ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

International Journal of Scientific
Research and Sustainable Development
"Information Technology"

أمن المعلومات الخاصة في مواقع الإنترنيت والتواصل الاجتماعي وطرق حمايتها

نهى بنت عبدالله بن عبده اسكندر[1]

معلمة بالثانوية الخامسة للبنات –جازان – حي الروضة الشرقي– المملكة العربية السعودية[1]

الإيميل: Ns0000r@hotmail.com

الملخص

المعلومات هي عملة الإنترنت، وتعتمد خصوصية أي شخص على الإنترنت على إمكانية التحكم في كل من مقدار المعلومات الشخصية التي قام بتوفيرها ومن يمكنه الوصول إلى هذه المعلومات.

فعند القيام بالأنشطة اليومية عبر الإنترنت، فربما يمكن الكشف عن المعلومات الشخصية التي يمكن استخدامها بواسطة الآخرين للتعدي على الخصوصية، ويمكن أن يشمل ذلك معلومات حساسة مثل عنوان IP أو عنوان البريد الإلكتروني ، والموقع الجغرافي الحالي ، أو عنوان المنزل أو العمل .

يهدف البحث إلى بيان أمن المعلومات ووسائل التواصل الاجتماعي ،ووسائل أمن المعلومات الشخصية بشكل عام ، وأمن المعلومات الشخصية على الانترنت ، و أمن المعلومات على وسائل التواصل الاجتماعي ، و أمن المعلومات على الايميلات . وذلك لحفظ وحماية خصوصية الإنسان ومعلوماته الشخصية ، ويستفيد منه لضمان معلوماته الشخصية وخاصة ممن لا يراعي الآداب والأخلاق العلمية والإنسانية .

الكلمات المفتاحية : أمن ، معلومات ، التواصل الاجتماعي ، الإنترنت ، الايميلات ، حماية .

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

مقدمة

منذ اختراع الإنترنت حدثت ثورة كبيرة في المعلومات المتناقلة بين الناس، وتنوّعت الشبكات التي تستخدمها وتعتمد عليها، فثورة الإنترنت ربطت مناطق العالم معاً وجعلت منها قريةً صغيرةً بعد أنْ كانت عملية التواصل فيما بين الناس الذين يقطنون المناطق المختلفة صعبة وبعضها مستحيلاً. فسابقاً قبل دخول الإنترنت كان إذا سافر أحد الأشخاص لبلدٍ ما للدراسة أو العمل، كان من الصَّعب على بقية أفراد عائلته الاطمئنان عليه إلّا من خلال الهاتف، ولا يمكن لهم رؤية صورته إلّا من خلال الصور التي كان يبعثها ورقياً مع الرسائل لهم، ولكن الآن من خلال الإنترنت أصبح بإمكان الجميع التواصل بالصوت والصورة من خلال مكالمات الفيديو التي تُشعِر الشخص أنّه لا يبعد سوى مسافاتٍ قليلة عن بقيّة العائلة، كما يمكنهم التواصل من خلال شبكات التواصل الاجتماعي للبقاء على اتصالٍ دائم ومعرفة جميع الأخبار أولاً بأول .

ونظراً لأهمية حفظ وحماية خصوصية الإنسان ومعلوماته الشخصية ، فقد قمت بجولة في شبكات التواصل لجمع هذا البحث المختصر النافع ؛ ليطلع عليه القارئ ويستفيد منه لضمان معلوماته الشخصية وخاصة ممن لا يراعي الآداب والأخلاق العلمية والإنسانية .

وقد قسمت مقالي إلى ما عدد من العناوين الفرعية بغية تغطية شاملة ومختصرة للموضوع، وهي يأتي:

المبحث الأول: التعريف بأمن المعلومات ووسائل التواصل الاجتماعي.

المبحث الثاني: وسائل أمن المعلومات الشخصية بشكل عام.

المبحث الثالث: أمن المعلومات الشخصية على الإنترنت.

المبحث الرابع: أمن المعلومات على وسائل التواصل الاجتماعي.

المبحث الخامس : أمن المعلومات على الإيميلات .

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

International Journal of Scientific
Research and Sustainable Development
"Information Technology"

المبحث الأول: التعريف بأمن المعلومات ووسائل التواصل الاجتماعي.

أمن المعلومات

أمن المعلومات: له تعاريف من نواح عدة:

فمن ناحية أكاديمية: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

ومن ناحية تقنية: هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

ومن ناحية قانونية: هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت).

إن استخدام اصطلاح أمن المعلومات Information Security وان كان استخداماً قديماً سابقاً لولادة وسائل تكنولوجيا المعلومات، إلا إنه وجد استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال؛ إذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات– وتحديداً الإنترنت – احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة؛ بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.

شبكات التواصل الاجتماعي

وهو مصطلح أطلِق على الخدمة الإلكترونيّة التي تقدِّمها شبكة الإنترنت للأفراد والجماعات،

حيث تتيح لهم التواصل فيما بينهم حسب اهتماماتهم، فيستطيع أي شخص أن يجد أو ينشئ المجموعات حسب اهتمامٍ معين مثل القراءة أو بلد المنشأ أو الهوايات أو التخصص الجامعي وغيرها من الأمور المشتركة، شكّلت هذه المواقع حلقة وصلٍ بين جميع الأشخاص على اختلاف مواقعهم واختلاف دياناتهم وأعمارهم وأجناسهم، حيث أصبح أي فرد يستطيع الوصول إلى أي شخص في العالم من خلال هذه المواقع، وتعتمد مواقع التواصل الاجتماعي بشكلٍ أساسي على الأفراد أو المستخدمين؛ لأنهم هم من يشغِّلونها ويرفدونها بالمعلومات والبيانات.

التّواصل الاجتماعيّ

يحتاج النّاس إلى التّواصل فيما بينهم لمعرفة أخبار بعضهم البعض والاطمئنان فيما بينهم، فالإسلام أوصانا بصلة الرّحم والتّواصل لما لهذا من أهميَّة لزيادة التَّرابط بين أبناء المجتمع الإسلامي الواحد، وتحقيق التكافل بين الأفراد، وتعزيز الشعور ببعضهم البعض. في الزمان القديم كانت مظاهر صلة الرحم هي الزّيارات والتّواصل المباشر، ومع أهميّة هذه الطَّريقة في التواصل إلا أنها تكون مريحةً للأشخاص القريبين من بعضهم، بينما الأشخاص الذين يقطنون في المواقع البعيدة فإنها تصعب عليهم ولربما تمرُّ الشّهور والسَّنوات دون حدوث تواصل فيما بين الناس بسبب تباعد الأماكن .

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

المبحث الثاني: وسائل أمن المعلومات الشخصية بشكل عام .

هناك وسائل تقنية لأمن المعلومات ووسائل تنظيمية، وفيما يأتي بيانها :

الوسائل التقنية لأمن المعلومات

يُمكن حماية المعلومات والحفاظ عليها من خلال الوسائل التقنية الآتية:

1 . عمل نسخة احتياطية عادية، وحفظ أهمِّ ملفات البيانات من خلال تقنية التخزين عن بعد.

2. عمل نسختين احتياطيتين لجميع النظم الفرعية للشبكة المتعلقة بأمن البيانات.

3. إمكانية استدعاء مصادر الشبكة عند حدوث خلل بسبب المستخدمين .

4. تشغيل أنظمة تزويد الطاقة الكهربائية الاحتياطية عند حدوث خلل ما .

5 . التأكد من حماية المعلومات من التلف في حال حدوث حريق أو وصول ماء إليها .

6 . تثبيت البرامج التي تمنع الوصول إلى قواعد البيانات، أو أي معلومات لمن ليس لديهم الحق في ذلك .

الوسائل التنظيمية لأمن المعلومات

تستطيع الطرق البرمجية حماية المعلومات بالشكل الآتي:

طلب الكمبيوتر كلمة مرور عند إعادة التشغيل، وعليه يجب معرفة كيفية اختيار كلمة مرور قوية، والمحافظة عليها بالاستعانة بأدلة الأمان الأساسية الموجودة في أنظمة التشغيل Windowsو .Linuxتشفير عملية تخزين البيانات والمعلومات على أجهزة الكمبيوتر، والأجهزة

اللوحية، والأجهزة الذكية.

. تشغيل قفل الشاشة في حال ترك الكمبيوتر، وذلك متاح في أنظمةWindows ، وLinux، وMac، فهي تحتوي على اختصارات تُمكِّن إجراء ذلك بسرعة وسهولة.

.استخدام خصائص BIOS الخاصة بنظام الحماية والموجودة في إعدادات الكمبيوتر، بحيث تمنع أولاً الدخول إلى نظام التشغيل من جهاز USB أو CD-ROM أوDVD ، ثم يتم تحديد كلمة مرور قوية على BIOS نفسه بحيث لا يتمكن المتطفل من تغيير طريقة الدخول .

تفعيل خاصية "العثور على جهازي" إذا كان الهاتف الذكيsmart phone ، أو الحاسوب اللوحيtablet computer ، أو الحاسوب المحمول Laptop يحتوي عليها، حيث تساعد في تحديد موقع الجهاز أو مسح محتوياته عن بُعد في حال فُقدانه أو سرقته .

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

المبحث الثالث: أمن المعلومات الشخصية على الانترنت .

المعلومات هي عملة الإنترنت، وتعتمد خصوصية أي شخص على الإنترنت على إمكانية التحكم في كل من مقدار المعلومات الشخصية التي قام بتوفيرها ومن يمكنه الوصول إلى هذه المعلومات.

فعند القيام بالأنشطة اليومية عبر الإنترنت، فربما يمكن الكشف عن المعلومات الشخصية التي يمكن استخدامها بواسطة الآخرين للتعدي على الخصوصية، ويمكن أن يشمل ذلك معلومات حساسة مثل عنوان IP أو عنوان البريد الإلكتروني ، والموقع الجغرافي الحالي ، أو عنوان المنزل أو العمل .

كيف يمكن الوصول إلى المعلومات الشخصية على الإنترنت؟

تجمع الشركات والحكومات والمؤسسات الأخرى البيانات عندما الشخص بـ:

- إعداد حساب عبر الإنترنت.
- إجراء عملية شراء في متجر عبر الإنترنت.
- التسجيل في مسابقة.
- التقاط جزء في أحد الاستطلاعات.
- تنزيل البرامج مجانًا.
- تصفح الويب.

- استخدام التطبيقات على جهاز الكمبيوتر الخاص أو المحمول.
- نشر الصور أو الحالة الخاصة بالشخص على وسائل التواصل الاجتماعي.

كيف تنقل معلوماتي الشخصية ؟

تستخدم Microsoft وغيرها من الشركات المسؤولة معلوماتك الشخصية للمساعدة في تحسين تجربتك باستخدام منتجاتها وخدماتها – مثل من خلال مساعدتك في إكمال إحدى العمليات، أو تذكر تفضيلاتك، أو تقديم محتوى مخصص والعروض الخاصة.

ترتبط المعاملات عبر الإنترنت – مثل تسجيل الاشتراك في خدمة ما أو شراء شيء ما – بك بمعلومات مثل عنوان شحن أو رقم بطاقة ائتمان، ولكن في معظم الحالات، تقوم الشركات بشكل عام بجمع البيانات التي لا تتعرف عليك بالاسم، تتعقب مواقع الويب صفحات الويب التي تقوم بزيارتها ونقرات الماوس، ولكن ليس أنت شخصيًا.

يمكن أن تكون البيانات الشخصية أيضًا عبر الإنترنت لأنه ربما تكون قد أضفت معلوماتك الخاصة في سير ذاتية أو مخططات أو صفحات على شبكات التواصل الاجتماعي مثل Facebook، أو التعليقات في مجموعات المناقشات أو علىTwitter

قد يقوم الآخرون بنشر معلومات عنك، قد يقوم الأصدقاء بالكتابة عنك أو نشر صور لك ولعائلتك، ويمكن أن تكون سجلات الجهات الحكومية قابلة للبحث – على سبيل المثال، صور منزلك وقيمته، وشهادة الميلاد، ونسخ من توقيعك، وقد تكشف مجموعات النوادي والروابط الاحترافية عن اسمك بالكامل أو مكان عملك أو تاريخ تبرعك.

فالمعلومات المتوفرة حولك عبر الإنترنت لسببين:

- قد تستخدم الشركات والقائمين على التوظيف هذه المعلومات، والتي تشكل سمعتك عبر

الإنترنت، لقياس ملاءمتك لإحدى الوظائف.

- يستخدم المجرمون بياناتك عبر الإنترنت لاستهدافك بالرسائل الخادعة للتصيد الاحتيالي، وسرقة هويتك، وارتكاب جرائم أخرى.

ومع ذلك، فبخلاف البيانات المخزنة على الورق، يمكن أن تجعل محركات البحث القوية عبر الإنترنت وأدوات تجميع البيانات قوية من السهل سحب البيانات معًا لإنشاء ملف تعريف كامل لك.

بمجرد نشر البيانات عبر الإنترنت، تتوافر هناك للأبد، ووفقًا لنهج خصوصية الشركة التي تمتلك البيانات، يمكن رؤيتها في النهاية على الإنترنت، فقد تقوم المواقع بأرشفة أي شيء قمت بنشره بالإضافة إلى البيانات التي قامت بجمعها منك، ربما يقوم الأصدقاء (أو الأصدقاء السابقون) بالإفصاح عن معلوماتك أو قد يعرضها متطفلوا الأمان.

عليك مراقبة الآخرين لحماية معلوماتك الشخصية:

وذلك من خلال القيام بالآتي:

- ابحث عن اسمك على الإنترنت باستخدام محركات البحث الشائعة، ابحث عن الرسائل النصية والصور، إذا وجدت معلومات حساسة عن نفسك على موقع ويب، فابحث عن معلومات جهة الاتصال على موقع الويب وأرسل طلبًا لإزالة معلوماتك.

- بشكل منتظم، راجع ما يكتبه الآخرون عنك على المدونات ومواقع ويب شبكات التواصل الاجتماعي، اطلب من الأصدقاء عدم نشر صورك أو صور عائلتك دون الحصول على إذن منك، إذا كنت تشعر بعدم الراحة لمواد مثل المعلومات أو الصور التي يتم نشرها على مواقع الويب الخاصة بالآخرين، فاطلب إزالتها.

- على Facebook ووسائل التواصل الاجتماعي الأخرى، قم بتشغيل خيار مراجعة العلامة لمنع الأشخاص من وضع علامات الصور التي تظهر دون الحصول على إذن منك.

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

قد تؤدي مشاركة بياناتك إلى تحقيق فوائد، وغالبًا ما يكون من الضروري مشاركتها للتفاعل مع الأشخاص الآخرين في مجتمع اليوم، لكن هذا لا يخلو من المخاطر، فبياناتك الشخصية يمكن أن تكشف الكثير عنك وعن أفكارك وحياتك، حيث إنه من السهل استغلال هذه البيانات بسهولة لإيذائك، وهذا ما يشكل خطر على الأفراد والمجتمعات المستهدفين، مثل الصحفيين والناشطين والمدافعين عن حقوق الإنسان وأعضاء الجماعات المضطهدة والمهمشة.

لذلك من الضروري أن تكون هذه البيانات محمية بشكل صارم.

في الاتحاد الأوروبي، تعتبر حماية البيانات الشخصية حقًا أساسيًا، لذلك تم تفعيل اللائحة العامة لحماية البيانات (GDPR) كإطار جديد لحماية هذا الحق، تمكّن هذه اللائحة الأوروبيين من استعادة السيطرة على معلوماتهم الشخصية داخل وخارج نطاق الإنترنت، وعلى الرغم من أن اللائحة العامة تشمل المستخدمين في دول الاتحاد الأوروبي، إلاّ أن أثرها يمتد إلى العديد من الدول خارج الاتحاد الأوروبي، خاصة تلك التي تستخدم خدمات الإعلان على الإنترنت والتي قد تتعامل أيضاً مع حرفاء في داخل الاتحاد الأوروبي، إذ أنّ دول الشرق الأوسط وشمال إفريقيا على سبيل المثال ستتأثر بأحكام وقوانين اللائحة وبالتالي ستكون ملزمة في الخضوع للأحكام الواردة فيها والمتعلقة بحماية المعطيات الشخصية.

معنى أمن وحماية البيانات الشخصية

البيانات الشخصية هي أي معلومات تتعلق بك، سواء كانت متعلقة بالحياة الخاصة أو المهنية أو العامة في بيئة الإنترنت، حيث يتم تبادل ونقل كميات هائلة من البيانات الشخصية في جميع أنحاء العالم، يصبح من الصعب على الناس السيطرة على معلوماتهم الشخصية؛ لذلك أصبح من الضروري الحرص على حماية بياناتنا الشخصية.

يشمل تفعيل حماية البيانات الشخصية مجموعة من الممارسات والضمانات والقواعد الملزمة قصد ضمان التحكم في هذه البيانات. وباختصار يجب أن تكون قادرًا على تقرير ما إذا كنت ترغب في مشاركة بعض المعلومات، ومن لديه حق الوصول إليها، وطول مدة خزنها في قاعدة بيانات، ولأي سبب، كما أنه من الضروري أن تكون قادرًا على تعديل هذه البيانات متى شئت.

الحاجة إلى قوانين حماية البيانات الشخصية:

هناك سببان رئيسيان يجب على الحكومات اتباعها في إطار تشريع قوانين لحماية البيانات الشخصية:

يجب تحديث القوانين الحالية لمعالجة واقع اليوم فمع تطور استعمال الإنترنت واستفحالها في مختلف المجتمعات، ازدادت الحاجة إلى حماية البيانات التي يتم مشاركتها كل يوم ليس فقط على مواقع التواصل الاجتماعي، وإنما في جميع مواقع الويب، ورغم وجود قواعد أو قوانين تهتم بالخصوصية لكنها غير قابلة للتكيف بما يتناسب مع تحديات عالم اليوم.

وقد سبق أن دافعت الشركات والكيانات الكبرى التي تجمع بيانات الأشخاص منذ فترة طويلة عن تنظيم الخصوصية وحماية البيانات ليس من خلال الأطر الملزمة، بل من خلال آليات التنظيم الذاتي أو المشاركة التي توفر مرونة أكبر، ومع ذلك، فعلى الرغم من المحاولات العديدة، لا يزال يتعين علينا أن نرى أمثلة على أنظمة غير ملزمة تكون إيجابية بالنسبة لحقوق المستخدمين (أو في الواقع، بالنسبة للأعمال ككل).

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

المبحث الرابع: أمن المعلومات على وسائل التواصل الاجتماعي:

تتعرض وسائل التواصل الاجتماعي لعمليات القرصنة بشكل دائم، ولأن موقع الفيسبوك صار يعرض أفلامًا، برامجًا تليفزيونية وأحداثًا رياضية والتي يستوجب الدفع قبل مشاهدة بعضها أو تكون من خلال الاشتراك، فيوجد حوالي 31 مليون فقط حول العالم يطبقون ذلك بشكل قانوني، إلا أن عشرات الملايين من الأفراد يشاهدون المباريات بطرق غير مشروعة، فقد لا يكلفون الشبكات فحسب، ولكن رُعاة المشروع ذاته.

الفيسبوك مثله مثل الشبكات الأخرى، التي تراقب بجدية عمليات القرصنة، ولكنه لا يتحمل المسؤولية القانونية لتدفق الصفحات غير المشروعة، وبدلاً من ذلك، فأنه يعتمد على الأشخاص الذين يبلغون إدارة الموقع الاجتماعي بذلك، فأصبح من السهل نسبيًا على الموقع أن يكتشف مواقع القرصنة.

بالإضافة إلى ذلك تقدم أعضاء في البرلمان الأوروبي في ديسمبر عام 2015م، بمشروع قانون يلزم الشركات بالتبليغ عن الاختراقات وعمليات القرصنة، ما يعد الخطوة الأولى من نوعها على صعيد تعميم قوانين مكافحة القرصنة في الاتحاد.

ويشير القانون إلى الأهمية القصوى التي توليها الدول الغربية في مكافحة القرصنة والجرائم المعلوماتية، وتعد سرقة بيانات الشركات وسرقة الحسابات الشخصية لعملاء البنوك أحد أبرز عمليات القرصنة.

ورغم أن الناس لديهم تفاعلات ملحوظة داخل المجموعات الخاصة على موقع التواصل، ولكن إذا كان موقع التواصل يتحمل مسؤولية المحتوى المُقرصن أو لا يتحمله، فما عليك سوى تجنبه، سواء كان هذا المحتوى منشور على وسيلة تواصل اجتماعية ليس فقط فيسبوك فحسب، ولكن أيضًا على "واتساب"، أو "تليجيرم"، لأنه سيُسبب مشكلة كبيرة إذا اتبعت هذا المحتوى وما فيه من روابط.

ومن الخطوات لحماية البيانات الشخصية:

***استخدم أحد تطبيقات المراقبة:** لو كنت من الناس الذين يتفقدون حساباتهم على مواقع التواصل الاجتماعي من خلال هاتفك الذكي، فعليك أن تحرص على استخدام أحد تطبيقات البرامج الرقابية. فعلى سبيل المثال نجد بأن تطبيق"Social Media Vault" يعد من أفضل التطبيقات لهذا الغرض. فبالإضافة لتوفيره حماية عالية المستوى لكلمات المرور التي تختارها فإنه يملك ميزة إعلامك بمحاولة أحدهم اختراق حسابك. فضلاً عن هذا، فإن التطبيق يمكن أن يُستخدم كمنظم لكلمات المرور؛ حيث إنه وبمجرد أن تخزن عليه كلمات المرور التي تستخدمها يقوم هو بكتابتها بدلاً من أن تكتبها في كل مرة تريد أن تدخل حسابك الشخصي على أحد مواقع التواصل الاجتماعي.

***افصل بين حسابك الشخصي وحسابك الخاص بعملك :** غالباً ما تكون هناك معلومات حساسة متعلقة بالعمل الذي تشغله، وبالتالي فإنه يُفضل إنشاء حسابين منفصلين أحدهما للاستخدام الشخصي والآخر للعمل حتى تتمكن من إدارتهما بسهولة أكثر وبطريقة أكثر أمنًا. فضلاً عن هذا، فإنه يُفضل أن تتم متابعة حساباتك على مواقع التواصل الاجتماعي الخاصة بالعمل من قبل فريق تكنولوجيا المعلومات الخاص بالشركة التي تعمل بها لإعلامك في حال تعرضت حساباتك لأي محاولة اختراق.

* **لا تستخدم شبكة إنترنت لاسلكية مفتوحة :** لأنه يسهل على القراصنة سرقة طريقة اتصالك بالإنترنت ومن ثم تحميل الملفات من جهازك .

* **قم بتغيير كلمة المرور بين فترة وأخرى** ، وإن كان البقاء عليها يؤدي إلى حفظها ؛ لكن

ISSN 2537_ 0715
IJSRSD (2020): Volume 3, Issue 1, August 2020
Received: June 2020, Accepted: July 2020

للحذر من المخاطر التي يتعرض لها ، وينبغي أن تكون معقدة ، وهذا ما يوصي به الخبراء.

* **عليك الاستعداد لربما تتعرض لفتح روابط أمامك** ، فستجد رابطاً ينقلك إلى غيره ، فمن الطرق الشائعة المُتبعة على وسائل التواصل الآن؛ هو عرض الرابط لك لمدة دقائق بعد عرض ما فيها من محتوى ومن ثم تأخذك لروابط أخرى، وهذا من شأنه أن يجعلك تعرف المصدر نفسه من الروابط التي تتابعت في فتحها، ولكن إذا توقف الرابط الأول عن العمل فقط، يمكنك الرجوع إليه مرة أخرى وتحميله من جديد.

المبحث الخامس: أمن المعلومات على الإيميلات .

لحماية وأمن الإيميل من الاختراق يجب ما يأتي :

- **تفعيل نظام المصادقة الثنائية** : يُعد تفعيل نظام المُصادقة الثنائية (بالإنجليزية– Two Factor Authentication) و يُشار إليه بالاختصار (FA 2) أحد الأمور التي يجب تفعيلها عبر البريد الإلكتروني (Email) الخاص بالمُستخدِم لتجنُب تعرضه للاختراق، حيث إن تفعيل هذه الخاصية تجعل المُستخدِم مُطالَباً بتزويد أكثر من وسيلة تحقُق للدخول إلى حسابه؛ حيث يتوجب إدخال كلمة المرور، بالإضافة إلى وسيلة أمان ثانية تتمثل بإرسال رسالة نصية تحتوي على رمز للدخول يتم إرساله إلى رقم هاتف المُستخدِم، ويُوفر معظم مزودي خدمات البريد الإلكتروني هذه الخاصية عبر الحسابات الخاصة بهم.
- **تجنب استخدام الأجهزة والشبكات العامة:** يتوجب على المُستخدِم تجنُب تسجيل الدخول إلى حساب بريده الإلكتروني من أجهزة الحاسوب التي يتم استخدامها من قِبَل أكثر من شخص قدر الإمكان، كأجهزة الحاسوب الموجودة في المقاهي، أو الفنادق، أو غيرها من الأماكن العامة، إذ قد تحتوي مثل تلك الأجهزة على برامج خاصة بالتجسُس تؤدي إلى اختراق حساب البريد الإلكتروني الخاص بالمُستخدِم، كما يجب الحرص على تجنُب استخدام شبكات الواي فاي (Wi–Fi) العامة للوصول إلى خدمات الإنترنت

المُختلفة، وخاصة تلك التي تتطلب الوصول إلى حسابات شخصية كالبريد الإلكتروني.

- **تحديث البرامج الموجودة على الجهاز:** يُعد تحديث البرامج الموجودة على الجهاز الخاص بالمُستخدِم أمراً مهماً جداً للحفاظ على حسابه آمناً من التعرُض للاختراق، ويجب على المُستخدِم تحديث متصفح الإنترنت الذي يستخدمه للوصول إلى حساب بريده الإلكتروني، كما عليه تحديث نظام التشغيل الذي يعمل به الجهاز سواء أكان جهاز حاسوب أم هاتفاً محمولاً، فضلاً عن تحديث أيّة تطبيقات أخرى قد تكون قديمة، فتحديث برامج وأنظمة التشغيل الموجودة على الأجهزة تضمن للمُستخدِم الحصول على التحسينات الأمنية التي يوفرها التحديث، بالإضافة إلى تجنُب الأخطاء أو الثغرات التي قد توجد بها حالياً.
- **استخدام برامج الشبكة الخاصة الافتراضية:** يُوصى باستخدام ما يُعرَف ببرامج الشبكة الخاصة الافتراضية (Virtual Private Network) ويُشار إليها بالاختصار (VPN) ، إذ إنها ونقرة واحدة تحمي هذه البرامج التي يتم تفعيلها على أجهزة الحاسوب أو الهواتف المحمولة هوية المُستخدِم عند اتصاله بشبكة الإنترنت، وذلك من خلال تشفير جميع بياناته التي تمر عبر الشبكة، وهذا الأمر من شأنه أن يُبقي المُستخدِم آمناً ومُعرضاً لعدد أقل من الإعلانات التي تظهر أثناء استخدام الإنترنت.
- **استخدام كلمة مرور آمنة :** يتوجب استخدام كلمة مرور قوية، بحيث يكون من الصعب على الآخرين التنبؤ بها وبنفس الوقت من السهل على المُستخدِم نفسه تذكُرها، لذا يجب تجنُب استخدام كلمات شائعة لوضعها ككلمة مرور خاصة بحماية حساب البريد الإلكتروني كاسم المُستخدِم نفسه، أو اسم عائلته، وغيرها من الأسماء التي يسهل على المخترق الحصول عليها، ويُنصح باستخدام كلمات مرور مُركبة تحتوي على مجموعة من الأرقام، والأحرف الكبيرة، والصغيرة، وبعض الرموز الخاصة، بالإضافة إلى استخدام كلمة مرور جديدة لم يتم استخدامها مُسبقاً من قِبل المُستخدِم على أيّ من حساباته الأخرى على شبكة الإنترنت، ومن الأمور الأخرى المهمة التي تمنع تعرُض حساب البريد الإلكتروني للاختراق قيامه بعملية تسجيل الخروج من الحساب عند الانتهاء من استخدامه، كما يتوجب على مُستخدِم البريد الإلكتروني الحفاظ على سرية

كلمة السر الخاصة بحسابه بحيث يتجنب مُشاركتها مع أي شخص آخر.

- **تغيير أسئلة الأمان الخاصة بالحساب:** تُعد أسئلة الأمان (بالإنجليزية Security Questions) من الأمور التي قد يلجأ إليها المُخترقون للوصول إلى حساب بريد إلكتروني مُعين، وذلك من خلال الإجابة عن تلك الأسئلة بدلاً من إدخال كلمة مرور الحساب، وتشير الأبحاث المُتخصصة إلى أنّ ما يُقارب 20% من المُستخدِمين يقومون بالإجابة عن أسئلة الأمان بالإجابة نفسها، لذا يُنصح بوضع أجوبة على أسئلة الأمان بحيث يكون من الصعب تخمينها وتوقعها بشكل سهل.
- **استخدام برامج مكافحة الفيروسات:** يُمكن المُساعدة على حماية حساب البريد الإلكتروني ومنعه من التعرُض للاختراق من خلال استخدام برامج خاصة بمكافحة الفيروسات التي تحافظ على بيانات المُستخدِم آمنة وخالية من البرامج الضارة وبرامج التجُسس المُختلفة وبشتى أشكالها مثل برامج الفدية، لذا لا بد من تثبيت مثل هذه البرامج على الأجهزة التي يستخدمها الشخص للدخول إلى حساب بريده الإلكتروني سواءً أكانت أجهزة حاسوب أم هواتف محمولة.
- **تجنب فتح الرسائل المجهولة:** يُمكن اختراق حساب البريد الإلكتروني من خلال رسائل وهمية يُرسلها المُخترِق لحساب المُستخدِم، بحيث تحتوي تلك الرسائل على روابط أو ملفات مُضمنة بداخلها تسمح للمُخترق سرقة بيانات المُستخدِم بمجرد فتحها أو النقر عليها، لذا يتوجب تجنُب فتح أيّة رسائل مشبوهة وهذه هي الطريقة الأسهل لتلافي خطر هذا النوع من الاختراقات، ويُمكن الاستعاضة عن ذلك بفتح علامة تبويب جديدة في متصفح الإنترنت، ثم التأكد من معلومات الجهة المُرسِلة عبر الإنترنت، وقد يكون من السهل على المُستخدِم توقع الرسائل المشبوهة من خلال العديد من الأمور؛ إذ قد تكون مُرسلة من شخص غير معروف بالنسبة للمُستخدِم، أو أنّها مُرسَلة من شخص معروف وتحتوي على رابط أو ملف مُرفق دون وجود نص كتابي في الرسالة نفسها.
- **استخدام خدمة بريد إلكتروني آمنة :** يُمكن زيادة أمان حساب البريد الإلكتروني وتقليل احتمال تعرُضه للاختراق من خلال استخدام خدمة بريد إلكتروني آمنة تعتمد على استخدام ما يُعرَف بطبقات المنافذ الآمنة (بالإنجليزية Secure Socket :

(Layers والتي يُشار إليها بالاختصار (SSL) ، وتعني استخدام الموقع المُزوِّد لخدمة البريد الإلكتروني بروتوكول (HTTPS) بدلاً من بروتوكول(HTTP) ، ويُعنى هذا البروتوكول بتشفير اتصال المُستخدِم بالخادم الرئيسي للشركة المُزوِّدة لخدمة البريد الإلكتروني، ولا يعني أبداً تشفير نص الرسالة التي يتمّ إرسالها عبر البريد الإلكتروني، ويُمكن تشفير نص هذه الرسائل وجعلها غير قابلة للقراءة إلّا من قِبل المُستلم لها من خلال استخدام ما يُعرَف بشهادات الأمان على أجهزة كل من المُرسِل والمُستقبِل للرسالة.

- **تخصيص استخدام حسابات البريد الإلكتروني لأغراض مُختلفة**، حيث يُنصح بتخصيص حساب خاص بالعمل، وآخر خاص بالأمور الشخصية، وآخر للبيع والشراء عبر الإنترنت، حيث يحافظ هذا الأمر على بعض الحسابات في حال تم اختراق أحدها، وعدم فقدانها جميعاً.
- **حماية شبكة الواي فاي** من خلال وضع كلمة مرور عليها وتغييرها بشكل مُستمر.
- **استخدام عنوان بريد إلكتروني (Email Address) مُعقد**؛ بحيث لا يُمكن توقعه بسهولة من قِبَل أشخاص آخرين.
- **حذف البرامج والتطبيقات وإضافات مُتصفح الإنترنت** (بالإنجليزية Browser : Extension)التي ليس لها حاجة، وتثبيت البرامج والتطبيقات الأساسية في حال أمكن ذلك.
- **عدم إرسال معلومات الهوية الشخصية عبر البريد الإلكتروني.**
- **عدم الرد على بريد إلكتروني يطلب كلمة المرور الخاصة بك:** لن تطلب منك شركة Microsoft مطلقاً كلمة المرور الخاصة بك في البريد الإلكتروني، لذلك لا ترد أبداً على أي بريد إلكتروني يطلب الحصول على أي معلومات شخصية، حتى إذا كان يدعي أنه من Outlook.comأو من Microsoft.

المصادر والمراجع :

1. سرحان سليمان السرحان محمود المشهداني ،أمن الحاسوب والمعلومات ، دار وائل ، 2001 م.

2. فاروق سيد حسين ، التجارة الإلكترونية وتأمينها ، هلا للنشر والتوزيع ، 2001 م.

المواقع الإلكترونية :

3. http://www.ericson/org.

4. http://www.itu.int/.

5. http://www.ac.com/ecommerce/mcommerce_trends.html.

6. http://www.ericson/org.

./http://www.itu.int .7

.http://www.ac.com/ecommerce/mcommerce_trends.html .8

./http://www.nttdocomo.com .9

./http://www.wapforum.org .10

.http://www.sei.cmu.11