****

**الجرائم الإلكترونية وأنعكاساتهاعلى المجتمع ورؤية القانون لها**

يشهد العالم تطوراً كبيراً ونقلة نوعية في الجرائم الألكترونية و كيفية التواصل فيما بين البشر، أبتداءاً بالوسائل البسيطة من الريشة والحبر على ورق يرسل بمظروف وصولا الى تطور هائل بالتكنولوجيا تمثلت في ظهور الحواسيب والأجهزة المحمولة وانتشار شبكة ضخمة من المعلومات الالكترونية وهي ما تعرف بشبكة الانترنت… لقد كان الهدف الأساسي من إيجاد أجهزة الكمبيوتر والأجهزة الذكية الأخرى هو تسخيرها لخدمة الإنسان في مجال الأعمال والمعاملات ، وكان لظهور تلك الأجهزة وتطورها بسرعة من مجرد أجهزة تقوم بعمليات حسابية إلى مخازن قادرة على تجميع واستيعاب كم ضخم من المعلومات والبيانات ، وقادرة على أسترجعها بسرعة وبدقة ،أن أحدثت مشكلة خطيرة تؤرق الكثيرين حول كيفية حماية تلك المعلومات بعد أن أصبحت في متناول اليد وبأقل مجهود وأبسط حركة فلم يعد المجرم بحاجة إلى أدوات وآلات تقليدية لارتكاب جريمته ، نتج عن ذلك علاقات قانونية جديدة بحاجة إلى الحماية حال التعدي عليها سواء في مجال فروع القانون المختلفة أو بقانون خاص بها . إن التقدم العلمي والتطورات الحديثة ساهمت في إحداث وظهور أشكال وأساليب جديدة من صور الجرائم الالكترونية

وان هذا التطور احدث فارقا عظيما في حياة البشرية وحمل فوائد جمة لا تعد ولا تحصى اذ عمل هذا التطور الهائل على تقريب المسافات وسهولة الاتصال والتواصل بين البشرية عبر دول العالم

لذا تعد الجريمة الإلكترونية من أبــرز وأخطر التحديات الأمنية الـي تواجه كافة مجتمعات العالم في مجـال

استخدامات تقنية المعلومات والاتـصـالات على نطاق مؤسسات القطاع العام والخـاص والأفراد. والجرائم الإلكترونية نوعان: الأول: الجرائم الموجهة ضد جهاز الحاسب الآلي أو أنظمة تقنيةالمعلومات والاتصالات والهواتف المحموله، والنوع الثاني: تلك الجرائم الي يكون فيها الحاسب الآلي او الهاتف المحمول هما وسيلة لارتكابجرائم الاحتيال وسرقة الهويات وبطاقات الائتمان والأرصدة المالية والتزوير والاختلاس وسرقة حقوق الملكية الفكرية والإبتزاز والسلوك الانحرافي والاستغلال الجنسي للكبار وحتى للأطفال، إضافة إلى الترويج للعنصرية والطائفية و للأفكارالمتطرفة ودعم وتمويل الإرهاب

ظلت معدلات الجريمة الإلكترونية تتصاعد منذ عقد التسعينات وتضاعفت الجرائم وخسائرها

المالية بعد أن بلغ عدد مستخدمي الإنترنت 40% من سكان العالم في عام 2014 وقدرت الخسائر المالية – 450 مليار دولار وعدد الضحايا 556 مليون، وأصبحت الجريمة الإلكترونية مهدداً حقيقياًلأمن المعلومات ومصدر خطورة على الأشخاص كافة و الأمن القومي وعلى الأمن والسلم الدولين

اوتكوين صداقات ومعارف جديدة خارج نطاق الاسرة،

فالجريمة الألكترونية سنعرفها وبعدها نسرد اضرارها وعواقبها وخطورتها على المجتمع والامن الدوليين

حيث لم يتم وضع تعريف واضح من قبل المشرع لـ الجرائم الإلكترونية وما زال هناك اختلاف حول تعريفها ولكن يمكن نقول بانها سلوك غير قانوني يقدم على ارتكابه فرد او مجموعة من الافراد بواسطة الأجهزة الذكية والمواقع الالكترونية بهدف تحقيق مكاسب مختلفة، ويكون ذلك عن طريق ابتزاز الضحية وتهديدها وتخريب صورتها امام المجتمع الواقعي والافتراضي، أما بحسب وجهة النظر المجتمع الدولي فقد اعتبر الجريمة الالكترونية بأنها ممارسات وأعمال تتعلق بجهاز الحاسوب والأجهزة الذكية الأخرى التي تسعى لتحقيق مكاسب مادية او شخصية او التسبب بضرر.

لذا فوراء كل جريمة من الطبيعي مجرم الكتروني أقدم على أرتكابها لذا فالمجرم الالكتروني هو شخص يملك الكثير من القدرات والمهارات التقنية والبرمجية والذكاء ما يؤهله الى استغلال مداركه في اختراق الشبكات والحواسيب والأجهزة الذكية الاخرى واآليةعملها وتخزين البيانات والحصول عليها بالإضافة الى أستغلال مهاراته تلك في الاحتيال والسرقة والتزوير، وسمي مجرما لانه يستخدم مهاراته بطرق غير مشروعة وغير قانونية وتشكل فعلا محظورا بالقانون وفعلا مرفوضا ومنافيا للأخلاق بنظر المجتمع.والدين

تتنوع الجرائم الالكترونية بصور عديدة منها على سبيل المثال:

الجرائم الإلكترونية السياسية التي تعنى باستهداف الأمور السياسية الحساسة والهامة في الدولة، والتطفل على امن الدولة وسرقة المعلومات من خلال انتهاك المواقع العسكرية والسياسية التابعة للدولة.

الجرائم الإلكترونية التي تمارس ضد الحكومات عن طريق الدخول الى مواقع الوزارات بهدف تدمير البنية التحتية لتلك الوزارات او نشر اخبار كاذبه على تلك الصفحات العائدة لها.

وجرائم الإبتزاز والتهديد للأفراد: والتي تكون من خلال ابتزاز الضحية وتهديدها بنشر معلومات خاصة أو صور أو فيديوهات بهدف في نفس المجرم و في حال امتناع الضحية عن تنفيذ ما يتم طلبه يقوم المجرم بتنفيذ فعلة الأجرامي.

وجرائم التشهير الإلكتروني بحق الأشخاص من خلال الذم والتحقير والقذف ، وذلك عن طريق نشر معلومات عن شخص او هيئة معينة تنسب اليها بشكل مباشر.وايضا

الجرائم الإلكترونية لتزوير الهوية: وذلك من خلال انتحال شخصيات الافراد على مواقع التواصل بسرقة معلوماتهم الشخصية واستخدامها لأغراض غير قانونية.وكذلك

جرائم الملكية: وتكون عن طريق نشر روابط تؤدي الى الوصول الى الأجهزة وسرقة ما في داخلها من بيانات وبرامج وتعطيل تلك الأجهزة اما بشكل كلي او جزئي.

وغالبًا ما تنطوي الجريمة الالكترونية التي تستهدف أجهزة كمبيوتر على فيروسات وأنواع أخرى من البرامج الضارة.

قد يصيب المجرمون أجهزة الكمبيوتر بالفيروسات والبرامج الضارة لإلحاق الضرر بالأجهزة أو إيقافها عن العمل. وقد يستخدموا البرامج الضارة أيضًا لحذف البيانات أو سرقتها.

و لا يزال هناك صورعديدة لارتكاب الجرائم الإلكترونية والتي تستحدث بشكل مستمر، نتيجة التعمق بالمعرفة الالكترونية والاحتراف في البرمجة وغيرها

حيث وقّعت الولايات المتحدة على الاتفاقية الأوروبية بشأن الجرائم الالكترونية. تتميز الاتفاقية بنطاق واسع ويتم اعتبار الكثير من الجرائم الضارة المتعلقة بالكمبيوتر جرائم الكترونية. على سبيل المثال:

اعتراض البيانات بشكل غير قانوني أو سرقتها.

التدخل في الأنظمة بطريقة تعرّض الشبكة للخطر.

انتهاك حقوق النشر.

المقامرة غير المشروعة.

بيع السلع غير المشروعة عبر الإنترنت.

طلب مواد إباحية تستغل الأطفال أو إنتاجها أو امتلاكها.

إذًا، الآن وقد فهمت التهديد الذي تشكّله الجرائم الالكترونية، ما هي أفضل الطرق لحماية جهاز الكمبيوتر الخاص بك واجهزتك الأخرى الذكية من خطورة الجريمة الالكترونية هنا بعض النصائح الشائعة الذكر:

🌸إبقاء البرنامج ونظام التشغيل محدّثَين

يضمن إبقاء البرنامج ونظام التشغيل لديك محدّثَين استفادتك من أحدث تصحيحات الأمن لحماية جهاز الكمبيوتر الخاص بك.

🌸أستخدام برنامج مكافحة الفيروسات وإبقائه محدّثًا

يشكّل استخدام برنامج لمكافحة الفيروسات أو حل شامل لأمن الإنترنت مثل البرنامج الشهير

Kaspersky Total Security

هو بمثابة طريقة ذكية لحماية النظام من الهجمات.

ويتيح لك برنامج مكافحة الفيروسات فحص الجهاز واكتشاف التهديدات وإزالتها قبل أن تتطور لتصبح مشكلة. يساعد وجود مثل هذه الحماية في حماية جهاز الكمبيوتر الخاص بك وبياناتك من الجرائم الالكترونية، مما يوفّر لك راحة البال

إذا كنت تستخدم برنامجًا لمكافحة الفيروسات، فتأكد من إبقائه محدّثًا للحصول على أفضل مستوى من الحماية.

🌸وعدم تقديم المعلومات الشخصية إلا إذا كنت آمنًا

لا تقدم أي معلومات شخصية عبر الهاتف أو عبر البريد الالكتروني إلا إذا كنت متأكدًا تمامًا من أنّ الخط أو البريد الالكتروني آمن. تأكد من هوية الشخص الذي تتحدث معه.

🌸الاتصال بالشركات مباشرةً بشأن الطلبات المشبوهة

إذا اتصل بك أحد من شركة ما وطلب منك بيانات شخصية، فانهِ المكالمة. واتصل بها مجددًا باستخدام الرقم الموجود على موقع الويب الرسمي الخاص بها لضمان أنك تتحدث معها وليس مع مجرم إلكتروني.

🌸تكمن الطريقة الأمثل في استخدام هاتف آخر لأنه يمكن للمجرمين الالكترونيين إبقاء الخط مفتوحًا. عندما تعتقد أنك اتصلت بالشركة مجددًا، يمكنهم الادّعاء بأنهم من المصرف أو مؤسسة أخرى تعتقد أنك تتحدث معها.

🌸استخدام كلمات مرور قوية

تأكد من استخدام كلمات مرور قوية لا يمكن للأشخاص معرفتها ولا تقم بتسجيلها في أي مكان. أو استخدم برنامج حسن السمعة لإدارة كلمات المرور وذلك من أجل إنشاء كلمات مرور قوية بشكل عشوائي لتسهيل هذا الأمر.

🌸عدم فتح المرفقات في رسائل البريد الالكتروني العشوائية أبدًا

تشكّل مرفقات البريد الالكتروني في رسائل البريد الالكتروني العشوائية طريقة تقليدية لإصابة جهاز الكمبيوتر ببرامج ضارة وغيرها من أشكال الجرائم الالكترونية. لا تفتح أبدًا مرفقًا من مرسِل لا تعرفه

🌸عدم النقر فوق الروابط في رسائل البريد الالكتروني العشوائية أو على مواقع الويب غير الموثوق بها حيث يشكّل النقر فوق الروابط في رسائل البريد الالكتروني العشوائية أو الرسائل الأخرى أو مواقع الويب غير المألوفة طريقة أخرى ليقع الأشخاص ضحايا للجرائم الالكترونية. تجنّب القيام بهذا الأمر للحفاظ على أمنك على

الإنترنت

. 🌸التنبّه لعناوين مواقع

التي تزورها URL

راقب عناوين المواقع التي تزورها. هل تبدو مشروعة وحقيقية؟ تجنّب النقر فوق الروابط ذات عناوين

غير المألوفة أوالتي تبدو غير مألوفة

إذا كان برنامج أمن الإنترنت لديك يشمل وظائف لضمان أمن المعاملات عبر الإنترنت، فتأكد من تشغيل البرنامج قبل تنفيذ المعاملات المالية عبر الإنترنت

مراقبة بياناتك المصرفية🌸

ستساعدك نصائحنا في تجنّب الوقوع ضحية للجرائم الالكترونية. لكن إذا فشلت كل الإجراءات الأخرى، فمن المهم اكتشاف أنك وقعت ضحية جريمة الكترونية بسرعة.

راقب بياناتك المصرفية واستفسر عن أي معاملات غير مألوفة مع المصرف. يمكن للمصرف التحقيق فيما إذا كانت عملية احتيالية.

لذا ان اتباع ماتقدم يجنبك من التعرض الى التهديد بالجرائم الالكترونية، فاحمِ نفسك منها

فالهدف من أرتكاب الجرائم الالكترونية من قبل ضعفاء النفوس والمجرمين هو أنهم لا شك ساعين لتحقيق اهداف متعددة تتمثل في

طبيعة هؤلاء الأشخاص الداخلية القائمة على التطفل على حسابات الاخرين وسرقة معلوماتهم بطرق غير مشروعة ودون اذنهم.

تحقيق الربح المادي من خلال ابتزاز الاخرين والحصول على مقابل مادي منهم او من خلال سرقة الحسابات البنكية والاستحواذ عليها ولعل هذا الهدف هو اهم ما يسعى اليه المجرم بحيث ان بعضهم يعتبرون بان ممارستهم لتلك الجريمة يشكل دخل مادي لهم كما وانه اصبح هناك شركات توظف الأشخاص للقيام بعمليات الابتزاز والتزوير والاحتيال والسرقة من وراء شاشات الحاسوب ودون معرفة هويتهم

التشهير بسمعة اشخاص قد يكون المجرم على علاقة ليست بجيدة به، فيدفعه بغضه الشديد الى استغلال منصات التواصل الاجتماعي للتشهير به والقاء الاتهامات الباطلة بحقه وقدحه وذمه.

من الممكن ان يلجأ بعض الأشخاص الى ممارسة نوع من أنواع الجرائم تلك بغرض التسلية بحسب معتقده.

الحصول على معلومات سرية وهامة قد تتعلق بافراد او بشركات او وزارات واستخدامها كاداة للابتزاز لتحقيق مطالب معينة.

محاولة للبحث عن الذات والحصول على التقدير ظنا من مرتكبيها بان اقدامهم على ارتكاب تلك الجرائم يؤدي الى زيادة شهرتهم وظهورهم.

لذا مما تقدم ذكرة فأن الجرائم الألكترونية تنعكس على المجتمع لذا فأن إنعكاسات الجرائم الإلكترونية على المجتمع

بأنها تشكل وباء ينهش ويفتك بامن وسلامة المجتمع، ويلحق به العديد من المخاطر والاضرار منها

هدم بناء الاسرة وتفككها من خلال ارتكاب نوع معين من الجرائم بحق احد افراد الاسرة وبالإضافة الى الإساءة بسمعة الافراد واظاهرهم بصورة غير لائقة امام المجتمع والمحيط حولهم ومن المخاطر أيضا تلك التي تتسبب بالاضرار الاقتصادية للدولة من خلال تدمير النظام الاقتصادي عن طريق التطفل على خصوصيات الدولة وعلى الأموال العامة، كما وانها تشكل خطرا على سيادة الدولة فمن الممكن ان تؤدي الى حدوث انقلابات سياسية وارتكاب اعمال إرهابية لذل وبما ان وسيلة التواصل والتسلية والترفيه أصبحت عن طريق التكنولوجيا فان انتشار تلك الجرائم هذه من شأنها تنشئة جيل فاسد لا يعطي أي اعتبارات لمبادئ الأخلاق والإنسانية فالكثير منها تتسبب باضرار نفسية للضحية قد تؤدي به للتفكير باهدار حياته فيلجأ للأنتحار للتخلص من الخطر المهدد به نتيجة خوفه من الابتزاز ومن الممكن ان يتم اهدار روح الضحية من قبل المجرم ذاته عند عجز الضحية عن تنفيذ مايطلبه منه.

وكذلك نشر الاخبار الكاذبة وتضليل الناس عن الحقائق، ونشر معلومات مخلة بالنظام العام والاداب.والشرف لبعض الأفراد وتشويه سمعتهم من قبل المبتز وأيضا

الحاق ضرر بالذمة المالية للشخص ضحية التهديد نتيجة اقدامه على دفع مبالغ ضخمة مقابل التخلص من التهديدات..

لذا أن رؤوية القانون أتجاة تلك الجرائم هو انه أوجب بالدول لوضع تشريعات لمواجهتها وكانت بداية انفتاحها على القانون الجنائي والذي يرسخ بداية هذه الفكرة قانون جرائم المعلوماتية الفرنسي الصادر سنة 1988 ويحمل الرقم 19 وما تبعه من قانونين أخرى ذات صلة ومنها التشريع الفرنسي الصادر في 4أغسطس 1994 المسمى بقانون Toubon ، ومن ثم توالت الدول في سن القوانين و التشريعات ومن الدول العربية التي اجتهدت في ذلك قانون الجرائم الالكترونية الأردني

لذا على القوانين الدولية أن تتخذ تدابير وعقوبات صارمة أتجاه مرتكبيها كلما تطور مرتكبيها في ابتكار طرق مستحدثة للأرتكاب لذا على القانون ضرورة شمول الهجمات الإلكترونية بما يسري على الهجمات المسلحة وضرورة استعمال حق الدفاع الشرعي للدول التي تتعرض لهذه الهجمات بناء على نصوص ميثاق الأمم المتحدة والقانون الدولي العام، نظراً أنه فعلياً لا يوجد أي سند قانوني يبرر استخدام حق الدفاع الشرعي ضد هذا النوع من الهجمات، ولكن في هذا المقال نستطيع أن نوردها تحت مقارنه هذه الجرائم ومعادلتها بالجرائم المسلحه كونهم في الحالتين ضرر وخطورة على المجتمع وامن الدولة ويمكننا تسميته العدوان غير المسلح وغير المباشر.

شكرا لأطلاعكم على المقال دمتم في رعاية الله وحفظه