

الخدمات
المصرفية
الآمنة عبر
شبكة
الإنترنت



من نحن؟

أسس الجهاز القومي لتنظيم الاتصالات عام ١٩٩٨، وتم تحديد الإطار التشريعي والتنظيمي للجهاز بمقتضى قانون تنظيم الاتصالات رقم ١٠ لعام ٢٠٠٣ ، والجهاز هيئة قومية مسئولة عن تنظيم قطاع الاتصالات، يعتمد عمل الجهاز على مبادئ رئيسية منها المحافظة على مبدأ الشفافية والمنافسة الحرة والخدمة الشاملة وحماية حقوق المستخدم وعدم الإحتكار.

من أهم أهداف الجهاز ضمان حصول مستخدمى الاتصالات على أنسب الأسعار وأجود خدمة من خلال مشغلى الخدمات، والعمل على تحسين الخدمات لمواكبة أحدث وسائل التكنولوجيا والتطور الهائل فى مجال الاتصالات وتكنولوجيا المعلومات.

ومن منطلق تنفيذ أهداف الجهاز، تم تأسيس لجنة لحماية حقوق المستخدمين فى أغسطس عام ٢٠٠٤ والتي تتيح الفرصة للتواصل المباشر مع كافة شرائح مستخدمى خدمات الاتصالات من خلال حملات التوعية والإجراءات المختلفة للتواصل مع مجتمع المستخدمين. وتشكل اللجنة من شخصيات عامة ذات خلفيات متنوعة ويرأسها السيد الرئيس التنفيذى للجهاز القومى لتنظيم الاتصالات، وتجتمع اللجنة بصفة منتظمة.

وفى إطار تفعيل حق كل مستخدم لخدمات الاتصالات فى التمتع بجودة عالية للخدمات التى يحصل عليها والحصول علي معلومات واضحة ووافية وكذلك اشتراطات صحية وبيئية سليمة، قام الجهاز بإنشاء مركز اتصال، وحدد له الخط الساخن (١٥٥)، والرقم المجانى (٠٨٠٠٣٣٣٠٣٣٣) حيث يستقبل الشكاوى

والأعطال والإستفسارات من كل المواطنين فى مصر كمستوى ثانى لحل الشكاوى فى حالة عدم تلقى الشاكى الحل من قبل مقدم الخدمة، علي مدار اليوم طوال ايام الاسبوع.

كذلك يمكنك زيارة الموقع الإلكتروني الخاص بالجهاز www.tra.gov.eg لمعرفة أهم أخبار الاتصالات وتكنولوجيا المعلومات المحلية والعالمية، وكذلك الإطلاع على كل ما يتعلق بسوق الاتصالات داخل جمهورية مصر العربية.

أو مراسلة الجهاز على:

العنوان: القرية الذكية، مبنى B٤، الكيلو ٢٨ طريق القاهرة الإسكندرية الصحراوى، القاهرة.

تليفون: ٠٢٣٥٣٤٤٠٠٠

فاكس: ٠٢٣٥٣٤٤١٥٥

بريد إلكترونى: info@ntra.gov.eg

www.youtube.com/user/CRPCNTRA YouTube

www.facebook.com/CRPC.NTRA f

twitter.com/NTRAEGYOFFICIAL Twitter



"يكمن للمستخدم إدارة وتلبية احتياجاته المصرفية دون الحاجة إلى وجوده الفعلي في مقرات البنوك"

أصبحت قدرة الأفراد على القيام بإجراءات الخدمات المصرفية عبر شبكة الإنترنت (online banking services) عاملاً يضيف الكثير من التغييرات على نمط حياتهم، فمنذ أن تم استخدام هذه الخدمات استطاع المستخدمون توفير الوقت وتوفير وقتاً كبيراً من جراء الانتظار في البنوك.

يرجع رواج ونجاح تلك الخدمات إلى تمكينها للمستخدم من إدارة وتلبية احتياجاته المصرفية دون الحاجة إلى وجوده الفعلي في مقرات البنوك، ولكن للأسف استطاع المحتالون مواكبة الأمر حيث زادت حدة ووتيرة الجريمة الإلكترونية ذات الصلة بالخدمات المصرفية.

ولكن لحسن الحظ، سيكون أي مستخدم فطن لشبكة الإنترنت قادراً على الاستمرار في ممارسة أنماط حياتهم المصرفية عبر الإنترنت إذا ما التزم ببعض النصائح والاقتراحات المقدمة له، وفيما يلي بعضها منها:

يجب أن تتمكن من الحصول على حلول وبرامج جيدة لمكافحة الفيروسات والحائط الناري لمنع الاختراق:

يجب أن تستخدم برمجيات وحلولاً لمكافحة الفيروسات كالحائط الناري (Firewall) لمنع الاختراق، تجدر الإشارة إلى أن البرامج الضارة قد أصبحت معقدة ومتطورة جداً هذه الأيام وأي جهاز حاسب يفتقد إلى وجود نظام قوي محدث مضاد للفيروسات سيتعرض إلى مخاطر كبيرة للغاية.



إن الأجهزة المصابة بالفيروسات خاصة بالبرمجيات الخبيثة معرضة لكثير من المخاطر، فقد تقوم بكتابة وإرسال بياناتك المصرفية إلى البنك الذي تتعامل معه عبر شبكة الانترنت ولكن تلك المعلومات يمكن أيضا أن تصل دون علمك لبعض المجرمين في مكان ما من العالم.

ولحسن الحظ هناك الكثير من البرامج والحلول الجيدة المجانية التي تم تصميمها لمكافحة الفيروسات إذا كنت لا ترغب في دفع مقابل للحصول على تلك الحلول.

إذا كنت تعتقد أن الجهاز الخاص بك قد تم اختراقه، يجب أن تتصل بالبنك الذي تتعامل معه و قم بإيقاف التسهيلات المصرفية الالكترونية الخاصة بك حتى تقوم بتنظيف جهازك.

قم بتحديث المتصفح الخاص بك:

إن قيامك بإجراء بسيط مثل تحديث متصفح الويب الخاص بك بانتظام يمكن أن يحافظ على أمنك، إن القائمين على تصنيع متصفح الويب يقومون باستمرار بتحديث برامج التصفح الخاصة بهم عندما يتم الكشف عن أي نقاط ضعف يمكن النفاذ منها أو عندما يقوموا بتثبيت وتركيب تدابير أمنية إضافية في تطبيقاتهم. إن استخدامك لإصدار قديم لمتصفح الإنترنت يشبه تماما المشي ليلا دون وجود مرافقين لك أو حراس يحمونك من أي اعتداء.

اختر مكانا آمنا للقيام بمعاملاتك الالكترونية المصرفية:

لا تقم أبدا بإجراء أي معاملات مالية عبر شبكة الانترنت في الأماكن العامة، وإذا كنت تقوم بالاتصال بشبكة الإنترنت من أماكن معينة مثل المقاهي باستخدام خدمة الواي فاي المجانية فقد تكون معرضا لأحد المتطفلين على نفس شبكة الواي فاي، فلا تقوم بالنفاذ إلى شبكة

الانترنت إلا في أماكن آمنة مثل المنزل والمكتب الخاص بك (إذا كنت متأكدا من أن الشبكة آمنة).

راقب جيدا ما يجري على شاشة جهازك:

لا تقم بالنقر على أي رابط من المفترض أن يقودك إلى موقع البنك الذي تتعامل معه. قد يبدو هذا الرابط مشابها للرابط الخاص بهذا البنك ولكن في واقع الأمر قد يكون موقعا وهميا تم إنشاؤه لالتقاط التفاصيل المصرفية الخاصة بك وسرقة أموالك. يجب أن تلاحظ جيدا عنوان الرابط الالكتروني أو الموقع الخاص بالبنك والمدرج على المتصفح وتأكد من أنه عنوان الويب الصحيح لذا يجب أن تحفظ عن ظهر قلب عنوان الموقع الالكتروني للبنك الذي تتعامل معه، وتكتبه بنفسك في كل مرة.

تتمتع معظم النظم المصرفية الالكترونية بمستويات من التدابير الأمنية وتشمل خطوتين يتم من خلالهما الدخول إلى الموقع وذلك عبر بعض الصور أو العبارات التي قمت بتحديدتها مسبقا التي تظهر على الشاشة قبل كتابة كلمة المرور الخاصة بك، يجب أن تتأكد كل مرة أن الصور أو العبارات صحيحة.

"لا تطلب البنوك من عملائها

إعادة التحقق من تفاصيل حساباتهم المصرفية من

خلال رسائل البريد الإلكتروني كما

إنها لا تقوم

بتعليق حساباتهم

من خلال البريد

الإلكتروني"

**"لا تقم
أبدا بتقديم
المعلومات
السرية الخاصة
بحسابك إلى
أي شخص
بما في ذلك
موظفي البنك
الذي تتعامل
معه"**

تجاهل رسائل البريد الإلكتروني والرسائل النصية القصيرة:

لا تطلب البنوك من عملائها إعادة التحقق من تفاصيل حساباتهم المصرفية من خلال رسائل البريد الإلكتروني كما إنها لا تقوم بتعليق حساباتهم من خلال البريد الإلكتروني، كما إنها لا تقوم بعمل هذا من خلال الرسائل النصية. يمكنك بشكل آمن تجاهل أي طلبات من هذا القبيل. بالإضافة الى ذلك لا تقم أبدا بإرسال التفاصيل الخاصة بتسجيل الدخول وكلمة المرور الخاصة بك عبر البريد الإلكتروني.

تحقق من أكواد ورموز المعاملات البنكية:

يتعين عليك دائما التحقق من رقم حساب الغير المبين في الرسالة النصية التي يتم إرسالها للتحقق من الحساب والتي تظهر عند إجراء المعاملة المصرفية. إذا تم الكشف عن حسابك الإلكتروني، فإنك سترسل المال إلى شخص آخر غير الشخص المقصود. قد يبدو لك أنك ترسل مبلغا ماليا لابنك على سبيل المثال ولكن يتمكن أحد الفيروسات أو البرمجيات الخبيثة التي أصابت جهازك من تغيير تفاصيل حسابك المصرفي سرا عندما قمت بكتابتها وأصدرت تعليماتك إلى البنك الذي تتعامل معه لإرسال أموالك إلى مكان آخر. يمكنك عن طريق رسالة التحقق وأيضا من خلال سجلات المعاملات الالكترونية الخاصة بك أن تقوم بإيقاف عملية الاحتيال قبل أن ينتهز المحتالون الفرصة ويستولوا على أموالك.



المعاملات الهاتفية:

إذا لم تكن متأكدا من أي طلبات أو تعليمات أو اتصالات هاتفية تتلقاها، لا تتردد في الاتصال بخط المساعدة الخاص بالبنك الذي تتعامل معه للحصول على مزيد من المعلومات، في الوقت نفسه، كن حذرا للغاية إذا كنت تتلقى المعاملات من شخص يدعي أنه يقوم بتمثيل البنك الذي تتعامل معه، لا تقم أبدا بتقديم المعلومات السرية الخاصة بحسابك (مثل عبارة أو كلمة المرور، أو الصورة المختارة الخاصة بك) إلى أي شخص بما في ذلك موظفي البنك الذي تتعامل معه. إذا كنت تشك في هوية المتصل، يجب أن تقوم بإنهاء المعاملة واتصل بهاتف البنك بنفسك.

عندما يطلب أصدقاؤك المساعدة:

يستخدم مرتكبو الجرائم الالكترونية كافة أنواع الطرق للحصول على المعلومات المصرفية الخاصة بك. هناك طريقة واحدة شائعة يتم استخدامها كثيرا هذه الأيام ألا وهي استخدام حساب صديقك والذي يكون تم اختراقه يقوم بإرسال طلب لك للحصول على معلومات حسابك المصرفي من هذا الحساب. على سبيل المثال، قد تتلقى رسالة عبر بريدك الالكتروني أو رسالة فورية من صديق مقرب لك يخبرك فيها أنه موجود في مكان ما من العالم ولا يملك أي مبالغ مالية وبالتالي يطلب منك إرسال مبلغا ماليا له إلى رقم حساب مرسل في الرسالة، لا تصدق هذه الخدعة وهناك خدعة أخرى حيث يحاول المحتال أن يجعل الأمر يبدو حقيقيا وأن هذا الصديق قد أصيب في حادث محدد ويحتاج إلى مساعدة مالية عاجلة، ولذلك فيجب أن تتواصل مباشرة مع هذا الشخص وإذا كنت في شك من أمره يتعين عليك الاتصال بالشرطة للسؤال عن الأمر كله.

الشراء عبر شبكة الإنترنت:

يجب أن تمضي قدما وتقوم بعمليات الشراء عبر الإنترنت من مواقع معروفة لان هذه المواقع لديها أنظمة وإجراءات آمنة للتجارة الإلكترونية في المكان الذي يخلق بيئة آمنة للتسوق عبر شبكة الإنترنت، يجب أن تكون حذرا ولا تقوم بالشراء من مواقع مراوغة ولا تقوم بإجراء معاملات مباشرة مع المشتريين والبائعين الموجودين في المنتديات والمواقع الالكترونية. عند القيام بهذه الأنواع من المعاملات يجب أن تتوخي الحذر من تبادل الكثير من المعلومات المصرفية. فكل ما يريدون معرفته هو اسمك ورقم حسابك.

وباختصار، يجب أن تقوم بتحديث جهازك باستمرار وتركيب نظام قوي لمكافحة الفيروسات بحيث يكون قادرا على حمايتك عندما تكون متصلا بشبكة الإنترنت ويتعين عليك أن تتجاهل أي طلبات مشبوهة يتم إرسالها إليك فقط اتصل بالبنك من مكان آمن.

يجب أن تلتزم بالخطوات السابق ذكرها وبالتالي ستكون في مأمن من الجريمة الإلكترونية كما يتعين عليك أن تتقاسم هذه النصائح مع كافة معارفك وأقربائك الذين لديهم حسابا مصرفيا على شبكة الإنترنت.

لمستخدمي المحمول والانترنت والتليفون الثابت:

«إذا لم تتمكن من حل مشكلة واجهتك مع الشركة مقدمة الخدمة اتصل برقم ١٥٥ الخاص بمركز خدمة المستخدمين بالجهاز القومي لتنظيم الاتصالات الذي يعمل علي مدار اليوم طوال ايام الاسبوع



القرية الذكية مبنى B٤ - الكيلو ٢٨ طريق مصر/الاسكندرية الصحراوى
ت: +٢٠٢ ٣٥٣٤٤٠٠٠ ف: +٢٠٢ ٣٥٣٤٤١٥٥
الجهاز-القومي-لتنظيم-الاتصالات.مصر



www.youtube.com/user/CRPCNTRA YouTube

www.facebook.com/CRPC.NTRA Facebook

twitter.com/NTRAEGYOFFICIAL Twitter