الجريمة الإلكترونية: المنظور النفسي، الاجتماعي والأمني

2017-04-02د. منير طبي

يصف أستاذ علم الاجتماع الشهير بول تايلور وأساتذة آخرون في علم النفس، حسب مقال لنورا جبران نشر بجريدة الحياة السعودية حول سيكولوجيا الجرائم الالكترونية: الأنترنت تعري استعدادنا للجريمة، دوافع المجرمين الإلكترونيين بالفضول الشديد والانتقام، وأنهم يعانون من فراغ يسمح لهم بتمضية أوقات طويلة على شبكة الإنترنت، كما أنهم يتّصفون وفقاً لما جاء في كتاب The psychology of cybercrime أو الجرائم الإلكترونية، سيكولوجية الوساوس من يعانون بأنهم القهرية، فلا يمكنهم السيطرة على رغبتهم في ملاحقة الآخرين وإيذائهم.

كما أنهم مصابون باضطراب الشخصية النرجسية، ويعانون من تقدير ذات متدنٍّ، ولا يملكون القدرة على المواجهة أو التعامل مع المشكلات وإدارة العلاقات جيداً، ويفشلون في بناء علاقات صحّية، ويقلل اضطراب الشخصية النرجسية من قدرتهم على تقدير نتائج أفعالهم، ويرتكبون أفعالاً تخدم شهوتهم إلى الانتقام، أو فضول التجسّس لديهم، بغض النظر عن عواقب هذه الأفعال.

وتضيف نورا جبران أنّ استخدام الوسائل الإلكترونية في إيذاء الآخرين وملاحقتهم، متستّرين خلف هوية غير حقيقية، يشعرهم بمزيد من القوة والسيطرة اللتين تتطلّبهما نرجسيّتهم، وهوسهم المرضي بملاحقة ضحاياهم، وهو ما يوفره بسهولة الاتصال الدائم لهم ولضحاياهم على الشبكة العنكبوتية، من خلال أجهزة الهواتف والأجهزة المحمولة الأخرى، المرتبطة دائماً بالإنترنت، حيث ترتكز استراتيجيتهم في إيذاء الآخرين على الإصرار والمطاردة، وتتبع أصدقائهم ومن يتفاعلون معهم على شبكات التواصل الاجتماعي، ليروّجوا إشاعاتهم عن ضحاياهم وتشويههم أمامهم.

وتفيد دراسات أخرى بأن مجرمي الإنترنت هم أشخاص لديهم ميل مرتفع إلى القلق الخارج عن السيطرة، الذي يؤدّي إلى التهور في استخدام الوسائل الإلكترونية في شكل غير مدروس، في تصفية الحسابات والإساءة إلى الخصوم. كما أنّ لديهم اعتقاداً بأن الوسائل الإلكترونية أسرع في نشر الفضائح أو التشهير بالآخرين. وهم كذلك عرضة للاكتئاب أكثر وأسرع من غيرهم، ويشعرون بأن

الإساءة الإلكترونية أكثر أماناً لهم، واهمين أن من الصعب الوصول إليهم أو تحديد هويتهم الحقيقية.

ورغم أنه حتى الآن لم تظهر ملامح الصورة واضحة في تحديد صفات مجرمي الأنترنت والمعلومات وشرح سماتهم النفسية وتحديد دوافعهم، حسب ما تؤكده رجاء كامل في مقال حول الجريمة الالكترونية: الخطر داخل البيوت، خاصة مع قلة الدراسات الخاصة بهذه الظاهرة من جهة، ولصعوبة الفهم الجيد لمداها الحقيقي من جهة ثانية، والتطورات السريعة الحاصلة في ميدان الكمبيوتر والإنترنت من جهة ثالثة، فالمزيد من الوسائل والتكنولوجيات يعني المزيد من التغير في أنماط الجريمة وطرق الاعتداء، مما يساهم في إحداث تغير في سمات مجرمي الإنترنت، ومع ذلك يمكن تصنيف مجرمي الإنترنت وفق رجاء كامل حسب المنظور النفسي إلى الفئات التالية:

- فئة المتطفلين : أفراد هذه الفئة يرتكبون هذا النوع من الجريمة بغرض التحدي والإبداع، لدرجة أنهم ينصبون أنفسهم أوصياء على أمن الحاسوب في المؤسسات المختلفة وحمايتها.

- فئة المحترفين : يتميز أفراد هذه الفئة بالخبرة والفهم الواسع للمهارات التقنية، وبالتنظيم والتخطيط للأنشطة المرتكبة، وبالتالي فهي الأخطر مقارنة بباقي الفئات، وأساس اعتداءات هو تحقيق الكسب المادي لهم أو للجهات التي كلفتهم أو مولتهم أو سخرتهم، وقد تهدف إلى تحقيق أغراض سياسية أو التعبير عن موقف معين فكري أو نظري أو فلسفي.

- فئة الحاقدين : أفراد هذه الطائفة يرتكبون اعتداءاتهم الإجرامية بدافع الرغبة في الانتقام والثأر، وقد يكون الهدف هو شن حرب معلوماتية تقوم بها حكومة أو جهة سيادية معينة في مواجهة أخرى معادية لها، تهدف من خلال ذلك إلى شل وتدمير المواقع الخدماتية في إطار ما يسمى بالحكومة الإلكترونية أو المجتمع المعلوماتي، ومن أهم ما يميز أفراد هذه الفئة هو عدم تفاخرهم بأنشطتهم الإجرامية بل يعمدون إلى إخفائها دون وجود أي تفاعل أو تبادل للمعلومات بين أعضائها.

أما من المنظور الاجتماعي وفي ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظراً للعدد الهائل من

الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتاديها سواء كانوا أفراداً أم مؤسسات أم مجتمعات محافظة بأكملها، وهو ما دفع العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الإنترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجريمة، فراح المجرمون ينتهكون الأعراض ويغررون بالأطفال، إضافةً إلى اقترافهم لجرائم التشهير وتشويه السمعة عبر مواقع إلكترونية مخصصة لهذا الهدف.

إن انتشار وتوسع إطار الجريمة الالكترونية في العالم أمر ليس مستبعدا في ظل التطورات والقفزات الالكترونية الهائلة التي تشهدها الكثير من البلدان، ورغما عن وجود قوانين لجرائم المعلوماتية وما تشتمل عليه من عقوبات رادعة لكل من تسول له نفسه ارتكاب جريمة الكترونية إلا أن الأمر يتطلب كثيرا من الجهد من قبل القائمين على أمر هذه التكنولوجيا، حيث أن انتشار الجريمة الالكترونية قد يؤدي إلى خلل عام قد يهدد المجتمع كله في اقتصاده وسيادته وأمنه القومي بما يتطلب حماية المواقع المهمة والاستراتيجية من خلال استخدام التقنيات المتطورة ووسائل الكشف المبكر عن عمليات الاختراق.

وتشير رجاء كامل في معرض حديثها عن الجريمة الالكترونية إلى آخر إحصائيات تكلفة الجرائم الالكترونية على مستوى العالم، والتي بلغت 3 مليار دولار سنويا لاستغلال الأطفال جنسيا عبر الانترنت من خلال 100 ألف موقع إباحي للأطفال، وصل متوسط أعمارهم ال11 عام ذلك من خلال 26 شخصية كرتونية لاستدراجهم، وقال أن 25% من الاطفال تعرضوا للتحرش عبر الشات بجانب إفصاح 40% منهم عن بياناتهم الشخصية والعائلية بعفوية، وحذر بدرالدين ميرغني الأسر من استخدام أبنائهم للأنترنت وخطورة الموبايل بعد إضافة خدمات الانترنت، مشيرا إلى أن عدد المشتركين في الفيس بوك وصل إلى 500 مليون مشترك، مشددا على أحكام الرقابة على الأطفال وعدم السماح لهم بالاتصال الشبكي بشكل مستمر، ونادى الأسر بضرورة المراقبة اللصيقة لأبنائها ومنعهم من استخدامه بشكل مستدام خاصة عبر الموبايل، مشيرا إلى جهود شرطة المعلومات في مكافحة وصد هذا النوع من الجرائم، لما يترتب عليه من آثار اجتماعية وأخلاقية سيئة، مؤمنا على جهود القوات الأمنية في إجازة قوانين الجرائم الالكترونية حتى تواكب التطور التكنولوجي المتلاحق.

وفي ورقة علمية مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، نظمته أكاديمية شرطة دبي، لسلمان بن علي بن وهف القحطاني، حول أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة، أكد فيها أن المنظور الأمني للجريمة الإلكترونية يعني بشكل كبير أمن المعلومات من خلال الحماية من الاختراق، والاستخدام أو الوصول غير المصرح به، إضافة إلى عمليات أخرى لا تقل خطورة عما ذكرنا سابقا كالنسخ، الاتلاف، التعديل، التوزيع، النشر، والتدمير...

كل هذه العمليات الخطيرة تبرز أهمية أمن المعلومات في تأمين المعلومات وحمايتها من الأخطار التي تحيط بها، ويقوم هذا الجانب بتوفير الحماية والأمان من مختلف أنواع الجريمة الإلكترونية، إن مناقشة الأمن في ظل هذه التطورات التقنية ليس بالأمر السهل ومصطلح أمن المعلومات مفهوم شامل يحوي عدة أمور منها، أمن الشبكات وأمن الأجهزة المستخدمة وأمن المنظمات والأمن القانوني، ولوضع تصور شامل لحماية وأمن المعلومات، فلا بد أن نأخذ في الحسبان السياسة الأمنية أمن الأجهزة والأدوات أمن الشبكات الأمن المنظم والأمن القانوني، والسياسة الأمنية تعتبر الغطاء الأمني لجميع الجوانب الأمنية، وهي التي تعطي كيفية إنجاز الأمن ويجب بنائها على المتطلبات وليس على الاعتبارات التقنية، والأهداف السياسية لأي سياسة أمنية يجب أن تكون لإبقاء السرية والسلامة والكمال والتوفر لكل أصول الثروة المعلوماتية للمؤسسات واتصالاتها، وتشير السرية إلى المعلومات السرية التي لا يراها إلا البعض مثل: المدراء والمشرفون وبعض المستخدمين، وهذه معلومات يجب أن تبقى خاصة بالمؤسسات وببعض المستخدمين ضمن المؤسسات، وهي أيضاً تحفظ المعلومات من الاطلاع والكشف غير المخول أو المفاجئ، وتشير السلامة والكمال إلى معلومات وبيانات المؤسسات، ومن المهم أن تكون دقيقة وحديثة جداً، والتكامل أو السلامة تحمي المعلومات من التعديل الغير مخول أو المفاجئ، أخيراً التوفر ويشير إلى الوصول إلى معلومات ومصادر المؤسسات، ومن المهم جداً أن تكون معلومات ومصادر المؤسسات متوفرة بسهولة، والتوفر يضمن الوصول الموثوق فيه للبيانات متى وأينما دعت الحاجة لذلك، ويجب على السياسة الأمنية أن تضع في الحسبان هذه الأهداف الثلاثة عند دراسة اي تهديدات محتملة على المؤسسة.

وحسب وزارة الاتصالات وتقنية المعلومات السعودية، وفي مجال قريب من أمن المؤسسات والهيئات، أصدر مكتب التحقيقات الفيدرالي الأمريكي \"FBI\" تقريراً حديثاً حذر فيه من ارتفاع

متوقع لعدد ضحايا رسائل الاحتيال الإلكتروني في قطاع الأعمال، حيث تستهدف هذه الرسائل الشركات التجارية وتتسبب بخسائر مالية ضخمة، وأكد التقرير أن المخططين لهذه الرسائل يبذلون جهداً كبيراً في محاولة مطابقة عناوين البريد الإلكتروني، أو استخدام الهندسة الاجتماعية لانتحال شخصية الرئيس التنفيذي أو محامي الشركة المستهدفة، حيث يقومون بإجراء دراسة عن موظفي الشركة المسؤولين عن العمليات المالية، ويستخدمون صياغة محددة في رسائلهم لخداع الموظفين، ثم يطلبون في هذه الرسالة إجراء تحويل مصرفي مشبوه إلى حساباتهم، ورصد التقرير تنوّع شريحة الضحايا ما بين مؤسسات ضخمة وشركات تقنية وشركات ناشئة ومنظمات غير ربحية، وكانت الهجمات تستهدف الشركات التي لديها أعمال مع مورّدين أجانب، أو الشركات التي تقوم بعمليات تحويل مصرفي بشكل متكرر.

وأشار التقرير إلى ورود بلاغات عن عمليات الاحتيال هذه من جميع الولايات الأمريكية بالإضافة إلى79 دولة أخرى، كما تم رصد أكثر من 17 ألف ضحية لهذه العمليات ما بين شهر أكتوبر2013 وشهر فبراير 2016، وبالنسبة للخسائر المتوقعة لهذه العمليات فقدرها التقرير بـ 2.3 مليار دولار، مع ازدياد عمليات الاحتيال عبر البريد الإلكتروني بنسبة 270% منذ شهر يناير 2015، كما تراوحت الخسائر في ولاية أريزونا في كل عملية احتيال ما بين 25 و75 ألف دولار. يذكر أن عدداً من الشركات الكبيرة تضررت من هذه الرسائل، حيث قام عدد من الموظفين في سناب شات ،الاحتيالي البريد لرسائل ضحايا بالوقوع \"Fast\" وفاست ،\"Seagate\" وسيجيت ،\"Snapchat\" وقاموا بتحويلات مالية إلى هذه الحسابات.

ولذلك فإن الوقاية هي أمثل الأساليب نفعا لصد هذه الجرائم حسب سامر محمد سعيد، في كتابه الأنترنت: المنافع والمخاطر ومن بينها:

- استخدام جدار الحماية well fire : وهو حاجز يوضع بين الشبكة الداخلية للأنترنت وخادم شبكة الأنترنت، ومن أهم مهامه فحص المعلومات الداخلة والخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات، وتقديم تقارير عن التحركات المشبوهة، ولكنه يمكن أن يعطل بعض المعلومات ويحدث عطب.

- التشفير: وهو تحويل المعلومة من نص واضح إلى آخر غير مفهوم، وقد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.

- التوقيع الرقمي: وهو تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية.

- استخدام أنظمة كشف الاختراقات ووضع حلول للثغرات الأمنية

- وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقها.

- الاحتفاظ بنسخ احتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة. بالشبكة.

- تنصيب برامج لمنع ظهور الصور الخلاعية والاتصال بالمواقع الإرهابية.

- ضرورة استخدام بعض البرامج التي صممت خصيصا للكشف والوقاية من الفيروس والبعد عن استعمال كلمة السر البسيطة.

- عند فتح البريد الإلكتروني يجب معرفة من المرسل خشية أن يكون فيروس.

* باحث وأكاديمي جزائري

.....

* الآراء الواردة لا تعبر بالضرورة عن رأي شبكة النبأ المعلوماتية