كيف تحمي نفسك على الانترنت؟

من نحن؟

أسس الجهاز القومى لتنظيم الإتصالات عام ١٩٩٨، وتم تحديد الإطار التشريعى والتنظيمى للجهاز بمقتضى قانون تنظيم الإتصالات رقم ١٠ لعام ٢٠٠٣ ، والجهاز هيئة قومية مسئولة عن تنظيم قطاع الإتصالات، 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 الإتصالات على أنسب الأسعار وأجود خدمة من خلال مشغلى الخدمات، والعمل على تحسين الخدمات لمواكبة أحدث وسائل التكنولوجيا والتطور الهائل فى مجال الإتصالات وتكنولوجيا المعلومات.

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

وفى إطار تفعيل حق كل مستخدم لخدمات الاتصالات في 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 طوال أيام الاسبوع.

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

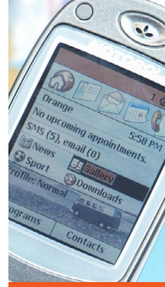
أو مراسلة الجهاز على:
العنوان: القرية الذكية، مبنى B٤، الكيلو ٢٨ طريق القاهرة الإسكندرية الصحراوى، القاهرة.
تليفون: ٠٢٣٥٣٤٤٠٠٠
فاكس: ٠٢٣٥٣٤٤١٥٥
بريد إلكترونى:info@ntra.gov.eg

www.youtube.com/user/CRPCNTRA

www.facebook.com/CRPC.NTRA

twitter.com/NTRAEGYOFFICIAL

لجنة حماية حقوق المستخدمين
الجهاز القومي لتنظيم الاتصالات
NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الاتصالات
Consumer Rights Protection Committee



كيف تحمي نفسك من البرمجيات الخبيثة والضارة:

عند استخدامك جهاز معين للدخول على شبكة الإنترنت، تحتاج إلى حماية نفسك من البرامج الضارة وهو ما يعني «البرمجيات الخبيثة» (malware) وهي برمجيات يتم تصميمها خصيصا للنفاذ إلى أو إتلاف جهاز الحاسب من دون علم مالكه. وهناك أنواع مختلفة من البرمجيات الخبيثة بما فيها برامج التجسس، والبرمجيات الضارة (key logger)، والفيروسات الضارة أو أي نوع من الشفرات الخبيثة التي تخترق وتتسرب الى أجهزة الحاسب.

عموما ينتهي الأمر بالمستخدم وقد أُصيب جهازه بالبرمجيات الخبيثة لأنه قد قام بتثبيتها عليه دون قصد، أكثر من مرة دون أن يعلم ويمكن لهذه البرمجيات الخبيثة أن تعمل فقط في حالة عمل الجهاز دون إيقاف.

البرمجيات الخبيثة تعمل مثل معظم البرمجيات الضارة أو الاحتيالية(spams) التي تتطلب بعض المساعدة الواعية أو غير الواعية من ضحاياها.

والسؤال: كيف يمكن أن ينتهي بك الأمر وأنت تقوم بتحميل وتثبيت برمجيات ضارة؟

أحيانا يتم جمع البرمجيات الخبيثة في حزمة واحدة مع البرامج القانونية المرخصة، وأحيانا يتم النقر على رسالة وهمية يمكن أن تحمل البرمجيات الخبيثة، إذا فإن أكثر الأساليب والأدوات شيوعا هي مرفقات رسائل البريد الإلكتروني.

عليك ان تتبع النقاط التالية حتى يمكنك حماية نفسك من البرمجيات الخبيثة:

» **يجب أن تحذر المواقع التي تزورها:**

العديد من المواقع التي تستضيف المحتوى الضار تستخدم لافتات وإعلانات تظهر فجأة، والتظاهر بأنها رسائل خاطئة أو تقدم جائزة للمستخدم. فعند زيارة هذه المواقع، يتم تحميل المحتوى الضار على الجهاز الخاص بك. و لذا يجب أن تتجنب الخضوع لأي دعوات من هذا النوع.

» **يجب أن تكون حذرا من المواد التي تقوم بتحميلها:**

لا تقم بتحميل البرامج من الموقع الالكترونية الحافلة بالإعلانات أو التي تعرض قوائم من البرامج المجانية، فهذه غالبا ما تكون ملفات وهمية، كن حذرا ووجه إليهم الأسئلة كما يتعين عليك أن تقوم بإخضاعهم للفحص بواسطة البرمجيات الأمنية (Security Software) وذلك قبل فتح أو تحميل البرامج واحرص على تحميل البرامج من المواقع أو الشركات المعروفة.

» **شراء البرمجيات الأمنية:**

لا يدرك العديد من المستخدمين أن استخدام البرامج المقرصنة(pirated software) لا يمكنها حماية جهاز الحاسب الآلي الخاص بالمستخدم ضد التهديدات والبرمجيات المقرصنة من الغير والتي قد تحتوي على فيروسات.

» **اتخاذ مزيد من الحذر عند استخدام برمجيات المحادثات:**

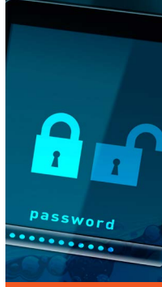
بما أن الملفات المشتركة على الشبكات القائمة علي المحادثات الكتابية او الصوتية او المرئية لا تتم مراقبتها فيمكن لأي شخص أن يرسل ويصدر أي شيء يريده عبر هذه الوسيلة، وعلى هذا النحو يتعين عليك أن تقوم باستمرار بفحص الملفات التي تقوم بتنزيلها قبل التشغيل.

» **قبول الملفات الواردة إلى البريد الالكتروني عند توقع ورودها:**

بعض التهديدات تكون قادرة على إتلاف الأجهزة وإرسال نسخ منها إلى قائمة جهات الاتصال الخاصة بالمستخدم وذلك بشكل تلقائي، فقد يبدو لك أن صديقك أرسل لك ملفا لكنك تدرك بعد ذلك أنه برنامج ضار .

» **معرفة تنسيق الملفات:**

يكون تنسيق الصور عادة هو (.gif، .bmp، .png، .jpg، JPEG، .tif) وتأتي الملفات القابلة للتنفيذ بامتداد (.exe - .bat-.com-.dll). إذا قال لك أحد الأشخاص أنه سيرسل لك صورة ولكن كان امتداد الملف (.exe) أو (.com) فلا تقم بفتحه لأنه قد يعرضك للخطر.



الجرائم المعلوماتية والتدابير الوقائية التي يجب اتخاذها

رسائل البريد الإلكتروني المزعجة (معلومات يجب معرفتها):

» **ما هي رسائل البريد الإلكتروني المزعجة «Spam»؟**

يطلق مصطلح رسائل البريد الإلكتروني المزعجة «Spam» على رسائل البريد الإلكتروني غير المرغوب فيها وهي الرسائل الاقتحامية والمزعجة المرسلة إلى حساب البريد الإلكتروني الخاص بك أو هاتفك المحمول، بعض هذه الرسائل يروج لمنتج أو يدعوك لزيارة موقع ما على شبكة الإنترنت والبعض الآخر يحاول خداعك وإقناعك بالاستثمار في مخططات احتيالية، أو الكشف عن تفاصيل حسابك البنكي أو بطاقتك الائتمانية وعادة ما تحمل تلك الرسائل المزعجة فيروسات.

» **كيف يمكنني معرفة هذا النوع من الرسائل ؟**

يمكنك معرفتها في حال تلقيك أي رسالة تجارية عبر البريد الإلكتروني أو هاتفك المحمول ولا تتوفر فيها الشروط التالية:

- موافقة متلقيها: يجب أن يتم إرسالها بعد أخذ موافقتك، سواء كانت تلك الموافقة صريحة أو ضمنية تم الاستدلال عليها من أي نشاط تجاري أو غيره من العلاقات القائمة بينك وبين إحدى الشركات أو الهيئات.
- بيانات دقيقة: يجب أن تحتوي على معلومات دقيقة عن الشخص أو الشركة المرسلة للرسالة.

"إذا تلقيت رسالة عبر بريدك الإلكتروني ووجدت أنها تبدو مريبة، أو يبدو مرسلها مشكوكا في أمره سيكون من الآمن لك أن تقوم بحذفها فورا دون أن تفتحها، وعدم الرد عليها وعدم الضغط على أي رابط بها"

- إلغاء الاشتراك : يجب أن تحتوي الرسالة على خاصية «إلغاء الاشتراك» والتي تسمح لك بأن تختار عدم تلقي أي رسائل أخرى من هذا المصدر.

» **ما الذي يمكنني فعله إذا تلقيت رسائل البريد المزعجة؟**

يتم إرسال بعض الرسائل غير المرغوب فيها بواسطة أشخاص احترفوا ارسال تلك الرسائل الاقتحامية محليا وعالميا، في حين يتم إرسال رسائل مزعجة أخرى من خلال شركات مرخصة قانونا، إذا كنت تتلقى رسائل تجارية عبر بريدك الإلكتروني أو هاتفك المحمول، سيكون لديك العديد من الخيارات.

» **لا تستجيب أبدا لفحوى الرسالة إذا بدت مريبة!**

إذا تلقيت رسالة عبر بريدك الإلكتروني ووجدت أنها تبدو مريبة، أو يبدو موضوعها أو مرسلها مشكوكا في أمره سيكون من الآمن لك أن تقوم بحذفها فورا دون أن تفتحها، كما يتعين عليك عدم الرد عليها وعدم الضغط على أي رابط، بما في ذلك وصلات «إلغاء الاشتراك»، لأن ذلك قد يؤدي بك إلى تلقي المزيد من هذا النوع من الرسائل.

لا تشتري منتجات أو خدمات يتم الإعلان عنها عبر رسائل البريد الإلكتروني المزعجة حيث أن الكثير منها يكون مزورا. إذا كان مصدر الرسائل يبدو حقيقيا، فاتصل بالشركة لتقديم شكوى من ذلك الامر. كما يمكنك الاتصال بها عن طريق الهاتف أو كتابةً لتقديم الشكوى وتطلب منهم أن يحذفوا بريدك من قوائم الشركة البريدية.

التفاعل عبر شبكات التواصل الاجتماع

إن التفاعل عبر شبكات التواصل الاجتماعي أو استخدام الخدمات القائمة على شبكة الإنترنت للتواصل والتفاعل مع الأفراد حول الأنشطة أو المصالح المشتركة قد تكون طريقة رائعة لتحقيق المصالح وإقامة وتعزيز العلاقات والصداقات القائمة والاشتراك في الألعاب وتبادل الأفكار.

بينما يوجد العديد من الفوائد التي تعود على المستخدم من التفاعل عبر شبكة الإنترنت، فإن قيامه بنشر الكثير من تفاصيل بياناته الشخصية في ملف شخصي على شبكة الإنترنت، أو في مدونته، أو حتى نشرها عبر قيامه بالدردشة مع مستخدمين آخرين قد يكون محفوفا بالمخاطر. إن سلوك المستخدم الذي يتسم بالإهمال والتسيب عبر شبكة الإنترنت يلحق به وبسمعته الكثير من الأضرار وذلك من جراء استخدامه غير المقصود لمعلوماته الشخصية أو عندما يصبح ضحية للاحتيال، أو يتعرض لسرقة هويته أو الاحتيال أو التحرش.

» **للحد من المخاطر التي تواجهك على شبكة الإنترنت:**

- يجب أن تتحكم في قدرة الآخرين على الوصول إلى المعلومات الخاصة بك.
- فكر جيدا قبل أن تعطي المعلومات الشخصية الخاصة بك (مثل اسمك، سنك أو عنوانك البريدي) أو التفاصيل المالية الخاصة بك (وخاصة تفاصيل بيانات بطاقتك الائتمانية أو حسابك المصرفي).
- قم بعمل إعداد جيد لكافة الإعدادات والإجراءات التي تؤمن خصوصيتك وأمنك على شبكة الإنترنت عندما تقوم بإنشاء ملف شخصي لك حتى تتأكد من أنك تعرف من يستطيع الوصول إلى المعلومات الخاصة بك.

» **الأضرار التي قد تلحق بسمعة المستخدم:**

يمكن أن يتم استخدام المعلومات أو الصور المنشورة في الملف التعريفي الخاص بالمستخدم على شبكة الإنترنت، أو المحادثات والصور او مدونته أو إحدى المواقع الإلكترونية أو يتم إخراجها من سياقها بغرض إحراج المستخدم أو الإضرار بسمعته، تذكر أن أي معلومات متاحة عنك على شبكة الإنترنت قد تظل منشورة ومتاحة عليها إلى الأبد ويمكنك التحقق من المعلومات المتاحة والمنشورة علنا عنك عن طريق البحث عنها من خلال محرك البحث.

» **الاحتيال وسرقة الهوية:**

كلما قدمت المزيد من المعلومات والصور والمشاركات عبر شبكة الإنترنت، بما في ذلك بياناتك الاجتماعية المنشورة على الملف التعريفي الخاص بك على شبكات التواصل الاجتماعي كلما كان من السهل على المحتالين والمجرمين استخدام تلك التفاصيل الخاصة بك لسرقة

أموالك أو سرقة هويتك، ولذلك يجب أن تقوم بالحد من المعلومات الشخصية التي تنشرها عبر شبكة الإنترنت وقبل أن تقوم بنشرها بالفعل.

» **جرائم الاحتيال عبر شبكات الإنترنت:**

ينجح المحتالون وطرق احتيالهم عبر شبكة الإنترنت لأنهم يقدمون أشياء وسلعا يريدها الأفراد والمستخدمون مثل الحصول على مبلغ ضخم من المال دون بذل أي جهد فيجب عند استخدامك لمواقع التواصل الاجتماعي ألا تستجيب لأي عروض أو طلبات غير متوقعة مقابل الحصول على معلومات شخصية أو مالية خاصة بك.

» **التحرش الإلكتروني:**

عندما تكون المعلومات الشخصية الخاصة بك المنشورة على شبكة الإنترنت متاحة للجمهور يمكن أن يستخدمها الأخرون للتحرش بك أو تهديدك فيجب أن تحافظ على سرية عنوانك وتكون حريصا جدا عند قيامك بنشر أسماء أو صور تظهر لوحات السيارات، وأسماء الشوارع والأماكن التي كثيرا ما تتردد عليها أو يسهل الربط بينها وبينك.

» **رعاية الأطفال على الإنترنت:**

مستخدمو الإنترنت هم المسؤولون عن كم المعلومات التي يصرحون بها وينشرونها على شبكة الإنترنت، ويمكن استخدامها لأغراض غير متوقعة. فيمكنك مساعدة أطفالك وحمايتهم حتى يظلوا في أمان على شبكة الإنترنت من خلال تذكيرهم بما يلي:

- ضرورة عدم التشارك في كلمات المرور، بغض النظر عن مقدار ثقتهم في أصدقائهم.
- ضرورة استخدام كلمات مرور قوية مكوّنه من مزيج من الحروف والأرقام
- عدم نشر تفاصيل شخصية عنهم وخاصة الصور.
- ضرورة حجب مرسلي الرسائل غير الملائمة أو المزعجة أو حذفهم من قائمة جهات الاتصال الخاصة بهم
- عدم إعطاء أرقام هواتفهم المحمولة لأشخاص لا يعرفونهم جيدا.

لمستخدمي المحمول والإنترنت 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

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

القرية الذكية مبنى B٤ - الكيلو ٢٨ طريق مصر/الاسكندرية الصحراوى
ت: ٠٠٠ ٣٥٣٤٤٠٠٠ ٢٠٢+ ف: ٣٥٣٤٤١٥٥ ٢٠٢+
الجهاز-القومي-لتنظيم-الإتصالات.مصر

www.youtube.com/user/CRPCNTRA
www.facebook.com/CRPC.NTRA
twitter.com/NTRAEGYOFFICIAL