الجرائـم الإلكترونية وآليـات التعامل معها للحد من تأثيرها على المجتمعات

بحث مقدم من

د/ رانيـا عبد الحميـد مبروك دسوقى

معلم أول (أ) ثانوى مواد فلسفية

دكتوراه الفلسفة فى التربية

(تخصص علم النفس التربوى)

كلية التربية

جامعة الاسكندرية

2023م

مقدمة

لقد أدى التطور السريع والمستمر لتقنيات الإعلام والإتصال إلى تزايد الإعتماد على الشبكات الإلكترونية ، فلم يعد الأمن مفهوماً ضيقاً يقتصر على ضبط الجرائم التقليدية بل ظهر نوع آخر من الجرائم يسمى بـ "الجرائم الإلكترونية" أو "جرائم شبكة المعلومات" أو "جرائم الانترنت" التى تنطوى على جرائم جمة تمس ؛ الحق فى المعلومات ، والحقوق المالية ، وحقوق الملكية الفكرية ، والحريات الشخصية ، وتهدد الأمن القومى ، والسيادة الوطنية ، وتشيع فقدان الثقة فى التقنية ، وتهدد إبداع وابتكار العقل البشري ، فهذا النوع من الجرائم يمثل خطورة على كافة المستويات الاقتصادية ، والاجتماعية ، والثقافية ، والأمنية و.....غيرها . ومن هنا وجب حماية الحق فى الخصوصية فى مواجهة الإنتهاك الإلكترونى .

مشكلة البحث

مع التطور التكنولوجى والتقنى وثورة الاتصالات ، صار الإعتماد المكثف على النظام الرقمى الذى مكن الأفراد من الاتصال بشكل أكثر فعالية وأقل تكلفة مقارنةً بالماضى ، حيث انعكس هذا التطور على أساليب ووسائل ارتكاب الجرائم ، بواسطة الربط بين هذه التقنيات ، حيث التعدى سواء من خلال القرصنه وسرقة الهويات أو الحسابات على شبكات التواصل الاجتماعى أو عن طريق اختراق البريد الالكترونى وما يترتب عنه فى اعتداء حرمة المواصلات والمراسلات وسرقتها (عبد الحليم بوفرين ، 2019) ، ويؤكد خالد إبراهيم ممدوح (2009) أنه كلما ظهرت تقنية جديدة ظهرت معها جرائم جديدة .

و لم يصبح الانترنت أيضاً وسيلة للتعارف والتواصل الاجتماعى فقط ، بل أصبح وسيلة للتعرض للمواد الإباحية واستغلال الشباب والأطفال (ناعوس بن يحى الطاهر ، 2015 ، 14) ، من هنا تعد الجريمة الإلكترونية من أكبر التحديات التى تواجهنا فى عصرنا اليوم ، إن لم تكن أكبرها على الإطلاق ، حيث تعددت أشكالها وصورها مما يتطلب تكاتف الجهود لمواجهة مخاطر تلك الجرائم الإلكترونية والعمل معاً لتحقيق مبدأ التكافل والتكامل بين المجتمعات (أكرم عبد الرازق المشهدانى ، 2015).

أهداف البحث

تتمثل أهداف البحث الحالى فى التالى :

1. بيان أنواع الجرائم الإلكترونية و أشكالها وصورها.
2. ابراز مخاطر الجرائم الإلكترونية على المجتمعات وخصوصاً فئة الشباب.
3. تفسير الأسباب الكامنة وراء الجرائم الإلكترونية.
4. التنبؤ (اقتراح) بآليات معالجة لتلك الجرائم الإلكترونية.

أسئلة البحث :

تتمثل أسئلة البحث فيما يلى :

1. الجرائم الإلكترونية : تعريفها– أسبابها– دوافعها
2. ماهى أنواع الجرائم الإلكترونية ؟
3. ما هو الفرق بين الجرائم الإلكترونية و الجرائم المعلوماتية ؟
4. ما هى مخاطر الجرائم الإلكترونية ؟
5. ما هى الفئات التي تستهدفها الجرائم الإلكترونية ؟
6. ما هو دور التنظيمات الإجتماعية لمواجهة الجرائم الإلكترونية وصولاً لآليات للتعامل مع هذه الجرائم ؟
7. ما هى الآليات المقترحة للتعامل مع هذه الجرائم الإلكترونية ؟

الجرائم الإلكترونية **Cyber Crimes**

يعرف محمد أمين الشوابكة (2011) الجرائم الإلكترونية بأنها " الجرائم المتعمدة التى تستخدم نظام المعلومات للحصول على المعلومات أو إتلافها أو اساءة استخدامها مما يؤدى إلى إلحاق الضرر بالمجنى عليه وتحقيق فائدة غير مشروعة للجانى ولها صور متعددة منها: تزوير بطاقات الإئتمان ، الاحتيال الإلكترونى، جرائم الكمبيوتر ، جرائم الانترنت ، قرصنة البرامج الكمبيوترية ، تزوير الأقراص المبرمجة".

وتعرف جريمة تقنية المعلومات بأنها" أى سلوك سئ متعمد يستهدف الإضرار بتقنية المعلومات أو يستخدم تقنية المعلومات لإلحاق الضرر ، أو ينتج عنه حصول أو محاولة حصول المجرم على فائدة لا يستحقها" . (Al-saggaf, Yeslam, 2011)

ويعرف حازم محمد مطر (2015) الجرائم الإلكترونية بأنها " نشاط اجرامى يتم عن طريق الانترنت ويمكن أن يشمل ذلك سرقة الملكية الفكرية ، سرقة الحسابات المصرفية ، نشر وتوزيع الفيروسات الضارة على أجهزة الكمبيوتر الأخرى ، نشر المعلومات السرية ، تعطيل البنية التحتية للبلاد" .

ويعرف فاطمة الزهراء دريم (2017) الجرائم الإلكترونية بأنها:"كل سلوك عدوانى يقوم بإحداث خلل على النظام القائم إحدى أوجه الجرائم والانتهاكات العدائية التى تهدد النظام القائم على شبكة الانترنت ويحدث فيه خلل"

ويعرف هنيدى بن عطية البشرى (2020) الجرائم الإلكترونية بأنها " مجموعة من الأفعال الغير مشروعة ، وتكون أجهزة الكمبيوتر وشبكة المعلومات وسيلة لإرتكابها وتسبب الكثير من المخاطرعلى مستوى الفرد والجماعة والمجتمع".

وتستخلص الباحثة أن "تعريف الجرائم الالكترونية يشمل جميع الجرائم التي تتم عبر شبكة الإنترنت عن طريق استخدام المعدات التقنية مثل الحاسوب والجوال، هذه الجرائم تمثل الكثير من الأضرار الجسيمة التي تلحق بالأشخاص، الجماعات، الحكومات، المؤسسات الخاصة، هذا لأن الغرض الأساسي لهذه الجرائم يتمثل في اختراق الأجهزة الإلكترونية والتسلل إليها للحصول على المعلومات والصور الشخصية وخلافه من الأغراض التي يتم الاختراق بغرض الاستيلاء عليها، و تختلف أساليب هذه الجرائم تبعًا للذكاء الخارق الذي يملكه هؤلاء المجرمين الذين يقوموا بتنفيذ هذه الجرائم الإلكترونية.

أسباب الجرائم الإلكترونية

يوجد العديد من الأسباب التي تؤدى إلى هذا النوع من الجرائم ألا وهى :

1- جرائم إلكترونية تتم على المستوى الفردي حيث تهدف هذه الجرائم إلى الحصول على هؤلاء المجرمين على التقدير من قبل الشخاص وذلك لأن هذه الجرائم تتم من قبل أشخاص ذات فئات صغيرة في العمر، كما أن التطور التكنولوجي السريع أدى إلى إتاحة الكثير من الفرص للعديد من الأشخاص العاطلين عن العمل ويحتاجون إلى الهروب من الواقع والتحدث مع أشخاص غرباء، والرغبة في إقامة الكثير من العلاقات الوهمية عبر شبكات التواصل الاجتماعي والذين يملكون معرفة كبيرة بالتقنيات الحديثة التي تساعدهم على القيام بمثل هذه الجرائم، تتم هذه الجرائم بواسطة أشخاص ذات نفوس مريضة حيث تعمل هذه الجرائم على إشاعة الخوف والرعب بين الأشخاص.

2- توجد أسباب تتعلق بالجرائم الإلكترونية على المستوى المجتمعي لزيادة التحضر المجتمعي الذي عناصره جميعًا، بالإضافة إلى زيادة نسبة البطالة ومعاصرة ظروف اقتصادية صعبة حيث أن هذه الجرائم تحقق الكثير من المكاسب المادية عن طريق وسائل غير شرعية، لهذا يلجأ بعض الأشخاص إلى ارتكاب هذه الجرائم للهروب من الواقع المجتمعي والرغبة في الثراء، يقوم هؤلاء المجرمين لعدم فرض عقوبات صارمة في بعض الدول مع وفرة التقنيات الرقمية التي تساعد هؤلاء المجرمين حين الرغبة في ارتكاب تلك الجرائم الإلكترونية.

3- كما توجد أسباب تتعلق بالجرائم الإلكترونية تتمثل في سرعة التنفيذ لهذه الجرائم بالإضافة إلى استمتاع هؤلاء المجرمين بتمثيل هذه الجرائم نظرًا لأن نفوسهم مريضة، التمكن من اخفاء الجريمة بالكامل وصعوبة الحصول على المجرمين لتميزهم بالذكاء الخارق وقدرتهم البالغة في التعرف على جميع الوسائل الإلكترونية الحديثة.

دوافع ارتكاب الجرائم الإلكترونية

يوجد الكثير من الدوافع التي يقوم المجرمين بتمثيلها ، لتنفيذ هذه العمليات الإجرامية من أجل الحصول علي:

1. للحصول على مكاسب مادية.
2. الرغبة في التمكن من إختراق المواقع الاباحية المحجوبة.
3. فك الشفرة للمواقع التي تحتوي على معلومات أمنية خطيرة.
4. لأغراض سياسية حيث يقومون بالتسلل إلى المعلومات السرية التي تهدد الأمن الوطني والعمل على القضاء عليها، إثبات القدرة على اختراق وتهديد الأمن القومي.
5. وجود دوافع الانتقام من أشخاص أو مؤسسات حيث يلجأ الكثير من العاملين إلى القضاء على شبكات المعلومات الخاصة بالمؤسسة التي تم الفصل مثلًا أو للعديد من الأسباب بغرض الانتقام.
6. يعمل بعض المجرمين على ارتكاب هذه الجرائم بغرض التسلية، أو نشر الكثير من الشائعات والمعلومات المغلوطة عن رجال الأعمال والأشخاص ذات المناصب العالية والمهمة في الدولة.

أنواع الجرائم الإلكترونية

يشتمل تعريف الجرائم الالكترونية على العديد من الأساليب التي تستهدف الحصول على المعلومات السرية، الاستيلاء على الأموال، سرقة البيانات، كما تشتمل هذه الجرائم على العديد من الأنواع تتمثل في:

1. جرائم إلكترونية تستهدف الأشخاص: هي جرائم تهدف إلى الاستيلاء على المعلومات الشخصية الاسم، العنوان، أيضًا للتعرف على كلمات المرور السرية الخاصة بالبريد الإلكتروني، البرامج المشفرة على الجوال، في بعض الأحيان يقوم المجرم بانتحال شخصية الضحية للقيام بأعمال منافية للآداب العامة، والتهديد للضحية لإخضاع والقيام بتنفيذ جميع الأوامر التي تطلب منه.
2. جرائم إلكترونية تستهدف الحكومات: هذا النوع من الجرائم يستهدف تدمير البنية التحتية للحكومات بالإضافة إلى القضاء على كافة البرامج والشبكات المسئولة عن الأنظمة الشبكية الخاصة بهذه المواقع الرسمية للحكومات.
3. جرائم إلكترونية تستهدف الملكية: هذا النوع من الجرائم الإلكترونية يعمل على تدمير كافة الملفات الهامة مع اختراق المعلومات السرية المتعلقة بالمؤسسات الخاصة، وكذلك

المؤسسات الحكومية والعمل على القضاء على جميع البرامج والأجهزة المسؤولة عن هذه المؤسسات.

4. جرائم الاحتيال والنصب الإلكتروني: هذه الجرائم تتمثل في عمليات النصب والاحتيال التي تتم عبر استخدام مواقع التواصل الاجتماعي حيث تستهدف الفئات العمرية المختلفة، يهدف هذا النوع إلى الاستيلاء على الأموال بدون وجه حق، كما يتمكن هؤلاء المجرمين من إرسال روابط تشتمل على برامج تجسس تخترف الأجهزة الإلكترونية بمجرد الضغط عليها، علاوة على ذلك .. يتم تنفيذ الإرهاب المتصل على الانترنت اليوم من خلال الإعلام الإجتماعى حيث تجند المنظمات الارهابية عن طريق هذه الشبكات الاجتماعية الافراد وتقوم بإرسال طلبات الصداقة وتحميل الفيديوهات واطلاق الألعاب الإلكترونية ، حيث تستخدم المنظمات الارهابية الاعلام الاجتماعى للحصول على معلومات حول الأعداء من خلال مراقبة أنشطة الجنود على الشبكات الاجتماعية ((98.Arab Media,2016,p

5. جرائم التحرش الإلكتروني: تتعدد أنواع التحرش الإلكتروني فيوجد تحرش عبر الإنترنت، تحرش عبر الجوال، تحرش عبر واتس أب، حيث يتم هذا النوع من التحرش عن طريق إرسال رسائل عبر البريد الإلكتروني أو رسائل نصية، مقاطع صوتية أو مرئية تحتوي على مدلول جنسي، تؤدي هذه الجرائم في الغالب إلى القيام بأعمال مشينة حيث تستهدف الأطفال والمراهقين والأشخاص ذات النفوس الضعيفة على وجه الخصوص.

6. جرائم الابتزاز الإلكتروني: تهدف إلى تهديد الأشخاص وابتزازهم ماديًا خوفًا من نشر المعلومات الشخصية عبر شبكة الإنترنت. يقومون باستغلال البيانات التي يسرقونها من صور ومقاطع فيديو في ابتزاز أصحاب الحسابات من المستخدمين، مقابل طلب أموال لعدم نشر تلك الخصوصيات.

الفرق بين الجرائم المعلوماتية والجرائم الإلكترونية:

الجرائم المعلوماتية : هى سلوك غير قانوني يحدث عند انتهاك الأجهزة الإلكترونية والذكية والحواسيب، التي تعتمد على الإنترنت في عملها، فيستغل المجرم شبكة الإنترنت للوصول إلى المعلومات الشخصية للأفراد، حيث أنّ هذه الوسائل تعتبر من أضخم بنوك المعلومات لدى جميع الناس في هذا الزمن، كما أنّ العديد من الأعمال والصفقات التجارية، أصبحت تنفذ عن طريق الشبكة العنكبوتية وعن بُعد؛ لذلك يجب زيادة الوعي في كل ما يخص البيانات والمعلومات المرفقة على المواقع الإلكترونية.

الجرائم الإلكترونية : جرائم ترتكب ضد أفراد أو جماعات أو مؤسسات كاملة ؛ باستخدام وسائل الاتصال الحديثة واستخدام الحاسوب ، والهدف الأساسي منها يكون ابتزاز الشخص أو تشويه سمعته ، وإلحاق الضرر به للحصول على مقابل مادي مثل النقود أو لتحقيق أهداف سياسية ، أو إفشاء أسرار أمنية تكون خاصة بالمؤسسة.
https://mawdoo3.com/

أضرار و مخاطر الجرائم الإلكترونية على المجتمع

أصبحت الجرائم الإلكترونية أحد أكبر المخاطر التي يتعرّض لها مستخدمو الإنترنت، حيث إنّ ملايين المستخدمين حول العالم تعرّضوا لسرقة بياناتهم خلال السنوات الأخيرة، وتؤكد دراسة الشمرانى (2014) ، و دراسة خالد مخلف الجنفاوى (2016) ، و دراسة منتصر محمد علام (2016) ، ودراسة ياسر عبد الفتاح القصاص ، وأيمن أحمد جلالة (2017) مخاطر الجرائم الإلكترونية على المجتمع وهى تتمثل فى :

1. نشر الفساد والمشاهد غير الأخلاقية المنافية لأخلاقيات المجتمع.
2. مشاهدة مواد تحث على الكراهية والحقد والعنف داخل المجتمع.
3. مشاهدة مواد تحث على القيام بأعمال غير قانونية داخل المجتمع.
4. الإنشغال عن تأدية الشعائر الدينية بإنتظام.
5. العمل على ضعف الهوية الثقافية للشباب
6. تعتبر وسيلة للإفراغ الجنسي.
7. الإطلاع على أفكار غريبة على المجتمع تجعل الشخص فى صراع نفسي.
8. الإنصراف عن طاعة الوالدين ومساعدة الأسرة.
9. الهروب من مواجهة المشكلات بواقعية.
10. تبادل مقاطع الفيديو والصور مع أشخاص مجهولين.
11. انتشار بعض القيم السلبية كالفردية والأنانية.
12. الإنحراف الدينى أو تغيير الدين.
13. انتهاك الخصوصية للآخرين عن طريق نشر صورهم دون موافقتهم.

(هنيدى بن عطية البشرى ،2020)
www.pandasecurity.com https://mawdoo3.com/

الفئات التي تستهدفها الجرائم الإلكترونية:

يُمكن تصنيف الجرائم الإلكترونية بناءً على الفئة المستهدفة من الهجوم كالآتي:

1) الجرائم ضدّ الأفراد: تشمل هذه الجرائم عادةً الإزعاجات والمضايقات الإلكترونية، ونشر المحتوى غير الأخلاقي، وجرائم الاحتيال على بطاقات الائتمان، وسرقة الهوية الإلكترونية، والاستغلال، والتشهير أو الإساءة على مواقع الإنترنت.
2) الجرائم على الممتلكات: تهدف هذه الهجمات للوصول لأجهزة الكمبيوتر وخوادمها وسرقة محتوياتها، حيث تُخرّب الأجهزة وتنتهك حقوق النشر والملكية.
3) الجرائم ضدّ الحكومات: تستهدف هذه الجرائم انتهاك سيادة الدول، والوصول إلى معلومات سرّية، ويُمكن أن تصل إلى شنّ الحروب و أعمال إرهابية.

www.swierlaw.com https://mawdoo3.com/

أمثلة على الجرائم الإلكترونية:

يوجد العديد من الأمثلة على الجرائم الإلكترونية التي حدثت في العالم وفي ما يأتي أشهرها:

- 2014م: متاجر التجزئة الأمريكية ، اختُرقت أنظمة نقاط البيع، وسرق المهاجمون 50 مليون بطاقة ائتمانية شخصية وحصلوا على تفاصيلها.
- 2016م ، أكبر المواقع الإلكترونية ، استُخدم في هذا الهجوم أكثر من مليون جهاز كمبيوتر متصل على الإنترنت واختُرق أغلبها بإستغلال ثغرات أمنية على البرامج، وأدّى الهجوم لإيقاف مجموعة كبيرة من أكبر المواقع على الإنترنت.
- 2017م ، مختلف مستخدمي الإنترنت أُغلقت خلال هذا الهجوم محتوى 300,000 جهاز كمبيوتر حول العالم، وطُلب من المستخدمين دفع مبالغ مالية مقابل فكّ التشفير وإتاحة وصولهم لبياناتهم مرّةً أخرى.

(Vicky Ngo-Lam, 2019)
www.exabeam.com

معاقبة الجرائم الإلكترونية في قوانين دولة مصر

أصدر مجلس النواب قوانين مختلفة لكل جريمة إلكترونية فمثلاً:

1. معاقبة المخالفين لخصوصية الآخرين بإرسال رسائل له دون رغبته أو نشر معلومات عنه بالحبس لمدة 6 أشهر وغرامة تصل إلى 100 ألف جنيه.
2. يعاقب بالحبس لمدة عامين وغرامة تصل إلى 300 ألف جنيه كل من يستخدم التكنولوجيا لربط صور أو أحاديث أو معلومات عن شخص بمحتوى ينتهك الآداب العامة أو محتوى إباحي

3. أي شخص يستخدم مواقع أو صفحات على وسائل التواصل الاجتماعي لتسهيل أداء جرائم أخرى يعاقب بالسجن لمدة عامين وغرامة قدرها 100000 دولار.
4. يعاقب بالحبس مدة ستة أشهر وبغرامة تصل إلى مائتي ألف جنيه كل من يهرب معلومات أو بيانات عن طريق امتلاك أو إدارة مواقع.
5. يعاقب كل من عطل استخدام الإنترنت أو تعمد التشويش على الشبكات بالسجن لمدة تصل إلى ستة أشهر وغرامة تصل إلى 500 ألف جنيه ، وإذا لم تسدد الغرامة تشدد إذا وقعت على شبكة مملوكة للدولة أو جهة حكومية وبغرامة تصل إلى مليون جنيه.

https://www.law-house.net Access in 16/8/2022

دور التنظيمات الاجتماعية فى مواجهة الجرائم الإلكترونية:

تؤكد دراسة منصور بن عبد الرحمن بن عساكر (2012) ، ودراسة منى الجراحى (2015) ، ودراسة خالد مخلف الجنفاوى (2016) ، و دراسة منتصر محمد علام (2016) ، ودراسة ياسر عبد الفتاح القصاص ، وأيمن أحمد جلالة (2017) على أهمية دور التنظيمات الإجتماعية فى مواجهة مخاطر الجرائم الإلكترونية على المجتمع وتحدياتها ومعالجتها.

أولاً : دور الجامعة فى مواجهة الجرائم الإلكترونية من وجهة نظر الشباب الجامعى وهى:

1. توعية الشباب بأحدث برامج الحماية للوقاية من الجرائم الإلكترونية.
2. نشر الثقافة المعلوماتية بين الشباب الجامعى من خلال موقع الجامعة.
3. الشراكة مع الجهات المجتمعية المتخصصة للتوعية بمخاطر الجرائم الإلكترونية.
4. عقد اللقاءات وورش العمل للوقوف على كل جديد فى مجال الجرائم الإلكترونية.
5. إلقاء المحاضرات بصفة دورية للتوعية بخطورة الجرائم الإلكترونية.
6. شغل أوقات فراغ الشباب الجامعى بالعديد من الأنشطة و البرامج.

ثانياً: دور الأسرة فى مواجهة الجرائم الإلكترونية:

1. ترشيد الأسر لوقت بقاء الأبناء على شبكات الإنترنت.
2. تنفيذ برامج توعوية تثقيفية للوالدين عن كيفية التعامل مع الجرائم الإلكترونية.
3. تنفيذ برامج توعوية تثقيفية لنشر الوعى بين الأسر وأبنائها حول وسائل حماية المعلومات الشخصية.
4. عدم ترك الأبناء لفترة طويلة داخل غرفهم خلف أبواب مغلقة دون رقابة.
5. تعديل الإعتقادات الخاطئة لدى الأسر المرتبطة بشراء كل جديد مع عدم مراعاة إيجابياته وسلبياته.

ثالثاً : دور المؤسسات الإجتماعية الأخرى فى مواجهة الجرائم الإلكترونية :

1. التنسيق مع مراكز الحماية الإجتماعية للقيام بإتخاذ الإجراءات القانونية لتوفير الحماية الإجتماعية والنفسية للشباب الذين أصبحوا فريسة الجرائم الإلكترونية.
2. قيام الجهات المتخصصة بتوضيح أهم برامج الحماية للشبكات للوقاية من الجرائم الإلكترونية.
3. تدعيم القوانين والتشريعات التى تحرم ارتكاب الجرائم الإلكترونية.
4. إنشاء مراكز متخصصة للتعامل مع الجرائم الإلكترونية.
5. إهتمام وسائل الإعلام المقروءة والمسموعة والمشاهدة بالجرائم الإلكترونية وكيفية التعامل معها والحماية منها .
6. تكوين لجان وطنية تضم خبراء من العلوم الإجتماعية والنفسية لدراسة الجرائم الإلكترونية ووضع سياسات للتعامل معها ومع آثارها.
7. تمويل ودعم البحوث والدراسات التى تولى إهتماماً كبيراً للجرائم الإلكترونية وكيفية التعامل معها.
8. دعم وتشجيع الدعاة فى المؤسسات الدينية والدعوية للتوعية بخطورة الجرائم الإلكترونية.
9. قيام الجهات المتخصصة بحجب المواقع التى تبث القيم والمعتقدات السلبية تجاه المجتمع وثقافته.
10. عقد العديد من اللقاءات المشتركة بين ممثلى الوزارات المختلفة للتوعية بمخاطر الجرائم الإلكترونية ووسائل الحماية منها .

الآليات المقترحة للتعامل مع هذه الجرائم الإلكترونية

1. يجب على الدولة إعلام جميع المواطنين عن تعريف الجرائم الالكترونية .
1. العمل على زيادة الوعي بأخطار القيام بهذه الجرائم.
2. التشديد على جميع وسائل الإعلام والشبكات الإلكترونية بنشر إعلانات توعية للمواطنين.
3. مساعدة المواطنين على التعرف على طرق مكافحة الجرائم الإلكترونية وتعريفهم على الإجراءات التي يجب على الضحية التي تعرضت لمثل هذه القيام بها.
4. الحرص على عدم نشر معلومات شخصية أو صور على مواقع التواصل الاجتماعي.
5. حفظ المعلومات الهامة على أجهزة غير متصلة بالإنترنت مثل استخدام الأقراص المدمجة.
6. التحقق من مصداقية الموقع الذي تضع فيه كلمات المرور الخاصة بالبريد الإلكتروني أو الرقم السري الخاص ببطاقات الائتمان والبطاقات المصرفية.

7. تجنب فتح روابط من أشخاص مجهولين لأنها تحتوي في الغالب على برامج تجسس تخترق الجهاز الخاص بك وتسلل إلى جميع المعلومات على الجهاز.
8. عدم استخدام برامج غير معلومة المصدر.
9. عدم الضغط على الإعلانات التي تظهر أثناء استخدام بعض المواقع على شبكة الإنترنت.
10. القيام بتثبيت برامج مكافحة الفيروسات على الجوال وجهاز الكمبيوتر الخاص بك بالإضافة إلى تثبيت برامج حفظ المعلومات السرية على الأجهزة الإلكترونية.
11. قيام الدولة باتخاذ إجراءات قاسية تجاه هؤلاء المجرمين مع تطوير الطرق المسئولة عن تتبع هؤلاء المجرمين.
12. كما يجب على الدولة أن تفرض عقوبات صارمة لردع هؤلاء المجرمين ومنعهم من القيام بمثل هذه الجرائم والتشهير بهم في الإعلانات والصحف العامة للحد من هذه الجرائم المشينة.

ويؤكد معلوى بن عبد الله الشهرانى (2019) على :

1. تعزيز واحترام القيم الدينية والأخلاقية والاجتماعية والتربوية والسلوكية من قبل المواطنين من خلال المنصات .
2. تعزيز الأنشطة والبرامج الفردية والجماعية والجماعية والمجتمعية والمؤسسية التى تهدف إلى عدم استقلال الشباب.
3. المناقشة الجماعية عبر غرف الدردشة وهى من أساليب وقاية الشباب من الآثار السلبية للجرائم الإلكترونية ومساعدة الشباب على تعديل أفكارهم الخاطئة عن طريق الحوار الفكرى الإلكترونى.
4. الندوة عبر المنتديات الإلكترونية : التى تهدف إلى تعديل وتصحيح الأفكار الخاطئة لدى الشباب المتواصل أو المتردد عبر الشبكات الإجتماعية للحد منها.
5. الأنشطة المعرفية الإلكترونية : التى تساعد على تصحيح الأفكار والمعارف الخاظئة لدى الشباب الجامعى المتواصل عبر الشبكات الإجتماعية ، وتوسيع المدارك الثقافية لديهم للحد من هذه الجرائم.
6. نشر الفكر الوسطى عبر سبكات التواصل الإجتماعى من خلال وسائل فعالة تهاجم مواقع الجماعات الإرهابية ، ومواجهة الفكر الضال الذى ينشر عبر الشبكات الإجتماعية للحد من هذه الجرائم.

الحماية من الجرائم الإلكترونية

فيما يأتي بعض من الإجراءات التي يُوصى بإتباعها لحماية المُستخدم من الجرائم الإلكترونية :

1. حماية بيانات المستخدم بكلمة مرور قوية، ولا بد أن تكون هذه الكلمة سهل على المُستخدم تذكرها وصعب على الآخرين التنبؤ بها.
2. عدم السماح للمستخدمين الآخرين بفتح أي مواقع تم التسجيل بها باستخدام كلمة المرور، دون وجود المستخدم الرئيسي أثناء فتح هذه المواقع.
3. حفظ البيانات المهمة على جهاز كمبيوتر غير مُتصل بالإنترنت.
4. حفظ نسخة من بيانات المستخدم على أقراص تخزين خارجية.
5. عدم الدخول إلى المواقع الخطرة وغير الموثوقة أو المواقع التي تحتوي على محتوى غير لائق.
6. لا تعطي أي معلومات شخصية لأي شخص ولا تملأ الاستبيانات.
7. مراقبة حركة الأموال المرسلة من وإلى حسابك المصرفي.

(Tim Papker, 2012)
https://mawdoo3.com/

كيفية الإبلاغ عن الجرائم الإلكترونية

في البدايه يتم من خلال بلاغ يتم تقديمه في أي قسم من أقسام الشرطه مرفق معه أي مستندات أو وسائل اثبات ليتم إحالته للنيابه المختصه بالتحقيق فيه إلا أنه يتم الآن الابلاغ في مقر شرطه مكافحه الجرائم الإلكترونيه و التي تعد جهاز كبير تابع لوزاره الداخليه , و التي تضم العديد من المهندسين و الفنيين القادرين علي تتبع تلك الجرائم و التاكد من حدوثها من عدمه .

https://ujeeb.com Access in 16/8/2022

توصيات البحث

فى ضوء النتائج التى توصل إليها البحث الحالي توصى الباحثة بالآتى :

1. ضرورة توعية الشباب بالإستخدام الأمثل للمواقع الإلكترونية لعدم استغلال عواطفهم لأفكار ضالة ومضللة ، مثل الإنحراف الدينى ، ونشر مقاطع للتنصير والإلحاد والإنحراف الأخلاقى (التشجيع على التدخين، المساعدة على تجارة المخدرات وتهريبها والانحراف الأسرى).
2. ضرورة الاهتمام بوضع برمجيات تمنع نشر الألفاظ المسيئة والضبط القانونى والأمنى (التوعية الأمنية بمخاطر المواقع المتطرفة) و الضبط الاجتماعى (توعية الشباب بالحفاظ على الضرورات الخمس).
3. ضرورة تشجيع الشباب على الإعتدال والتدين وحسن الجوار واحترام الآخر إلكترونياً.
4. تمكين الشباب من ممارسة الحوار البناء وأساليب التواصل الإلكترونى مع الآخرين .

5. تحذير الشباب من اعتناق الإتجاهات الفكرية المتطرفة عبر الموافع المتطرفة .
6. يستلزم الحد من الجرائم الالكترونية رفع مستوى التوعية لدى المواطن من خلال اللقاءات والندوات عبر المواقع الإلكترونية .
7. الحرص على وضع آليات لضبط استخدام المواقع الإلكترونية للوقاية من الجرائم الإلكترونية.
8. ضرورة الاهتمام بأوقات فراغ الشباب وقضائها فى أمور ايجابية مفيدة.
9. دعوة المنظمات المجتمعية من مدارس وجامعات من خلال وحدات الأنشطة الطلابية بإجراء مزيد من الدراسات عن مواقع شبكات التواصل الإجتماعى وآثارها التربوية والاجتماعية المختلفة حتى تكون النتائج قابلة للتعميم.
10. ضرورة حجب المواقع الضارة التى تدعو إلى الفساد والشر والإرهاب والعدوان والإعتداءعلى الآخرين بغير حق.
11. ضرورة إدخال مادة دراسية فى الكليات والمدارس للقضاءعلى الجرائم الإلكترونية وعقوبتها وأمن المعلومات.

المراجع

أكرم عبد الرازق المشهدانى (2015). " الجرائم الإلكترونية : التحديات والمعالجة" ، مجلة الدراسات المالية والمصرفية ، الأكاديمية العربية للعلوم المالية والمصرفية ، مركز البحوث المالية والمصرفية ، 23(1) ، 23-28.

حازم محمد مطر (2015). " القاموس الشامل لمصطلحات العلوم الاجتماعية والانسانية " ، دار الحامد للنشر والتوزيع، الأردن .

خالد إبراهيم ممدوح (2009). " الجرائم المعلوماتية "، القاهرة، دار الفكر العربي.

خالد مخلف الجنفاوى (2016). " الجرائم الإلكترونية وطرق معالجتها من وجهة نظر أعضاء هيئة التدريس فى أكاديمية سعد العبد الله للعلوم الأمنية بالكويت" ، مجلة الخدمة الاجتماعية ، الجمعية المصرية للأخصائيين الاجتماعيين، القاهرة ، ع(56) ، ج(2) ، 371-399.

عبد الحليم بوفرين (2019) . " أثر الجريمة الإلكترونية على الحياة الخاصة للأفراد" ، المجلة الأمريكية للبحوث القانونية والسياسية ، جامعة عمار تليجى الأغواط ، كلية الحقوق، الجزائر ، 3(2) ، 62-71.

فاطمة الزهراء دريم (2017) . " دور الأجهزة الإعلامية فى مكافحة الجريمة الإلكترونية" ، مجلة الرواق للدراسات الإجتماعية والإنسانية ، المركز الجامعى أحمد زبابة غليزان ، مخبر الدراسات الاجتماعية والنفسية والأنثربوبوجية ، ع7، 84-94.

محمد أمين الشوابكة (2011). جرائم الحاسوب والانترنت ، الجريمة المعلوماتية، عمان ، دار الثقافة العربية للنشر والتوزيع .

معلوى بن عبد الله حسين الشهرانى (2019). " تصور مقترح لوقاية الشباب الجامعى من مخاطر الإرهاب السيبرانى" مجلة المشكاة للعلوم الإنسانية والإجتماعية ، جامعة العلوم الإسلامية العالمية ، عمادة البحث العلمى ، مج(6)، ع(2) ، 483-527.

منتصر محمد علام (2016) . " دور الأنظمة والتشريعات فى ضبط استخدام شبكات التواصل الاجتماعى من منظور الخدمة الاجتماعية " ، مجلة الخدمة الاجتماعية ، الجمعية المصرية للأخصائيين الاجتماعيين، القاهرة ، ع(56) ، 423-468.

منصور بن عبد الرحمن بن عساكر (2012). " استطلاع آراء الشباب السعودى حول دور المؤسسات الإجتماعية فى التبصير بالجرائم الإلكترونية" ، مجلة دراسات وبحوث ، العدد السادس ، جامعة الخليفة ، الجزائر.

منى الجراحى (2015). " دور الجامعات السعودية فى تنمية وعى الشباب بخطورة الجرائم المعلوماتية لدعم قضايا مكافحة الإرهاب الإلكترونى ، مؤتمر الإرهاب الإلكترونى ، جامعة الإمام محمد بن سعود الإسلامية ، الرياض.

ناعوس بن يحيى الطاهر (2015) . " مكافحة الإرهاب الإلكتروني ضرورة بشرية و فريضة شرعية" ، الألوكة.

هنيدى بن عطية بن عبد المعطى (2020) . " الجرائم الإلكترونية وكيفية التعامل معها من وجهة نظر الشباب الجامعيين" ، جامعة طنطا ، كلية الآداب ، (38) ، 633-664.

ياسر عبد الفتاح القصاص ، وأيمن أحمد جلالة (2017). " آليات تفعيل الشراكة بين الجامعات والمدارس للحد من مخاطر تعرض الطلاب للجرائم المعلوماتية " ، مجلة الخدمة الاجتماعية ، الجمعية المصرية للأخصائيين الاجتماعيين، القاهرة ، ع(57) ، ج(1).

سايبرون ، "ما هي الجرائم المعلوماتية "، اطّلع عليه بتاريخ 2022/8/14،
مؤسسة دعائم تقنية للحاسب الآلي، "ما هي الجرائم الإلكترونية "، الاطلاع عليه بتاريخ 2022/8/5.

Arab Media, (2016).More information than you ever wanted: Does face book Bring out the Green –Eyed Monster of jealousy? Cyber Psychology &Behavior, Vol. (12), No.4.

Al-saggaf,Yeslam,(2011).Saudi Females on face book An Ethnographic Study, **International Journal of Emerging Technologies& Society**.Vol.(9).

Tim Papker, (2012). "6 Ways to Protect Yourself against Cybercrime", www.investopedia.com, Retrieved 1-2-2019. Edited. Access in 16/8/2022

"What Are the Three Types of Cyber Crimes?" www.swierlaw.com, Retrieved 19-2-2021. Edited Access in 16/8/2022

Vicky Ngo-Lam, (2019). "Cyber Crime: Types, Examples, and What Your Business Can Do"، www.exabeam.com, Retrieved 13-2-2021. Edited Access in 16/8/2022.

security .com, "Types of Cybercrime", Retrieved 13-2-2021. www.panda Edited. Access in 16/8/2022.

https://mawdoo3.com/

https://ujeeb.com Access in 16/8/2022