة لمقاومة الفيروسات واختراقات الأنظمة فهي إحدى أكثر الوسائل فعالية في حماية جهاز الكمبيوتر.

٤. اعرف كيف تستجيب للحوادث

- تعلم كيف تستجيب للحوادث وكيف تميز الحادث وتدرك وقوع خطأ.
- تذكر أن الاستجابة السريعة يمكن أن تكون حاسمة، لذا عندما يحدث أمر خطأ أو تواجه حدثا مثيرا للشبهات الأمنية، قم بالإبلاغ عنه مباشرة
- إذا لم تعرف كيفية الإبلاغ عن الحادثة، اتصل بمركز الخدمة الهاتفية أو أقرب فرع مباشرة.

٥. تذكر أن أمن المعلومات هو مسؤولية الجميع

• من خلال حمايتك لنفسك والأنظمة التي تستخدمها، واستخدامها بالشكل الصحيح والحذر المطلوب، فإنك تصون أموالك وخصوصيتك وبياناتك الخاصة.

٦. ما هي الهندسة الاجتماعية؟

• إنها فن التلاعب بالناس بهدف الالتفاف على الأنظمة الأمنية والقيام بعمليات احتيال.

• وينطوي هذا الأسلوب على الحصول على المعلومات عبر الهاتف أو البريد الإلكتروني أو الفاكس أو البريد التقليدي أو الاتصال المباشر.

• ولاتخاذ إجراء مضاد، استخدم المنطق السليم ولا تكشف أيا من المعلومات التي قد تعرض بياناتك للخطر لأي كان.

• بغض النظر عن نوع المعلومات التي تطلب منك، فإننا ننصحك بالتالي:

[١] تحقق من هوية الشخص الآخر من خلال توجيه أسئلة طلبا لمعلومات محددة مثل الاسم الأخير والاسم الأول والدائرة ورقم الهاتف...الخ.

[٢] تأكد من صحة المعلومات التي حصلت عليها.

[٣] اسأل نفسك ما مدى أهمية المعلومات التي طلبت منك

٧. تزوير الرسائل الإلكترونية

• عندما تبدو الرسالة الواردة عبر البريد الإلكتروني أنها قادمة من مصدر ما، بينما هي في الحقيقة قادمة من مصدر آخر.

• ويهدف هذا التزوير في الغالب إلى خداع المستخدم لكي يقدم بيانات مهمة أو يكشف معلومات حساسة. (مثل كلمات السر).

• ومن الأمثلة على ذلك الرسائل الإلكترونية التي تدعي أنها مرسلة من قبل البنك وتطلب من العملاء أن يتبعوا رابطا إلكترونيا ويدخلوا أرقام بطاقاتهم الائتمانية أو كلمات المرور إلى خدمة الإنترنت أو الأرقام السرية.

• يجب أن تلاحظوا أن البنك يطلب منك تغيير الأرقام السرية / كلمات المرور بشكل متكرر، لكنه لا يحدد أبدا الكلمة أو الرمز البديل ولا يرسل لك رسالة إلكترونية تحتوي على رابط يطلب تغييرها.

• كما ان المؤسسات المالية الحقيقية لن تطلب منك أبدا أن ترسل لها أية معلومات مهمة عبر البريد الإلكتروني أو الهاتف أو الفاكس أو البريد التقليدي أو أية وسيلة أخرى.

٨. ضرورة فهم مسألة كلمات السر وعملية التأكد من الهوية

• كلمات السر والطرق الأخرى للتأكد من الهوية مثل أجهزة التوثيق «tokens» هي وسائل تستطيع الأنظمة من خلالها أن تتأكد من هويتك التي تدعيها.

• في حال استخدم شخص آخر اسم المستخدم وكلمة السر الخاصين بك على سبيل المثال، فإن النظام سيعتقد أن هذا الشخص هو أنت. وبإمكان هذا الشخص أن يقوم بالعمليات التي تقوم بها (مثل العمليات المالية المصرفية).

• لا تطلع أحدا على كلمات السر ورموز الدخول الخاصة بك، ولا تخزنها في ملفات غير مشفرة، ولا تكتبها إلا إن حفظتها في مكان آمن مغلق.

• يجب أن تكون كلمات السر قوية ومعقدة بحيث لا يمكن تخمينها أو فكها بسهولة.

• استخدم كلمات سر معقدة لا تقل عن ستة رموز واستخدم الأرقام والحروف والرموز الخاصة فيها.

٩. أمن التراسل - البريد الإلكتروني والرسائل الفورية- عمليات الاحتيال الإلكتروني من جديد

- البريد الإلكتروني و الرسائل الفورية هي وسائل رائعة للتراسل لكن يمكن استخدامها أو إساءة استخدامها بطرق متنوعة.
- القاعدة العامة هي ألا ترسل معلومات سرية أو حساسة مثل الأرقام السرية وأرقام الحسابات أو أية معلومات سرية عبر رسالة إلكترونية أو رسالة فورية غير مشفرة.
- لا تفتح أية رسالة مشكوك فيها، يمكن ان تكون محتوية على مرفقات غير معتادة أو أن تكون من مرسل مجهول.
- تذكر أن البريد الإلكتروني عرضة للتزوير والتدليس لذا عليك أن تفكر بمنطق سليم قبل أن تفترض أن الرسالة شرعية.
- احذر من الاحتيال الإلكتروني الذي هو نوع خاص من الهجوم حيث يرسل لك المحتال معلومة كاذبة مثل: «يقوم البنك حاليا بإجراء تحديث للبيانات وينصح العملاء بالدخول إلى حساباتهم وتحديث قوائم التفضيلات الخاصة بحساباتهم وأي تقصير في القيام بذلك سوف يؤدي إلى إلغاء حسابكم أو الخدمة عنكم». ويتم ارشاد العميل إلى موقع إلكتروني مزور للحصول منه هناك على معلومات تتعلق بحسابه أو بطاقات الائتمان الخاصة به.