نصائح مشروع التوعية المصرفية التابع للجنة خبراء المخاطر المعلوماتية في القطاع المالي

Banking Awareness tips by the financial sector information risk committee

Chapter 1: Traveling Tips

الفصل الأول: نصائح للسفر

General Tips

نصائح عامة

Memorize your PIN and e-banking passwords as they are personal information. Do not write your PIN or e-banking passwords down.	تذكر الرقم السرى الخاص ببطاقتك المصرفية وكلمة سر حساب الانترنت البنكي الخاص بك ولا تكتبهما في أي مكان لأنها معلومات شخصية وحساسة.
Do not share your PIN and e-banking information with anyone as the bank will not be responsible of any issues resulting from such action.	لا تفصح عن الرقم السرى الخاص بالبطاقة وكلمه سر حساب الانترنت البنكي لأى أحد وأعلم أن البنك لن يكون مسئولا عن أي عواقب تنجم عن هذا الإفصاح.
Do not forget your card after using the ATM or after paying at the merchant.	لا تنسى استرداد بطاقتك بعد استخدام جهاز الصراف الآلي أو الدفع لدى البائع.
Update your banking/personal information directly in the bank's branch.	حديث بياناتك البنكية/الشخصية من خلال فروع البنك الذي تتبع له.
Protect your PIN, type it yourself and hide it while keying.	احمِ الرقم السري لبطاقتك ,أكتبه بنفسك ولا تدع أحد يتمكن من رؤيته خلال الكتابة.
Call your bank immediately if: 1. lost your payment card. 2. a suspicious transaction or a transaction that you do not recognize occurred. 3. the ATM retained your card.	أتصل بالبنك فوراً في الحالات التالية: 1. إذا فقدت بطاقتك. 2. في حال اشتبهت بوجود عمليه بنكية لم تقم بها. 3. إذا لم تستطع استرداد البطاقة من الصراف الآلي.
Use preferably an ATM that is in public clear sights.	يفضل استخدام أجهزة الصراف الآلي المرئية جيدا والتي توجد في أماكن عامة.
Make sure nobody is watching you while keying your PIN, stay alert.	توخَ الحذر وتأكد من عدم وجود أي شخص قريب يمكنه رؤية الرقم السرى الخاص ببطاقتك.
Do not use an ATM where the keypad or the card slot is not properly attached or looks suspicious (fake card slot or something comes out of it).	لا تستخدم أجهزه الصراف الآلي إن كانت لوحة الأرقام أو فتحه إدخال البطاقة غير مثبتة جيدا.
Keep all receipts and transaction records with you.	احتفظ بكل الإيصالات والمستندات الخاصة بالعمليات التي قمت بها.
Wait as long as possible to withdraw your cash at the ATM, if you do not receive the money call the bank immediately while standing in front of the ATM.	انتظر قدر الإمكان لاستلام النقود من جهاز الصراف الآلي وإذا لم تستلمها اتصل بالبنك فورا أثناء تواجدك أمام الصراف الآلي.

Before Travel Tips

نصائح قبل السفر

Check the limit of your credit card and its expiry date.	راجع مقدار الحد الأقصى المسموح به للبطاقة وتاريخ انتهاء صلاحيتها.
Make sure you have the bank's contact numbers before you travel and that the bank has your up to date information.	تأكد أن لديك أرقام الاتصال بالبنك، وأن البنك لديه كافه البيانات الحديثة للاتصال بك.
Take your mobile phone with you when you travel to receive transaction notifications.	تأكد من أخذ الهاتف المحمول الخاص بك عند السفر لتتمكن من استلام إشعارات عملياتك المصرفية.
Make sure that all the information written on your payment card is clear.	تأكد من وجود اسمك على البطاقة. في حال عدم وجوده اتصل بالبنك.

During Travel Tips

نصائح أثناء السفر

Keep your payment card safe, treat it as money.	حافظ على بطاقة الدفع الخاصة بك وتعامل معها كأنها نقود.
Make sure you are reachable by phone and or email so the bank can contact you.	تأكد من أن البنك يمكنه الاتصال بك عبر هاتفك المحمول أو من خلال بريدك الالكتروني.
Make sure that you are handling your card while paying or you are keeping it in sight.	ناول البائع البطاقة بنفسك أثناء عمليه الدفع وأبقها تحت رقابتك.
Do not carry all your payment cards at the same time.	لا تحمل جميع بطاقاتك في نفس الوقت.
Keep some money for emergencies.	احتفظ ببعض النقود للطوارئ.

After Travel Tips

نصائح عند الرجوع من السفر

Change your online banking passwords regularly, and particularly after returning from travel.	غير رقمك السرى الخاص بالعمليات المصرفية في الانترنت باستمرار وخاصة بعد الرجوع من السفر.
Review your bank account transactions after your trip and compare with the payments and receipts kept during your holidays	راجع معاملاتك المصرفية التي قمت بها وقارنها بالإيصالات التي احتفظت بها معك لمدفوعاتك خلال الرحلة.
If fraudulent transactions happens follow up on your return.	إذا اشتبهت أن هناك عمليات تمت بطريقة احتيالية بعد عودتك أتصل بالبنك وأستبدل البطاقة/البطاقات المستخدمة أثناء الرحلة.

Chapter 2: Online Purchasing Tips

الفصل الثاني: نصائح عمليات الشراء عبر الانترنت

Research the merchant before placing an order: Always buy from reputable stores and resellers websites. Reliable companies should advertise their physical business address and at least one phone number, either for customer service or for ordering products. Call the phone number and ask questions to determine if the business is legitimate.

- Make sure the website is reputable. If you are uncertain, order over the phone instead of online
- Check for anything that looks unfamiliar, unprofessional, or out of place to you.
- Check the amount before placing the order
- Site spoofing - Websites that appear professionally designed and legitimate with the purpose of collecting sensitive information from unsuspecting visitors. These website can be detected by carefully checking the URL.
- Never respond to or open internet links or attachments in unsolicited emails.

تحرى عن التاجر قبل التسوق منه عبر الإنترنت :

- اشتري دائما من مواقع متاجر و بائعو بالتجزئة حسنو السمعة .
- الشركات الموثوقة لابد ان تسوق لعنوانها التجاري و رقم هاتف واحد على الاقل لخدمة العملاء او لطلب المنتجات .
- اتصل على رقم الهاتف وابدأ بطرح الاسئلة لتتمكن من تحديد قانونية العمل التجاري .
- تأكد من سمعة الموقع الالكتروني، و بإمكانك الطلب عن طريق الهاتف بدلا من الموقع اذا لم تكن متأكدا .
- تحقق من اي شي غير مألوف او غير مهني او في غير محله .
- تحقق من الكمية قبل اتمام عملية الطلب .
- تحايل المواقع الالكترونية: هي تلك المواقع التي تبدو قانونية و مصممة بحرفية بهدف جمع معلومات خاصة من الزوار الذين ينقصهم الوعي. ويمكنك تحديد تلك المواقع عن طريق مراجعة العنوان الإلكتروني بدقة.
- لا تتجاوب أبدا او تفتح الروابط الالكترونية او المرفقات الخاصة بالرسائل الالكترونية غير موثوقة او معلومة المصدر.

Shop at secure websites: A secure website uses encryption technology to transfer information from your computer to online merchant's computer system which keeps safe confidential information such as credit card details. You may identify a secured web site by:

- Looking for "Https" in the web address or URL (when you enter your personal or private information). This means that the information is encrypted between your browser and the site you are purchasing from, which keeps it safe from prying eyes. Don't let sites keep your credit card information on file.
- Making sure there is a tiny closed padlock in the address bar, or on the lower right corner of the window.
- Always check for the browser "lock" icon, but understand that this only signifies a secure communication channel, not necessarily a legitimate Web site.

تسوق في المواقع الالكترونية الآمنة : تستخدم المواقع الالكترونية الآمنة تكنولوجيا التشفير لنقل الملفات من جهاز الحاسب الخاص بك الى نظام الحاسب الخاص بالتاجر في الشبكة الالكترونية ، والذي بدوره يحافظ على سرية المعلومات مثل تفاصيل البطاقة الائتمانية. يمكنك التعرف على المواقع الالكترونية الآمنة:

- يمكنك ذلك بالنظر الى "Https" في URL او شريط العنوان (عند إدخال البيانات الشخصية او المالية). ويعني ذلك سرية المعلومات المتداولة بين المتصفح الخاص بك والموقع الالكتروني الذي تحاول الشراء منه وهذا بدوره يبقيه بمأمن من أعين المتطفلين. لا تسمح للمواقع الالكترونية الاحتفاظ بالمعلومات الخاصة ببطاقتك الائتمانية في ملف .
- تأكد من وجود قفل صغير الحجم في شريط العنوان ، او في الزاوية السفلية من الجهة اليمنى في نافذة العرض.
- تأكد دائما من وجود رمز القفل في المتصفح ، ولكن اعلم ان وجود الرمز يدل على قناة اتصال آمنة ولكن لا يدل بالضرورة على شرعية الموقع الالكتروني.

Keep your system and web browser software up to date: Make sure you install all the latest updates for your system and internet web browser software. Keeping your browser and operating

الحفاظ على تحديث برمجيات النظام و متصفح المواقع : تأكد دائما من تثبيت التحديثات الأخيرة للنظام و لبرنامج متصفح مواقع الانترنت. الحفاظ على تحديث المتصفح ونظام التشغيل لديك يضمن لك سلامة الاعدادات وفعاليتها العالية في الأداء.

system up to date will ensure that these settings are safeguarded and performing as well as possible.

Install and keep up to date your security software (firewall, antivirus and anti-spyware software): It's important to install and keep this software up-to-date, and perform regular scans of your computer to help protect you from such threats as viruses, spyware, spam and generally safeguard your personal information. A number of different providers produce complete security software packages. Review all packages available in assessing which security software is best for you.

احرص على تثبيت برمجيات الأمن وتحديثها باستمرار(**firewall, antivirus and anti-spyware software) : من المهم القيام بتثبيت هذه البرمجيات وتحديثها باستمرار ، كما انه من المهم القيام بفحص الحاسب الالكتروني (scan) بشكل دائم للحفاظ عليه من التهديدات المتمثلة بالفيروسات** viruses**او ملفات التجسس** spyware **او الرسائل الإلكترونية التطفلية spam**، وحماية معلوماتك الخاصة . هناك عدد من الشركات تقوم بتزويد حزم برمجيات امنية كاملة . قم باستعراض الحزم المتوفرة بهدف تقييمها واختيار البرمجيات الامنية المناسبة لك.

Save all transaction details and regularly check your bank statements: Print out or make note of the seller's identification, the item description and the time, date and price you paid or bid on the item. Print and save copies of your order confirmation screen and all email communications. **Regularly check statements** for any transactions that look suspicious. If any found, report it immediately to your bank

- **You can also request that your bank send sms confirmations of online transactions. This will provide you with an early warning of any fraudulent activity.**

احفظ كل المعلومات المتعلقة بالمعاملات المصرفية و راجع كشوفك المصرفية بشكل دائم :
احتفظ بنسخة او دون ملاحظة تعريفية بالبائع ، وصف المنتج ، وكذلك الوقت والتاريخ والسعر المدفوع او عروض الأسعار على المنتج. قم بالاحتفاظ بنسخ مطبوعة من شاشة تأكيد الطلبات وكل التعاملات التي تمت عن طريق البريد الالكتروني. تحقق باستمرار بشأن المعاملات المصرفية المشبوهة واخبر البنك اذا وجدت اي منها .

- **يمكنك كذلك ان تطلب من البنك ارسال رسالة الى هاتفك لتأكيد المعاملات التي تمت في الانترنت وهذا من شأنه ان يزودك بتحذير مبكر حول اي عملية احتيال.**

Use your personal computer and private Wi-Fi for online shopping rather than a public computer and Wi-Fi.

استخدم جهاز الحاسوب الخاص بك و اتصل بشبكة خاصة بدلا من استخدام اجهزة الحاسوب العامة و الشبكات العامة.

Make sure that you logout from the shopping website.

تأكد دائما من تسجيل الخروج من حسابك الخاص في موقع التسوق.

Do not disclose your online payment and shopping passwords. For example, PayPal account, MasterCard securecode, VISA verified by VISA and online shopping account.

- When registering a memorable name, avoid using a family member's name or your children's names etc. - use an alternative which cannot be easily guessed by fraudsters
- Use a strong password—at least eight characters, with a combination of numbers, letters, and punctuation symbols.
- Don't use the same password for banking that

لا تفصح عن مدفوعاتك في الانترنت او عن كلمة المرور الخاصة بالتسوق . على سبيل المثال : حسابك الخاص في موقعPayPal او MasterCard securecode او VISA verified
تفادى ذكر اسماء ابنائك او عائلة والدتك قبل الزواج عند تسجيل كلمة تذكيرية في الموقع ، واستخدم بدلا عن ذلك البدائل التي يصعب على المحتالين تخمينها .

- استخدم كلمة مرور قوية بحيث لا يقل فيها عدد الرموز عن 8 ، وان تكون عبارة عن مجموعة من الأرقام والحروف وعلامات الترقيم .
- لا تستعمل في تعاملاتك المصرفية كلمة مرور مستخدمة في حساباتك الخاصة الاخرى على الانترنت.
- احرص ان تكون كلمة المرور في مكان آمن ، لا تخزنها في ملف في جهاز الحاسوب ولا تدونها على ورقة ملاحظة

you use for other online accounts.

- Keep your password safe—don't leave it in a file on your computer or in a sticky note on your monitor.
- Change your password periodically.

ملصقة على شاشة العرض .

- غير كلمة المرور بشكل دوري .

Chapter 3: Phishing Spam Tips

الفصل الثالث: رسائل الاحتيال الإلكترونية

Phishing is the act of obtaining information by pretending to be a legitimate source. Phishing could occur in two ways:

1. You reply to an email that asks for your personal or secretive information.
2. You open an attachment or a link provided in an email.

The following is a list of information you should pay attention to before giving out:

- ID number
- Bank account number
- Full Name Company you work for
- Credit card number
- Credit limit
- The number of cards you have
- Information about the last transaction you made

الاحتيال الالكتروني: هو عملية طلب معلومات عن طريق التظاهر بشرعية المصدر. يظهر التحايل الالكتروني في حالتين:

عند الرد على بريد الكتروني يطالبك بذكر معلوماتك الخاصة او السرية .
او عند فتح ملف مرفق او رابط في البريد الالكتروني .
يجب عليك ان تأخذ المعلومات التالية بعين الاعتبار قبل تقديمها للغير:

- رقم الهوية
- رقم حساب البنك
- الاسم الكامل
- مكان العمل
- رقم البطاقة الائتمانية
- السقف الائتماني
- عدد البطاقات التي تمتلكها
- معلومات حول آخر عملية مصرفية قمت بها

Protect

الوقايه

Update your computer on regular basis.	قم بتحديث جهازك بشكل دوري.
Update your browser and the browser's plug-ins regularly.	قم بتحديث المتصفح الالكتروني و جميع الوظائف المرافقة الخاصة به دورياً.
Install the necessary software to protect your device, such as firewall, spam filters, anti-virus and anti-spyware, and ensure that they are updated regularly.	قم بتحميل وتحديث برامج الجدار الناري و برامج منع الرسائل الإلكترونية المزعجة و برامج المكافحة الفيروسات و برامج مكافحة التجسس لحماية جهازك.
Never type secretive (e.g. passwords or PIN) or personal information (e.g. name, location or salary) on shared or public devices.	لا تقم ابدا بطباعة معلوماتك الخاصة و السرية على اجهزه مشتركة او عامة.
Check your transactions regularly. If you see any unusual transaction that you have not made, contact your bank immediately.	راجع تعاملاتك المصرفية بشكل دوري. في حال شكك باي معاملة غير معتادة في حسابك، قم بالاتصال بالبنك فوراً.
Change your email or your online banking account passwords regularly.	قم بتغيير كلمات المرور الخاصة ببريدك الالكتروني و حسابك المصرفي الالكتروني بشكل دوري.
Do not reply emails with personal information.	لا تقم بالرد على الرسائل الإلكترونية بمعلومات شخصية.

Detect

تحرى

Avoid responding to an email that:	تجنب الرد على أي بريد الكتروني بالمواصفات التالية:

1. Contains jargons, poor grammar or spelling mistakes. 2. Asks for your personal information. 3. Creates a sense of urgency. 4. Is not signed with the bank's logo or contact information.	1. اذا احتوى على اخطاء املائه و لغوية. 2. اذا طلب منك معلومات شخصية. 3. اذا اختلق حالة بالغة الاهمية. 4. اذا لم يحتوي على شعار و توقيع البنك و بيات الاتصال.
Never respond to calls or emails that ask for secret information such as PIN or passwords.	لا ترد على أي بريد الكتروني او مكالمة تطالبك بكلمة المرور او الرقم السري الخاص بحسابك المصرفي.
Never respond to calls or emails that ask for personal or banking information e.g. credit card number, bank account number, id, name or phone number.	لا تتجاوب مع اي بريد الكتروني او اتصال يطالب بمعلومات خاصة او معلومات مصرفية مثل: رقم بطاقة الائتمان او رقم حسابك المصرفي او رقم الهوية او اسمك او رقم هاتفك.
Verify the identity of a caller before giving out any of your personal information, and directly call the call center.	تحقق من هوية المتصل قبل الادلاء باي من معلوماتك الشخصية مع اجراء اتصال هاتفي على الفور بمركز الاتصال .
Do not open email attachments unless you expect and trust them.	لا تفتح او تحمل مرفقات البريد الالكتروني الا اذا كنت تتوقعها.
Avoid opening URLs and attachments that you receive by email, unless you expect them (e.g. password resetting URLs).	تجنب الضغط على الروابط التي تصلك عبر البريد الإلكتروني الا في حال توقعك وصولها، كروابط تغيير كلمت السر.
If you would like to visit your bank's website, type the address on the browser yourself.	قم بطباعة موقع البنك في المتصفح بنفسك ، اذا اردت تصفح موقع البنك .
React	**استجب**
inform your bank Immediately about any suspicious email or phone call that ask for your banking information.	اعلم البنك باي بريد الكتروني او مكالمه تصلك مشكوك بها تستعلم عن معلوماتك المصرفية.
Contact your bank immediately if you believe that you have given your financial information while answering a phone call or an email.	اخبر البنك على الفور في حال ادلائك بمعلوماتك المصرفية و الشخصية عبر الهاتف او البريد الالكتروني.
Change your email or online banking account passwords immediately if you suspect that your passwords might have been compromised.	قم بتغيير الكلمات السرية الخاصة ببريدك الالكتروني او حسابك البنكي فورا اذا شككت بأنه تم اختراقها.
Contact your bank immediately,If you receive a transaction message from your bank that you do not recognize.	تواصل مع البنك في الحال، اذا استلمت رسالة على هاتفك بشأن معاملة مصرفية غير مألوفة .