بنك بيبلوس
العراق

إشعار أمان تطبيق الخدمات المصرفية عبر الهاتف الجوّال

أمن الخدمات المصرفية عبر الهاتف الجوّال

يعدُّ أمن هاتفك الذكي أو أيّ جهاز محمول آخر في غاية الأهمية، خصوصاً إذا كنت تستخدمه في الخدمات المصرفية. يجب أن تهتم بأمن هاتفك الجوّال بنفس القدر بنفس القدر الذي تهتم به بأمن حاسوبك. في حال فقدان هاتفك أو سرقته، عليك إبلاغ البنك على الفور لمنع وصول الغير مصرّح به إلى حساباتك أو سرقة هويتك أو أشكال الاحتيال الأخرى.

يقدّم تطبيق الخدمات المصرفية عبر الهاتف الجوّال من بنك بيبلوس مجموعة كاملة من التشفير والحماية التي يجب استخدامها في الخدمات المصرفية الإلكترونية. ومع ذلك، كما هي الحال في المجالات الأخرى حيث أصبحت التكنولوجيا أكثر تقدماً، لا يمكنك أبداً أن تكون مؤمناً او محتاطاً تماماً.

من هذا المنطلق، ثمّة بعض الاحتياطات التي يجب أن تأخذها في الاعتبار متى قرّرت اللجوء إلى الخدمات عبر الهاتف الجوّال.

1. إستخدم القفل التلقائي. تأكّد من ضبط جهازك لإقفال نفسه تلقائياً بعد عدم استخدامه لفترة زمنية محدّدة، وهو ما يستلزم، إذا أمكن، إدخال كلمة مرور أبجدية-رقمية قوية لفتحه. هذا الإجراء يساعد في منع المستخدمين غير المصرّح لهم من الوصول إلى البيانات والموارد المخزّنة في جهازك في حال فقدانه أو سرقته، أو إذا لم تكن موجوداً للإشراف على استخدامه.

2. ثبّت كلمة مرور قوية لحسابك. لا تستخدم اسمك أو تاريخ ميلادك أو أيّ معلومات شخصية أخرى يمكن كشفها بسهولة في كلمة المرور الخاصّة بك، إذ إنّ ذلك قد يساعد المخترقين في فكّ تشفيرها. بالإضافة إلى ذلك، حاول تغيير كلمة المرور الخاصة بك بشكل متكرّر.

3. لا تخزّن معلومات شخصية أو أيّ معلومات حسّاسة في جهازك الجوّال. إذا وصل أيّ طرف غير مصرّح له إلى جهازك، ستكون حينها أكثر عرضةً للخطر في حال خزّنتَ معلومات شخصية في الجهاز مثل كلمات المرور وأرقام الحسابات. يُوصى أيضاً بحذف سجلّ المتصفّح والرسائل النصّيّة والملفات من جهازك بانتظام.

4. إبق على اطلاع بجميع التحديثات المتعلقة بحاسوبك المحمول أو غير المحمول، علماً بأن الأجهزة الجوّالة تحتاج إلى تحديثات لتصحيح نقاط الضعف وإصلاح مشكلات البرامج، التي تتطلّب منك حرصاً على إجراء التغييرات اللازمة بصورة منتظمة.

5. إحرص على تنزيل برمجية الحماية ضد الفيروسات. يجب أن يكون هذا البرنامج قادراً على فحص الجهاز، وتحديد البرامج الضارّة وإزالتها، والتحقّق من خلوّ التطبيقات من البرامج الضارّة قبل تنزيلها من متاجر التطبيقات.

6. إبتعد من نقاط اتصال الإنترنت اللاسلكي (واي فاي) العامّة. معظم نقاط اتصال الإنترنت اللاسلكي (واي فاي) العامّة غير آمنة، ما يعني أنّ أيّ شخص متصل بنقطة الاتصال هذه قد يكون قادراً على مراقبة ما تفعله. إستخدم فقط شبكة إنترنت لاسلكي آمنة (اتصالات لاسلكية شفّرة) أو اتصال "3 جي" أو "4 جي" لمشغّل شبكة الهاتف الجوّال. من المفيد أيضاً تعطيل شبكة الإنترنت اللاسلكي (واي فاي) عندما لا تكون قيد الاستخدام ممّا يقلّص فرصة الاتصال عن طريق الخطأ بشبكة غير آمنة أو مشبوهة.

7. يمكن أن يكون "البلوتوث" ضارّاً. في الأماكن العامة، يمكن للآخرين كشف جهازك والوصول إليه عبر "البلوتوث". إذا حصل ذلك، سيتم إرسال إخطار لتنبيهك. ومع ذلك، يكمن الخيار الأكثر أماناً في تعطيل تشغيل "البلوتوث" أو إبقائه في وضع غير قابل للكشف وذلك لجعله غير مرئي للأجهزة الغير موثوقة.

8. إحرص دائماً على حماية بطاقة وحدة تعريف المشترك (SIM) الخاصّة بك من خلال كلمة مرور. في حال فقدان جهازك الجوّال أو سرقته، سيساعد ذلك في حماية أيّ معلومات خاصّة وحسّاسة.

9. توخّ الحذر عند تنزيل التطبيقات. إحرص على تنزيل تطبيقات الهاتف الجوّال فقط من مصادر موثوقة، ويُفضّل أن يكون المصدر أحد متجرَي "آبل" أو "غوغل بلاي"، وذلك لتتجنب تنزيل التطبيقات التي تحتوي على برمجيّات خبيثة أو رموز ضارّة أخرى.

10. إقرأ التفاصيل الدقيقة. إمنح نفسك لحظات لقراءة سياسة خصوصية التطبيق لتكون على دراية بما يفعلونه بمعلوماتك الخاصّة وما إذا كان التطبيق سيعرض هذه البيانات لمستخدمين آخرين أو أيّ مشترٍ محتمَل.

11. كن حذِراً عند استخدام تطبيقات الشبكات التواصل الاجتماعي. قد تكشف هذه التطبيقات عن معلومات شخصية (أرقام الهواتف الجوّالة، وأسماء الأصدقاء الموثوق بهم، وما إلى ذلك) أكثر مما تريد لجهات غير مقصودة. كن حذِراً بشكل خاصّ عند استخدام الخدمات التي تتعقّب موقعك.

12. لا تُخضع جهازك المحمول لعمليّة "روت" أو "كسر الحماية". "كسر الحماية" هي عملية إزالة الميزات المقفلة أو القيود التي يفرضها نظام تشغيل "روت" الخاص بك (مثال آي أو أس أو أندرويد). إذا أقدمتَ على كسر أمن الشركة المصنّعة في جهازك، لا تكون بذلك قد أبطلت ضمانتك فحسب، بل تجعل جهازك أيضاً أكثر عرضةً لهجمات المحتالين.

13. تأكّد من حذف جميع التفاصيل الشخصية متى قرّرت بيع هاتفك الذكي. إذا كنت ستبيع هاتفك الذكي، من الضروري أن تحذف جميع المعلومات الشخصية أوّلاً. يمكن أن يشمل ذلك الرسائل النصّيّة والرسائل الإلكترونيّة والصور وتفاصيل الاتصال وروابط الإنترنت. يمكن للمجرمين استخدام مثل هذه المعلومات لارتكاب عمليات احتيال ضدك و/أو انتحال صفتك.

14. لا تفتح أبداً الملفات المرفقة ولا تُقدم على تنزيل التطبيقات من مصادر غير موثوقة. يستخدم المحتالون المستندات والتطبيقات الهشّة لنشر برامجهم الضارّة (برمجيّاتهم الخبيثة) وتعريض هواتف الضحايا الذكيّة للخطر. لا تُقدم البتّة على فتح ملف مرفق أو تنزيل تطبيق من شخص أو موقع إلكتروني أو أيّ مصدر آخر لا تعرفه أو لديك شكوك بشأنه.

15. أبلغ عن فقدان جهازك المحمول أو سرقته. في حال فقدت جهازك، أبلغ عن ذلك فوراً من خلال زيارة فرعك أو الاتصال بمركز خدمة العملاء على الرقم 9647511205050+ كي نتمكّن من تعطيل حسابك للخدمات المصرفية عبر الهاتف الجوّال وردع أيّ محاولة لسرقة الهوية.

16. كن مستعدّاً لمسح بيانات جهازك. في حال فقدان جهازك أو سرقته، يجب أن تعرف كيفية مسح البيانات من بُعد، أي إزالة جميع بياناتك الشخصية وإعادة الجهاز إلى حالته الأولى لدى التّصنيع. تأتي أجهزة "آيفون" و"آيباد" و"بلاكبيري" و"ويندوز 7" مزودة بهذه الإمكانية المضمّنة في أنظمة التشغيل الخاصة بها، ويمكنك تنزيل تطبيقات "أندرويد" تقوم بهذا العمل أيضاً.

17. إحرص دائماً على تسجيل الخروج. عند الانتهاء من الاطّلاع على رصيدك، أو تحويل الأموال بين الحسابات، أو دفع فاتورة، تأكّد من تسجيل الخروج من حسابك. كجزء من ميزات الأمان التي نوفّرها، سيتولّى تطبيق الهواتف الجوّالة والصفحة الشبكيّة (ويب) الخاصّين ببنك بيبلوس تسجيل خروجك تلقائيّاً بعد خمس دقائق من عدم النشاط، ولكن يجب ألّا تترك الأمر للحظّ: أمورٌ كثيرة يمكن أن تحدث في غضون الخمس دقائق.