ورقة بحثية بعنوان

إختراق البريد الالكتروني EMAIL HACKING

إعداد الدكتور

كمال الدين يوسف يسن

2012

Km77_it@yahoo.com

المقدمة

يعتبر البريد الالكتروني من أهم إنجازات الثورة المعلوماتية التي تتيح للأشخاص والمؤسسات والشركات و كافة القطاعات تبادل الرسائل فيما بينها،مما انعكس ايجابا على العمل وذلك نسبة للسرعة الفائقة التي يتميز بها وقلة التكلفة الاقتصادية وإمكانية الارسال المتعدد وإعادة الانتاج الى عدد كبير من الجهات وبنفس الكفاءة وفي ذات الوقت.

لذلك يعتبر البريد الالكتروني ولما يشكلة من قيمة وإعتمادية عالية في قطاع الأعمال ظل هدفاً لقراصنة المعلومات والشبكات ومحوراً مهماً تستهدف المؤسسات من خلاله وفي حالة إختراقه تكون المعاملات قد تعرضت لخرق خطير في أمن المعلومات.

لذلك كله تناقش هذه الورقة العلمية اختراق البريد الالكتروني في ثلاثة مباحث حيث يتناول المبحث الأول خصائص البريد الالكتروني وخصوصية المعلومات والاتصالات ، يحتوي المبحث الثاني على تجريم اختراق البريد الالكتروني دينياً وقانونياً ، يناقش المبحث الثالث والأخير أهم الطرق التقنية لحماية البريد الالكتروني من خطر الإختراق.

المبحث الأول

خصائص البريد الالكتروني وخصوصية المعلومات والاتصالات

1-1 مميزات البريد الإلكتروني :

يمتاز البريد الإلكتروني عن غيره بمجموعة من المميزات منها:

1.السرعة المتناهية في إرسال واستلام الرسائل ، حيث لا تستغرق إرسال الرسالة بضع ثوانٍ فقط لكي تصل إلى المرسل إليه وفي حال عدم وصول الرسالة فإن البرنامج يحيط المرسل علما بذلك.

2.المرونة العالية في إرسال مرفقات باستخدام ا مرفقات(Attachment)

3.التكلفة المالية القليلة جداً، مقارنة بالفوائد التي يجنيها المرسل والمستلم للرسائل.

4.المرونة العالية والكفاءة الجيدة في إرسال نفس الرسالة ومرفقتها إلى عشرات الأشخاص.

5. نستطيع أن نرسل رسالة مفردة إلى جميع الزملاء في العمل بنفس اللحظة.

6.يستطيع البريد المستقبل إعادة إرسال نفس الرسالة وبنفس الدقة.

7.يسمح بتخزين الرسائل بغرض التوثيق وأيضاً يستطيع المستخدم عمل تصنيفات للرسائل المخزنة.

8.تسمح بالاتصال مع البرامج التطبيقية ويمكن إرسال أي ملف واستقباله بسرعة عالية.

يتميز بالسهولة في الاستخدام.

9.يمكن تخزين صور هامة مثل الجواز والبطاقة الشخصية وكرت العائلة وغيره ثم القيام بسحبة في حالة السفر وفقدان احدها لا سمح الله.

10.بعض برامج البريد الإلكتروني لها خاصية البريد (Expressaliall)

11.يمكن ربط بعض الهواتف الذكية بالبريد بحيث يتم سحب الأرقام والصور والرسائل (حسب الرغبة) إلى البريد الالكتروني وتصفحها بسهولة.

12.لا يوجد وسيط لتسليم البريد الالكتروني لك فهو مباشرة بين المرسل والمستقبل.

تستطيع تحويل الرسالة من بريد إلى آخر تلقائيا.

13.إرسال رسالة تتضمن نصا صوتيا أو فيديو والصور والخرائط أو مايعرف برسائل الوسائط المتعددة.

14.يمكن للمستخدم أن يستخرج الرسائل من صندوق البريد عن طريق برنامج البريد الذي يمكن المستخدم من مشاهدة الرسائل وبناء على رغبته إذا شاء أن يرسل جوابا لأي منها وعندما يبدأ طلب بريد الإلكتروني يتم إخبار المستعمل بوجود رسائل بالانتظار في صندوق البريد عن طريق عرض سطر واحد لكل رسالة بالبريد الإلكتروني قد وصلت السطر يعطي اسم المرسل ووقت وصول الرسالة وطول الرسالة في القائمة.

15.يمكن للمستخدم أن يختار رسالة من الموجز ونظام البريد الإلكتروني يعرض محتوياتها وبعد مشاهدة الرسالة على المستخدم أن يختار العملية التي يرغب فيها فإما أن يرد على المرسل أو يترك الرسالة في صندوق البريد لمشاهدتها ثانية عند الحاجة أو يحتفظ بنسخة عن الرسالة في ملف أو التخلص من الرسالة بإلغائها.

1- 2كيفية عمل البريد الالكتروني:

عندما تريد إرسال رسالة فإنها تحتاج إلى برنامج عميل البريد مثل Microsoft outlook أو استخدام مواقع مضيفة للبريد الالكتروني ،تضع عنوان المستقبل وبعد أن تضغط زر الارسال يقوم برنامج العميل بتنسيق الرسالة على هيكل بريد إلكتروني ويكون على صيغة معينة وبعدها يقوم البرنامج بإرسال الرسالة بواسطة بروتوكول (smtp)أو برتوكول الانترنت بالنسبة لمستخدمي الشبكة العنكبوتية إلى عميل الإرسال (MTA) transfer agent mail وهو مثلاً km77_it@yahoo.com

1. وهو يبحث عن العنوان km77_it@yahoo.com فيقوم بمراسلة خادم yahoo.com
2. يقوم الخادم yahoo.com بإرسال عنوان موزع البريد (exchange mail) ويكون غالبا mx.yahoo.com إلى خادم yahoo.com

3. يقوم yahoo.com بإرسال الرسالة إلى mx.yahoo.com بواسطة بروتوكول SMTP

4. يقوم mx.yahoo.com بوضع الرسالة في صندوق Pop
5. يقوم بوب بجلب الرسالة بواسطة النظام(POP3 (Protocol Post Office من صندوق بريده.

3-1 خصوصية المعلومات والاتصالات

تعرف الخصوصية بأنها حق الأفراد بالحفظ على مكنوناتهم وأسراهم من ان تنتهك أو تنشر بدون علمهم وهنالك انواع متعددة للخصوية أذكر منها:-

1. خصوصية المعلومات: وهي الخصوصية المتعلقة بالمعلومات التي تطلب من الأشخاص حالة طلبهم للخدمات مثل الحصول على حساب في البنك أو التقديم لوظيفة معينة وفي حالةاستخدام هذه المعلومات خارج نطاقها نكون قد انتهكنا خصوصية هؤلاء الأشخاص مما يلحق الضرر بهم.
2. خصوصية لاتصالات: وهي عملية التجسس على المكالمات الهاتفية التي تجري بين الأشخاص.
3. الخصوصية الجسدية: وهي حماية الأشخاص من التعرض للفحوصات الطبية والجسدية مثل فحص مرض نقص المتاعة المكتسبة أو الفحص ضد المخدرات.
4. الخصوصية الجغرافية: وهي تتعلق بالعلاقات الدولية وعلاقات المجتمعات فيما بينها ومراعة أداب وسلوك الدخول للدول وللملكيات الخاصة للأفراد والمجتمعات.

ومن النقاط أعلاه يعتبر الهجوم او اختراق البريد الالكتروني تعدي واضح على المعلومات والاتصالات التي تنشأ بين الأطراف المختلفة سواء كان ذلك في شبكة خاصة بالشركات أو بشبكة المعلومات الدولية ينتج عنه أضراراً بمصالح الأفراد والمجتمعات والهيئات ومختلف الجهات.

المبحث الثاني

تجريم اختراق البريد الالكتروني دينيًا وقانونيًا

2-1الرؤية الاسلامية لإختراق البريد الالكتروني

حرَّمت الشريعة الإسلامية المطهرة العدوان على خصوصيات الآخرين ، وجاء الوعيد الشديد للمتعدي على حرمات المسلمين ، ومن ذلك تحريم التجسس ، وتحريم النظر من عقب الدار ، وتحريم سماع مكالمات أو حديث الناس دون إذنهم ، وقد سبق الإسلام بهذا دعاوى كثيرين ممن يزعمون أنهم راعوا خصوصيات الناس .

والبريد الإلكتروني هو من خصوصيات الإنسان ، فمنه يرسل ويستقبل رسائل تتعلق بالأسرة والعمل وسحب المال ، وغير ذلك ، وهذا يجعل اختراق البريد الخاص بالشخص من المحرمات ، ولا يحل لأحدٍ فعل ذلك ابتداءً .

وقد يوجد من الناس من هو مفسد مجرم ، يُعرف عنه الفحش والسوء ، يجاهر به ، ولا يراعي ذوقاً ، ولا حياءً ، ومثل هؤلاء يُفتي بعض العلماء بجواز اختراق بريدهم ، وسرقته .

ويظن بعض المتحمسين للدين أن هذا الجواز ينسحب على الكافر ، وهذا غير صحيح ، ولا نعلم أحداً من أهل العلم يفتي بذلك .

وعلى ذلك يقول العلماء

1. لا يجوز سرقة البريد الإلكتروني من أحدٍ من الأصدقاء ، لهواً ، وعبثاً ، ومزحاً .

فعَنْ السَّائِبِ بْنِ يَزِيدَ رضي الله عنه أَنَّه سَمِعَ رَسُولَ اللَّهِ صلى الله عليه وسلم يَقُولُ : (لاَ يَأْخُذَنَّ أَحَدُكُمْ مَتَاعَ أَخِيهِ لاَعِبًا وَلاَ جَادًّا ، فَمَنْ أَخَذَ عَصَا أَخِيهِ فَلْيَرُدَّهَا إِلَيْهِ) .

رواه الترمذي (2160) وأبو داود (5003) ، وحسَّنه الألباني في " صحيح الترمذي " .

قال شمس الحق العظيم آبادي رحمه الله :

"قال الخطابي : معناه : أن يأخذه على وجه الهزل وسبيل المزاح ، ثم يحبسه عنه ، ولا يرده ، فيصير ذلك جِدّاً . انتهى .

وجه النهي عن الأخذ جِدّاً : ظاهر ؛ لأنه سرقة ، وأما النهي عن الأخذ لعباً : فلأنه لا فائدة فيه ، بل قد يكون سبباً

لإدخال الغيظ ، والأذى على صاحب المتاع" .انتهى من " عون المعبود شرح سنن أبي داود " (13 / 236) .

ومن أعظم حكَم هذا التحريم : هو عدم ترويع صاحب الشيء المأخوذ .

فعَنْ عَبْدِ الرَّحْمَنِ بْنِ أَبِي لَيْلَى قَالَ : حَدَّثَنَا أَصْحَابُ رَسُولِ اللهِ صَلَّى الله عَلَيْهِ وَسَلَّمَ أَنَّهُمْ كَانُوا يَسِيرُونَ مَعَ رَسُولِ اللهِ صَلَّى الله عَلَيْهِ وَسَلَّمَ فِي مَسِيرٍ ، فَنَامَ رَجُلٌ مِنْهُمْ ، فَانْطَلَقَ بَعْضُهُمْ إِلَى نبْلٍ مَعَهُ ، فَأَخَذَهَا ، فَلَمَّا اسْتَيْقَظَ الرَّجُلُ فَزِعَ ، فَضَحِكَ الْقَوْمُ ، فَقَالَ : مَا يُضْحِكُكُمْ ؟ ، فَقَالُوا : لا ، إلا أَنَّا أَخَذْنَا نبْلَ هَذَا فَفَزِعَ ، فَقَالَ رَسُولُ اللهِ صَلَّى الله عَلَيْهِ وَسَلَّمَ : (لا يَحِلُّ لِمُسْلِمٍ أَنْ يُرَوِّعَ مُسْلِمًا) رواه أحمد (23064) - واللفظ له - وأبو داود (4351) ، وصححه الألباني في "صحيح أبي داود" .

والمطلوب ممن فعل ذلك : أن يتوب من فعلته ، ويعزم على عدم العوْد ، وأن يرجع البريد لصاحبه ، كما في الحديث الأول (فليردَّها إليه) .

2. يجوز الاستيلاء على بريد من عُرف عنه التعدي على الناس ، وعلى خصوصياتهم ، وابتزازهم ، والتعدي عليهم وظلمهم ، وهذا له شروط :

أ. أن يُجزم بعدوانه وتعديه على المسلمين .

ب. أن تتلف الرسائل وموادها مباشرة دون النظر إليها ، أو حفظها .

ج. أن يُجزم أو يغلب على الظن نفع هذه الطريقة ؛ لأن الغالب على أهل الفساد الاحتفاظ برسائل وصور وملفات من يتعدون عليهم على أجهزتهم ، وليس في بريدهم .

3. الاستيلاء على بريد المجرمين والمفسدين من الكفار والمسلمين لا بقصد أخذ بريدهم والاستيلاء عليه ، بل بقصد تتبع خططهم ومراقبة تصرفاتهم وأفعالهم ، وهذا واجب على من قدر عليه ، وله شروط :

أ. أن يُجزم أو يغلب على الظن فسادهم أو إجرامهم .

ب. أن تكون المراقبة والتتبع من مجموعة أو هيئة حسبة ، ولا ينفرد بها شخص وحده ؛ والتجسس على الكفار لا يكون لمصلحة الفرد الواحد ، ولا باجتهاده الشخصي ، بل يكون ذلك جزءا من عمل جهادي ، يقصد به النكاية في

العدو ، أو إعانة المجاهدين عليهم ، ومعرفة عوراتهم ومواطن ضعفهم ، ومحاربتهم من خلال ذلك ، أو استخدام ذلك فيما يسمى بالحرب النفسية ، وإذا كان " الغزو لا يجوز أن يقيمه كل واحد على الانفراد " [نقله ابن مفلح في الفروع 200/6] ، فمن باب أولى مثل هذه الأعمال التي لا يتمحض فيها جانب الجهاد ، ولا تتحقق فيها مصلحة النكاية في العدو دائما ، بل يخشى منها مفسدة الافتتان بما يجده في هذه الرسائل أو الإيميلات الخاصة ، ثم يخشى عليه أيضا أن يتحول ذلك عنده إلى بلاء في نفسه ، يفتح عليه محبة الاطلاع على العورات ، وهتك الأستار.

ج. عدم الاحتفاظ بخصوصيات الناس ، وعدم تتبع مسائل صاحب البريد الشخصية ؛ لعدم دخوله في استثناء التعدي على حقوق الآخرين وخصوصياتهم .

قال الدكتور عبد الرحمن بن عبد الله السند حفظه الله :

" واستثناء من ذلك فقد يكون التجسس مشروعاً في أحوال معينة كالتجسس على المجرمين ، فقد لا يعرفون إلا بطريق التجسس ، وقد أجاز الفقهاء التجسس على اللصوص وقطاع الطريق ، وطلبهم بطريق التجسس عليهم وتتبع أخبارهم - انظر " تبصرة الحكام لابن فرحون " (171/2) - ، وكذلك يجوز التجسس في حال الحرب بين المسلمين وغيرهم لمعرفة أخبار جيش الكفار وعددهم وعتادهم ومحل إقامتهم وما إلى ذلك .

وكذلك يجوز اختراق البريد الإلكتروني للمجرمين المفسدين في الأرض واللصوص وقطاع الطريق ، لتتبعهم ، ومعرفة خططهم وأماكن وجودهم ، لقطع شرهم ودفع ضررهم عن المسلمين ، وهذا موافق لمقاصد الشريعة الإسلامية التي جاءت بحفظ الدين والعرض والمال والنفس والعقل " .

2- 2التكييف القانوني لأختراق البريد الالكتروني

إن واقعة الاعتداء على البريد الإلكتروني تشكل العديد من الجرائم المبينة نصاً في قانون العقوبات وهي تتعدد بتعدد غرض الجاني (القصد الجنائي) وسلوكه الإجرامي ، فهو فعل واحد إلا أن الجرائم تتعدد وتتنوع ، سواء كانت لدافع إجرامي واحد أم لدوافع متعددة . فبمجرد وقوع الاختراق تتحقق جريمة انتهاك الحرمة ، فكما لا يجوز الدخول إلى المساكن والسيارات وتفتيش الحقائب ، لا يجوز أيضاً الدخول إلى البريد الإلكتروني، وبما أن هذه الانتهاكات تمثل جرائم يعاقب عليها القانون ؛ فإن اختراق البريد الإلكتروني يمثل جريمة يعاقب عليها القانون . أما إذا استعمل الجاني البريد الإلكتروني وهو خاص بالغير على اعتبار أنه هو صاحبه خصوصا في مخاطباته مع الغير أو توجيه أو استقبال مراسلات عليه فهو يعتبر انتحال للشخصيه , حيث أن الإيميل - كما تقدم ذكره - يرقى ليتمازج مع شخص صاحبه ,إذ أن العلاقات المميزة للبريد إلكتروني عن غيره هي ذاتها التي تميز الشخص الطبيعي في العالم الإلكتروني,إذ يعرف الشخص بمسمي بريده الإلكتروني , ومن ثم يكون الجاني قد استعمل اسم الشخص صاحب البريد الإلكتروني (المجني عليه) وانتحل شخصيته في العالم الإلكتروني , وهذه الجريمة هي ذاتها الجريمة المنصوص عليها في المادة 355 عقوبات والتي تنص علي : (يعاقب بالحبس مدة لا تتجاوز سنة كل من ضلل الغير بانتحال شخصية أخرى لتحقيق منفعة لنفسه أو للغير أو لإلحاق ضرر بآخرين ، أو انتحل لنفسه أو لغيره اسماً مزوراً أو صفة كاذبة أو انتحل صفة تترتب عليها آثار قانونية ، كل هذا ما لم يكن الفعل جريمة أشد ضد الثقة العامة

أما إذا اختلس الجاني أشياء أخرى أو ممتلكات موجودة فإنها إضافة إلي ما ذكر تمثل جريمة سرقة إذا ما اكتملت فيها الأركان , وفي بعض الأحيان لا تقتصر المسؤولية على الجاني بل تتعداه إلى الغير ، وذلك عندما تقع الجريمة من داخل مقهى إنترنت على سبيل المثال ، أو من غير صاحب الخط الخاص ، عندها تكون المسؤولية مسؤولية

مركبة ، ليست مقتصرة على الجاني فقط - كما سبق بيانه - ، فإن القانون الذي ينظم نشاط مقاهي الإنترنت هو القانون التجاري ، سواء من حيث ضرورة الالتزام باستصدار ترخيص ، أو من حيث مسك الدفاتر التجارية ، إذ ألزمت المادة من القانون التجاري الليبي - على سبيل المثال – ضرورة مسك دفترين ، أحدهما دفتر الجرد والميزانية ، والآخر دفتر اليومية، وهذا الأخير مهم جداً ، إذ من الأحوال اليومية المتعلقة بمحل الإنترنت تسجيل الزبائن ، وساعة الحضور والانصراف ، وغيرها من البيانات التي تقلل من وقوع الجرائم الإلكترونية وتساعد كثيراً في ضبطها .

وإذا ما التزم صاحب ألنت بهذه الدفاتر فإنه لا يحمل المسؤولية ، فإذا ما حدث جرم مما ذكر ،- إذا لم يقم بذلك – فإن المسؤولية التقصيرية تلحقه ، وهي يترتب عنها إلزامه بالتعويض .

2-3الأساس القانوني لتجريم السطو على البريد الالكتروني

تنقسم القواعد القانونية من حيث الإلزام إلى قواعد آمرة وأخرى مكملة ؛ والقواعد الآمرة ـ وهي التي لا يجوز للأفراد الاتفاق على مخالفتها ، أما المكملة فهي التي يجوز للأفراد الاتفاق على مخالفتها ، والذي يتضح من هذا التعريف الموجز وبالرغم من أنه قصير إلا أنه يبين نتيجة هامة ، وهي أن القواعد الآمرة هي التي تمس كيان المجتمع ولا تقتصر على شخص معين ، بخلاف المكملة التي لا تتعدى الأفراد أطراف العلاقة ، وبتطبيق تلك القواعد التي تنظم جرائم السطو على البريد الإلكتروني سواء في التشريع التقليدي ، أو التشريع المستقبلي , فإنها من القواعد الآمرة لكون هذه الجريمة تمس الأمن العام الذي هو أحد عناصر النظام العام ، وعلى اعتبار أن ذلك يمس المجتمع فهو من القواعد الآمرة التي لا يجوز الاتفاق على مخالفتها ، ومن ثم فإن هذه القواعد من النظام العام .

- الآثار القانونية المترتبة على اعتبار هذه القواعد من النظام العام :-

تنشأ على هذا التأصيل القانوني الذي سبق توضيحه من أن القواعد التي تنظم جريمة السطو على البريد الإلكتروني من النظام العام – وذلك شأنها شأن القانون الجنائي – عدة آثار ، أهمها :

1- اعتبار هذه القواعد القانونية من القانون العام : وهي أهم النتائج لأن هذه الجريمة تمس الأمن العام الذي هو أحد عناصر النظام العام الذي يرتبط مع القانون العام ارتباطاً شرطياً .

فالقانون العام بخلاف القانون الخاص - الذي ينظم العلاقة التي لا تتجاوز أطراف العلاقات الخاصة للأفراد أو من في حكمهم - ، أما القانون العام فهو الذي ينظم ويضبط العلاقات التي تتصل بالكيان الاجتماعي والتي عادة تتعهد الدولة أو أحد المؤسسات التابعة لها بتطبيقه.

2- إن الدولة هي التي تقوم بإصدار التشريعات اللازمة لحماية الأمن العام بواسطة الأجهزة التشريعية , وتنفيذها عن طريق أجهزتها التنفيذية ، ولها في سبيل تحقيق هذه المصلحة العامة المبتغاة امتياز التنفيذ المباشر باعتبارها ذات سلطة عامة ، سواء قامت بها هي مباشرة أم عهدت بها للغير .

3- إن من أهم امتيازات الدولة والمؤسسات التابعة لها بصدد تطبيق هذا القانون قيامها بمهمة الضبط الإداري للحد من جريمة السطو على البريد الإلكتروني .

والضبط الإداري يعتبر من أهم الوسائل التي يقوم بها رجال السلطة العامة في مكافحة الجريمة ، سواء من حيث التراخيص لمزاولة الأنشطة أو من حيث الإجراءات الإدارية التي ترسمها الإدارة للوقاية من الجريمة أو حصر أماكن وقوعها لسهولة ضبطها ، وهذه القواعد عادة تتواجد في القانون العام ، وقد تتواجد أيضاً في أحكام القانون الخاص ، وهي موجودة حالياً في التشريعات النافذة إلا أنني أهيب بالمشرع لدى الأنظمة العربية والدولية عموماً

بإصدار تشريع خاص بذلك وفق آخر التطورات ، والتي سوف يتضح شيء منها فيما يتعلق

2-4المسؤولية القانونية:

1.المسئولية الجنائية

لاشك أن السطو على الإيميل يمثل جريمة يعاقب عليها القانون ، سواء في أحكام التشريعات التقليدية أم تشريعات الإنترنت ، وأهيب بالمشرع إلى إصدارها فإذا ما تبين أن شخصاً ما تم ضبطه في جريمة سطو ، سواء بالإجراءات المذكورة أعلاه أو بأي إثبات آخر ، فإن فعله هذا يحمله المسؤولية الجنائية ، التي يترتب عليها العقاب ، الذي من شأنه أن يرتدع به الجاني ، كما يعتبر به الغيره .

لكن السؤال الذي يطرح نفسه ، هل التشريعات القنونية الحالية كافية لذلك ؟

أقول أنه بالرغم من أهمية هذه التشريعات من حيث أنها تمثل الجذور التاريخية لما سيصدر من تشريعات ، كما أنه لا يمكن الاستغناء عنها في الوقت الراهن ، إلا أنها قد شرعت في زمن لم تحدث به هذه التطورات الرهيبةفي عالم الإتصال والمعلومات ، ومن ثم فإن الأمر يتطلب تشريعات تواكب العصر وتساير الزمن.

2. المسؤولية المدنية :

إن الجرم الجنائي يمثل خطأ ، وهذا الخطأ ينشأ عنه ضرر وبالتالي فإن المسؤولية تكون تكاملت بتوافر عناصرها (الخطأ والضرر وعلاقة السببية)، وبالتالي فإن كل خطأ سبب ضرراً للغير يلزم مرتكبه بالتعويض (مادة 166 / مدني) فيكون من حق المتضرر أن يطالب محدث الضرر بالتعويض .

وهذه هي القواعد العامة للمسؤولية المدنية ، إلا أن الخصوصية التي يمكن إضافتها في الخطأ المترتب على جرائم السطو على البريد الإلكتروني ، تكمن في أمرين هما:-

الأول :- وهو ضرورة مراعاة خطورة السطو وكذا جرائم الإنترنت عموماً في تقدير قيمة التعويض ، إذ أنها ليست من الجرائم العادية ومن ثم فإن الأضرار الناجمة عنها عادة تكون بليغة ، وأرى أن يترك تقدير ذلك لقاضي الموضوع .

الثاني :- يحدث هذا النوع من الجرائم من صاحب الخط وقد يحدث من شخص آخر كما في مقاهي الإنترنت ، فإذا أثبت لنا الدليل الرقمي أن الجرم وقع من الخط (س) فإن من صدر باسمه هذا الرقم ومنح له ترخيص لاستعماله يكون هو المسؤول عن ذلك جنائياً ومدنياً ولو حدث من الغير ، ما لم يثبت أنه قام بتنفيذ الإجراءات الضبطية المطلوبة منه .

فإذا أثبت أنه قام بمسك السجل المطلوب – والذي سبق ذكره – فإنه في هذه الحالة تبرأ ساحته ، أما إذا تبين العكس فإنه يسأل عن تقصيره ، ويتحمل المسؤولية كاملة .

وبهذا يكون من شأن المسؤولية المدنية أن تقلل من جرائم السطو حيث تردع الجاني من العود ، وكذلك الغير .

المبحث الثالث

الطرق التقنية لحماية البريد الالكتروني من خطر الإختراق

يمثل البريد الإلكتروني أداة من أبرز أدوات التواصل العصرية ومن النادر وجود شخص لم يسمع عن البريد الإلكتروني أو لم يستخدمه، كما أنه أصبح من أول الأهداف التي يسعى وراءها المخترقون(Hackers) ، لذلك يجب الحرص على حمايته، والخطوات التالية توضح بعض الأساليب والطرق التي تساعد على حماية بريدك الإلكتروني:

1.المرفقات Attachments

وهي الملفات التي ترفق مع الرسالة، فقد يستغلها المرسل بإرفاق بعض البرمجيات الضارة، ومايالي بعض النصائح لتجنب ذلك:

1. عدم القيام بفتح أو حفظ أي مرفق إلا إذا كنت تتوقع استقبال ذلك الملف.
2. قبل فتح أي ملف مرفق قم بفحصه بأحد برامج مكافحة الفيروسات.

وفيما يلي أمثلة لبعض امتدادات الملفات المرفقة التي غالباً ما تحتوي على البرمجيات الضارة:

vbs, bat. pif, scr, exe, dll

2. الرسائل الاحتيالية Phishing

هي إحدى الطرق المفضلة لدى المخترق (Hacker) أو المحتال، حتى يتمكن من سرقة بريدك الإلكتروني أو معلوماتك الحساسة، والأمثلة على ذلك كثيرة ومتجددة، منها أن تصلك رسالة بنفس شكل وصياغة مزود خدمة بريدك الإلكتروني أو البنك الذي تتعامل معه، ويطلب منك تعديل بياناتك الخاصة لوجود مشكلة فنية ويضع رابط موقع إلكتروني مزيفا شبيها بموقع مزود الخدمة الأصلي أو البنك، وهنا قد لا يستطيع المستخدم تمييز الموقع المزيف ويضع جميع معلوماته المهمة ومنها كلمة السر. ولتفادي الوقوع في مثل هذه الحيل يجب التأكد من وجود قفل الأمان في زاوية المتصفح والتي تدل على وجود الشهادة الرقمية (digital certificate) لاعتماد الموقع عند صفحة تسجيل الدخول، كما ينصح بالحذر والتحقق قبل إدخال أي معلومة خاصة على أي موقع إلكتروني.

3. استخدام أكثر من بريد

الطريقة المثلى في التعامل مع البريد الإلكتروني هي الاشتراك في أكثر من بريد واحد، بحيث يكون أحدهما مخصصا للمراسلات المهمة والحساسة، وفي هذه الحالة ينصح بالتالي:

1.عدم نشر البريد للعامة.

2.اختيار كلمة سر لا تقل عن 8 خانات مكونة من حروف وأرقام ورموز.

3.الحرص على تغيير كلمة السر من فترة لأخرى.

4.عدم تصفح البريد الإلكتروني على الأجهزة العامة.

5.يفضل أن يكون حساب البريد الإلكتروني من شركة موثوقة.

أما البريد الآخر فيكون بعكس الأول بحيث يكون للاستخدامات غير المهمة، فعلى سبيل المثال بعض المواقع تلزمك بوضع بريدك الإلكتروني حتى تقرأ المحتوى وعند القيام بذلك تقوم بإرسال رسائل دعاية وتنشر بريدك لمواقع أخرى، لذلك سيكون أكثر عرضة للخطر والرسائل الاقتحامية - (SPAM) الاحتيالية.(Phishing)

4. استخدام النص الخالي من رموز لغة الترميز(HTML)

عند استقبال رسالة إلكترونية يكون الخط فيها بألوان عديدة وأحجام مختلفة، فهي دلالة على أنها مكتوبة برموز لغة النصوص التشعبية لذلك ينصح خبراء أمن المعلومات على أن تستقبل الرسالة الأصلية(plain text) أي تكون خالية من رموز(html) ؛ وذلك لتفادي خطرين أولهما احتمال معرفة معلومات خاصة بجهازك، والثاني احتمال زرع برمجيات ضارة في جهازك، وفيما يلي تفصيل لهذين الخطرين.

أولاً: خطر انتهاك الخصوصية

عندما يرسل لك شخص رسالة تحتوي على رموز (html) فقد يكون باستطاعته معرفة التالي عنك:

عنوان بروتوكول الانترنت (IP) لجهازك.

وقت قراءة الرسالة وتاريخها.

نوع نظام التشغيل ومتصفح الإنترنت.

ومعرفة هذه المعلومات من قبل المخترق تجعل جهازك أكثر عرضة لمخاطر أمن المعلومات.

ثانياً: احتواؤها على برمجيات تنفيذية

أيضاً باستطاعة المرسل أن يضيف من خلال رموز (html) بعض البرمجيات الضارة وتكون مخفية داخل الترميز ولا يستطيع المستخدم تمييزها.

5. الاتصال الآمن

تستطيع تصفح بريدك الإلكتروني بطريقة آمنة بأحد الأساليب التالية:

أولاً: عن طريق متصفح الإنترنت مثل هوتميل (Hotmail) وياهو(yahoo) ، ففي هذه الحالة تأكد أن الموقع يدعم بروتوكول التشفير(https) ، وتستطيع معرفة ذلك عن طريق ظهور أيقونة قفل صغير في شريط الحالة للمتصفح.

ثانياً: عن طريق برامج إدارة البريد مثل مايكروسوفت أوتلوك(Microsoft outlook) ، ففي هذه الحالة تأكد من وضع الإعدادات الصحيحة عند استخدام بروتوكول جلب البريد (pop3) وذلك عن طريق خاصية التشفير (ssl) ويكون البريد محمياً باسم مستخدم وكلمة سر.

6. استخدام التوقيع الإلكتروني

يستخدم التوقيع الإلكتروني في حال الحاجة للمراسلات الموثوقة والرسمية والتجارية، التي تتطلب قدراً أعلى من الحفاظ على السرية وأمن المعلومات. والتوقيع الإلكتروني لا يقصد به الاسم أو الصورة التي تظهر أسفل الرسالة، بل يقصد به توثيق مصدر الرسالة باستخدام شهادة رقمية تستطيع الحصول عليها من جهة موثوقة مخولة بإصدار هذا النوع من الشهادات، وتحتوي الشهادة الرقمية على مفتاح عام وحيد ومعلومات عن صاحب المفتاح العام، وأيضاً مفتاح خاص لا يعرفه إلا مالك الشهادة، والتوقيع الإلكتروني يولّد عن طريق برنامج البريد والمفتاح الخاص، والغرض من استخدامه تأكيد الرسالة وضمان عدم تحريف محتوى الرسالة.

الخاتمة

يتبع المخترقون مجموعة كبيرة من الأدوات والبرامج التي تمكنهم من مهاجمة وإختراق البريد الالكتروني وعلى تعددها وخطورتها يمكن للمستخدم الاحتراز والوقاية متها وذالك باتباع بعض النصائح منها:

- عدم الرد على رسائل البريد الإلكتروني التي تطلب معلوماتك الشخصية.
- . عدم التعامل مع الروبط المشبوهة
- الحرص على استخدام كلمات مرور قوية وتغييرها باستمرار لتجنب كشفها.
- عدم ارسال معلومات شخصية في رسائل البريد الإلكترونية المنتظمة.
- . ممارسة العمال مع المؤسسات الموثوقة فقط ، حتى لا تقوم بتمرير اسمك ومعلوماتك الشخصية للآخرين لحماية الكمبيوتر الشخصي الخاص بك.
- استخدام جدار الحماية وتحديث الكمبيوتر الخاص بك واستخدام برامج مكافحة الفيروسات والحرص على تحديثها باستمرار وشراء النسخ الأصلية من البرامج .
- استخدام أجهزة مراقبة المتطفلين على مستوى الحكومات والمؤسسات الكبيرة.
- تجنب خطر الهندسة الاجتماعية .

ختاماً اتمنى ان أكون قد وفقت في الالمام والإحاطة بجوانب هذا الموضوع المهمة

سبحانك لاعلم لنا الا ماعلمتنا إنك انت العليم الحكيم وآخر دعوانا أن الحمد لله رب العالمين

المراجع

1.كتب

أحمد صلاح الدين عبدالله،التجارة الالكترونية،جامعة السودان المفتوحة،الاولى،2005.

2.مواقع الكترونية

http://islamqa.info/ar/ref/114836 20/11/2012

http://www.minshawi.com/other/muhashy1.htm 12/10/2012

http://www.oman0.net/showthread.php?t=668233 20/11l2012

http://www.alwaei.com/site/index.php?cID=1089 20/11l2012

3.أوراق علمية وبحثية

عثمان سعيد المحيشي,ورقة عمل المنظمة العربية للتنمية الإدارية،ليبيا,2005م