مدعوم مـن

Funded by:

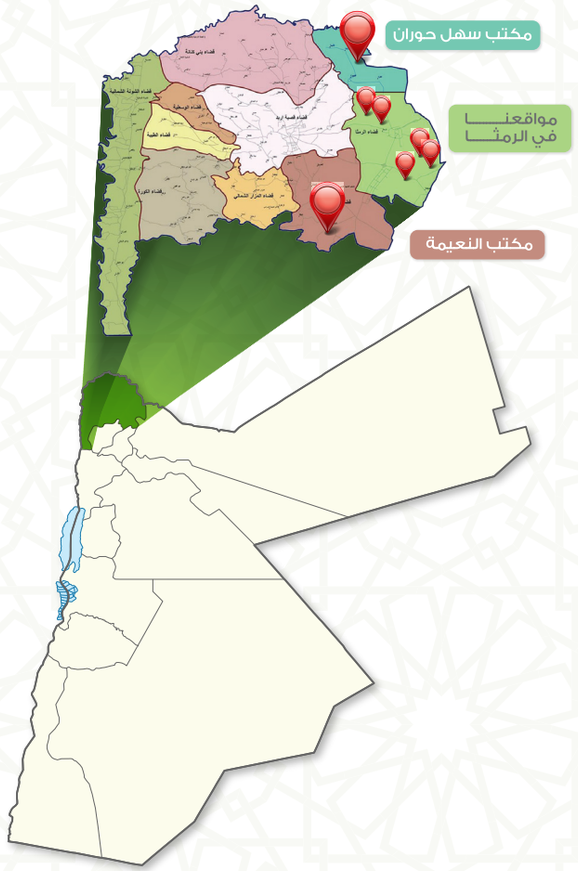
SIREN ASSOCIATES

جمعية التكافل الخيرية
المملكة الأردنية الهاشمية - الرمثا

دليلك للحماية من الجرائم الإلكترونية

100 سـؤال وجـواب

مقار جمعية التكافل الخيرية في محافظة إربد



مشاريعنا عطاء بلا حدود

إغاثيـــة - اجتماعيـــة - توعويـــة

+962 2 738 2300
+962 2 738 1300
+962 77 777 4922
+962 77 777 4922
@Altkaful
Altkafulmedia
Altkafulmedia
Altkafulpage
info@altkaful.net
www.altkaful.net

المقدمة

انطلاقاً من إدراكنا لأهمية مواكبة تسارع التغيرات التكنولوجية ومستجدات العصر وتطوراته، واستجابة للحاجة الملحة لوجود دليل إرشادي يساهم في حماية أفراد المجتمع من خطر الجرائم الإلكترونية؛ خاصة مع زيادة نسبة هذا النوع من الجرائم خلال الأعوام الأخيرة مع اتساع مساحة الفضاء الإلكتروني وزيادة عدد المستخدمين لوسائل التواصل الإلكترونية، وترجمةً لنهج ورؤى جلالة الملك عبدالله الثاني ابن الحسين –حفظه الله– بأهمية التعاون مع الأجهزة الأمنية لحفظ الأمن والأمان وترسيخ سيادة القانون جاء هذا الدليل الإرشادي كجزء من مبادرة بعنوان "مكافحة الجرائم الإلكترونية" نفّذتها جمعية التكافل الخيرية بالتعاون مع منظمة سايرن وبدعم مادي من البرنامج الأوروبي الإقليمي للتنمية والحماية لدعم لبنان والأردن والعراق **RDPP II** وهو مبادرة أوروبية مشتركة بدعم من جمهورية التشيك، الدنمارك،الاتحاد الأوروبي، ايرلندا وسويسرا.

يمثل محتوى هذا الدليل آراء جمعية التكافل الخيرية ومنظمة سايرن ولا يعكس بالضرورة سياسات أو آراء البرنامج الأوروبي الإقليمي للتنمية والحماية أو الجهات المانحة له.

1- ما هي الجريمة الإلكترونية؟

- كل فعل جرّمته القوانين من شأنه الاعتداء على الأحوال المادية أو/و المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات.
- أو كل فعل أو امتناع عن فعل باستخدام وسيلة تكنولوجية يعاقب عليه القانون بنص.

2- ما هي أنواع الجرائم الإلكترونية الرئيسية؟

- الجرائم ضد الأفراد: وهي التي تتعلق بالجرائم الشخصية على الإنترنت، كسرقة البريد الإلكتروني وغيره.
- الجرائم ضد الملكية: وهي التي تهدف إلى الوصول إلى أجهزة مملوكة لشركات أو حكومات أو بنوك أو حتى ممتلكات شخصية.
- الجرائم ضد الحكومات: وهي تعنى بمهاجمة مواقع المؤسسات الحكومية وأنظمة الشبكات، وغالبا ما يكون هدفها سياسي.

3- ما مدى خطورة الجريمة الإلكترونية؟

تكمن خطورة بعض الجرائم الإلكترونية بشكل عام في أنها جرائم عابرة للحدود، وبالتالي يكون من الصعب تتبعها، وكذلك اكتشافها وإثبات الجرم على المجرم، وذلك لعدم وجود أثر ملموس يمكن تقصيه والاستفادة منه.

4- من هم أكثر ضحايا الجرائم الالكترونية؟

تقريبا 80% من ضحايا الجرائم الإلكترونية هم من الفتيات أو النساء.

5- ما هي الفئة العمرية الأكثر تعرضا للجريمة الإلكترونية؟

الفئة العمرية الأكثر عرضة للجرائم الإلكترونية هي ما بين 14 سنة إلى 17 سنة.

6- ما هي الجرائم الإلكترونية الأكثر شيوعا في الأردن؟

الجريمة الإلكترونية الأكثر انتشارا هي جريمة الإبتزاز.

7- ما هي الجرائم الإلكترونية المبنية على النوع الاجتماعي؟

هي الجرائم الإلكترونية بمختلف أنواعها التي تكون قائمة على الفروق بين الذكر والأنثى.

8- هل الجرائم الإلكترونية المبنية على النوع الاجتماعي شائعة في الأردن؟

الجرائم الإلكترونية المبنية على النوع الاجتماعي متواجدة بشكل كبير في الأردن، وغالب من يتعرض لها هم الإناث.

9- ما معدل زيادة نسبة الجرائم الإلكترونية وقضاياها الأعوام الأخيرة؟

ارتفعت الجرائم الإلكترونية حتى عام 2021 بمقدار ألفي قضية مقارنة مع عامي 2019 و 2020.

10- ما هي العوامل والأسباب التي تؤدي إلى ارتكاب الجريمة الالكترونية؟

هناك عدة أسباب تستدعي بالشخص القيام بالجريمة الإلكترونية، ومنها:

- الرغبة في التعلم وجمع المعلومات عن طريق اختراق المواقع الممنوعة، أو المحمية.
- الرغبة في تحقيق مكاسب مالية، وتعتبر من أبرز الدوافع للقيام بالجريمة.
- دافع الانبهار بالتقنية والإثارة والمتعة، وغالبًا ما يكون دافعا لفئة صغار السن الذين يقضون أوقاتا طويلة أمام الشاشات.
- أسباب ودوافع شخصية كالحقد والكراهية تجاه أشخاص معينين بهدف إلحاق الضرر بالطرف الآخر.

11- ما هي أسباب الجرائم الإلكترونية على المستوى المجتمعي؟

- التحضر؛ وذلك من خلال لجوء الأشخاص غير المتمكنين الذين ينتقلون من الريف إلى المدن، إلى القيام بالاستثمار بالجرائم الإلكترونية.
- البطالة؛ ويكون ذلك من خلال استغلال الشباب العاطلين عن العمل قدراتهم في الكسب من الجرائم الإلكترونية.
- الضغوط العامة؛ كالفقر والظروف الاقتصادية الصعبة خاصة على فئة الشباب.
- البحث عن الثراء؛ وذلك أن الكسب من الجرائم الإلكترونية أسرع وأسهل وقليل الخطورة.
- ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية.

12- ما هي جرائم الملكية الفكرية الإلكترونية؟

هي انتهاك الملكية الفكرية عن طريق شبكة الإنترنت، وتعتبر جرائم الملكية الفكرية تهديدا كبيرا للشركات والمستهلكين، وتكون على شكل القرصنة والتقليد على حد سواء.

13- هل جرائم سرقة حقوق الملكية الفكرية عن طريق نسخ البرامج الأصلية وتسويقها واستخدامها دون إذن مسبق تعد جرائم إلكترونية؟

نعم، تعتبر من الجرائم الإلكترونية، وذلك حسب المادة ٤ من قانون الجرائم الإلكترونية الأردني، حيث "يعاقب كل من استخدم برنامجا عن طريق الشبكة المعلوماتية لسرقة أو نسخ أو تغيير أو نقل بيانات أو معلومات من دون تصريح."

14- هل يعتبر التعدي على شخصية عامة على وسائل التواصل الاجتماعي جريمة إلكترونية؟

يُعتبر التعدي على الشخصيات العامة من ضمن الجرائم الإلكترونية التي وردت في قانون الجرائم الإلكترونية الأردني فيما يتعلق بخصوصية الأفراد، بالإضافة إلى التعدي على البيانات الشخصية المتعلقة بالحياة الخاصة.

15- هل يعتبر تداول المادة الإباحية جريمة إلكترونية؟

إن نشر المواد الإباحية وتداولها عبر الوسائل الإلكترونية المختلفة جريمة إلكترونية، حيث تُعتبر من الجرائم الجنسية والإخلال بالآداب العامة، ويُعاقب عليها القانون الأردني الخاص بالجرائم الإلكترونية في المادتين ٩ و ١٠، وهذا يتضمن كل ما هو مسموع أو مقروء أو مرئي يحتوي على أعمال إباحية فيها استغلال جنسي أو ترويج للدعارة.

16- هل يعتبر عدم وجود دليل على مرتكب الجريمة نقطة ضعف لإثبات الجريمة الإلكترونية؟

يعتبر عدم وجود دليل على مرتكب الجريمة نقطة ضعف في إثبات الجريمة؛ وذلك لأن ضبط الجريمة يعتمد على جمع الأدلة الموجودة، وتكون وسائل إثبات الأدلة عن طريق المعاينة، والخبرة، والتفتيش، وضبط الأشياء المتعلقة بالجريمة، ولا يتخلل ذلك أي تعدي على حقوق الأفراد وحرياتهم.

17- هل بث الإشاعات عبر وسائل التواصل الاجتماعي جريمة إلكترونية تستحق العقوبة؟

تُعَدُّ الشائعات التي يقوم الأفراد بنشرها على مواقع التواصل الاجتماعي جرائم إلكترونية يعاقب عليها القانون، وذلك لكونها تساهم في تعكير صفو السِلم والأمان المجتمعي.

18- ما هي الجرائم التي يمكن اعتبارها جرائم ضد الحكومة؟

جرائم مهاجمة المواقع الرسمية، وأنظمة الشبكات الحكومية، والهجمات الإرهابية على شبكات الإنترنت، والتي يكون الهدف منها الإضرار بالبنى التحتية للدول وتدمير الخدمات، ويكون ذلك لأسباب سياسية بشكل رئيسي.

19- ما هو التصيد الصوتي، وهل يعتبر جريمة إلكترونية؟

يعتبر التصيد الصوتي أحد الأساليب الاحتيالية الإلكترونية التي تهدف إلى خداع الضحية، وذلك عن طريق جعله يكشف عن معلوماته الشخصية من خلال مكالمة هاتفية صوتية، وتبدأ هذه العملية بتوجيه مكالمات آلية إلى عدد من الأرقام العشوائية، وإيهام الضحية بأن الاتصال من جهات رسمية ومهمة، وبالتالي يقتنع بها ومن ثم يقوم بإعطائهم المعلومات الخاصة به، كما يمكن أن يكون من خلال إرسال بعض البرمجيات الضارة التي تجبر الضحية على التحدث مع رقم معين على أنه جهة رسمية، ولأن التصيد الصوتي قائم على الاحتيال والغش فإنه يمكن اعتباره جريمة إلكترونية.

20- هل يُعدُّ التحرش جريمة إلكترونية؟

يُعدُّ التحرش الإلكتروني من صور الجرائم الإلكترونية، ويُقصد به إلحاق الأذى أو المضايقة من الذكور إلى الإناث أو العكس باستخدام الوسائل الإلكترونية كالمراسلة والمحادثة باستخدام الهاتف وغيرها.

21- ما هو الاحتيال عبر الجريمة الإلكترونية؟

الاحتيال الإلكتروني يقع على مستخدمي الشبكات المعلوماتية والوسائل الإلكترونية للاستيلاء على أموال الأفراد وتبديدها، والاحتيال هو فعل خداع يقوم به المحتال ليجبر الضحية على تحويل المال له، بشكل لا يمكن أن يقبل به لو كان على أرض الواقع.



22- ما هو انتحال الهوية وهل يعد جريمة إلكترونية؟

إن جريمة انتحال الهوية أو الشخصية، هي جريمة إلكترونية حديثة وشاعت في الأوساط التجارية، ويكون ذلك الانتحال بطريقة غير شرعية بهدف الاستفادة من مكانة صاحب الهوية أو لإخفاء شخصية مجرمة لتسهيل ارتكابها جرائم أخرى.

23- ما هي الروبوتات في الجريمة الإلكترونية؟

تعد الروبوتات واحدة من أكثر الأساليب تعقيدًا في عالم الجريمة الإلكترونية التي يواجهها الإنترنت اليوم، وتكتسب الروبوتات اسمها الفريد نيابة عن مجرمي الإنترنت من خلال أداء مجموعة متنوعة من المهام الآلية. وتؤدي دورا هاما؛ خاصة في هجوم 'رفض الخدمة' على الإنترنت.

24- ما هي القنوات المختلفة التي يستخدمها مرتكبي الجرائم الإلكترونية؟

إن شبكة الإنترنت هي ما يتم عليها أغلب الجرائم الإلكترونية، فإما أن تكون هي الهدف من الجريمة كالدخول إلى أنظمة معلومات غير مصرّح بها، أو قد تكون هي الوسيلة التي يتم من خلالها مثلًا، الاستيلاء على الأموال أو التزوير أوالاحتيال. ومن الممكن أن تكون وسائل التواصل الإجتماعي هي الأداة كذلك التي يتم من خلالها القيام بالجرائم الإلكترونية.

25- ما هو التنمر الإلكتروني ؟ وما هي بعض الأمثلة عليه؟

هو القيام بفعل التنمر باستخدام الوسائل التكنولوجية المختلفة كوسائل التواصل الاجتماعي، ومنصات الدردشة، ومنصات الألعاب الإلكترونية، ويهدف المتنمر من قيامه بذلك إلى إيذاء الأشخاص أو اخافتهم أو إحراجهم، وما إلى ذلك.

ومن الأمثلة عليه:

- نشر الشائعات عن نشر صور متعلقة بشخص ما على وسائل التواصل الاجتماعي.
- إرسال رسائل تحمل أذى وعنف وتهديد إلى أشخاص من خلال منصات الدردشة.
- إرسال رسائل سيئة من حسابات وهمية فيها انتحال للشخصية نيابة عن أشخاص آخرين.

26- ما هـو التحرش الإلكتروني ؟ وما هي بعض الأمثلة عليه؟

يعـرّف التحـرش الإلكتروني على أنه القيام بأي عمل جنسي غير مرغوب به على أي منصة إلكترونية خاصة أو عامة، ويكون من خلال الصور، الفيديوهات، المنشورات، والرسائل، وذلك ما يجعل الفرد يشعر بالتهديد، الاستغلال، الكره، الإذلال، أو التحيّز والتمييز الجنسي ضده.

ومن الأمثلة عليه:

- مشاركة مقاطع الفيديو والصور الحميمية بطريقة غير توافقية.
- الاستغلال والإكراه والتهديد.
- التنمر الجنسي.

27- ما هو الابتزاز الإلكتروني؟

هو استخدام المجرم الوسائل الإلكترونية المختلفة لابتزاز وتهديد الطرف الآخر لإجباره على القيام بأفعال أو الامتناع عن فعلها.

28- ما هو انتزاع الفدية؟

انتزاع الفدية هي تسمية تطلق على نوع من الفيروسات أو البرامج الضارة التي تستهدف بيانات الضحية؛ فتقوم بتشفيرها، ويتطلب من الضحية دفع فدية ليتم فك التشفير والإفراج عن البيانات، وإذا تخلّف الضحية عن دفع الفدية فإن الجاني يهدد بمسح البيانات، أو زيادة قيمة الفدية.

29- ما هي أشكال الابتزاز الالكتروني؟

يوجد أشكال وأنواع مختلفة من الابتزاز، فمنها المالي، العاطفي، الجنسي، والسياسي، والابتزاز الإلكتروني الذي يكون بالصور، أو الابتزاز بالفيديوهات.

30- ما هي أسباب الابتزاز الإلكتروني؟

إن القيام بالابتزاز يرجع لأسباب منها ما يكون مادي تدفع بالمجرم القيام به لكسب المال من الضحية، ومنها ما يكون انتقامي أو جنسي أو سياسي، وكل

ذلك يؤدي إلى الإضرار بالضحية نتيجة التعدي على خصوصياته، واستخدامها كمادة للابتزاز.

31- ما هي أضرار استخدام مواقع التواصل الاجتماعي؟

يوجد أضرار عديدة لاستخدام مواقع التواصل الاجتماعي، ومنها:

- تقلل من مهارات التفاعل والتواصل الشخصية على أرض الواقع بالإضافة إلى إضعاف العلاقات الاجتماعية.
- إضاعة الوقت لوجود كم هائل من المواد الترفيهية الجاذبة.
- قضاء وقت طويل على مواقع التواصل قد يسبب الإدمان عليها، مما يجعل تركها صعبا.
- ضياع هوية وثقافة الأفراد واستبدالها بالهوية العالمية.
- انعدام الخصوصية بجعل كل المعلومات متاحة عليها.
- هشاشة تكوين الصداقات.
- انتحال الشخصيات يكون بطريقة أسهل على مواقع التواصل الاجتماعي.
- استغلال هذه المواقع لأغراض يُقصد بها الإضرار والإيذاء.

32- ما هي وحدة مكافحة الجرائم الإلكترونية؟

نتيجة لانتشار التكنولوجيا مؤخراً واستخدام الهواتف الذكية وكثرة المواقع الالكترونية أيضا أدى إلى انتشار نوع جديد من الجرائم هو الجرائم الالكترونية التي تعد من الجرائم الحديثة، لذلك لا بد من أن يكون هناك تشريعات جديدة تفرض عقوبات على هذه الجرائم الحديثة، فالجريمة الالكترونية هي عبارة عن أي نشاط الكتروني يتم بطرق غير مشروعة أثناء التعامل بهذا النشاط بين الناس. وقد كافحت المملكة الأردنية الهاشمية الجرائم المعلوماتية وأحدثت مديرية الأمن العام في إدارة البحث الجنائي عام 2008م "قسم الجرائم الالكترونية"، كما قامت بتطويره في العام 2015م وذلك تحت مسمى "وحدة مكافحة الجرائم الالكترونية"، و تقدم وحدة مكافحة الجريمة الالكترونية في الأردن جهداً كبيراً للتوعية المجتمعية حول مخاطر هذه الجرائم سواء على المواطنين أو على المجتمع، كما تعمل بالمشاركة مع الشركات والمؤسسات الدولية والمحلية بالإضافة أيضا إلى المؤسسات الخاصة والمصرفية والمالية وشركات الاتصالات ومؤسسات المجتمع المدني لتحقيق الهدف الرئيسي لها وهو مكافحة الجرائم الالكترونية.

33- ما هي الخطوات القانونية التي يجب إتباعها للقيام برفع قضية على مرتكب الجريمة الإلكترونية؟

بخصوص رفع الدعوى في هذه الأحوال فإنه يتم عن طريق تقديم بلاغ مباشر للشرطة يتم فيه شرح ما وقع من أفعال مخالفة للنظام وما لدى الشاكي من بيانات. وعلى إثره تقوم الشرطة بالتحقيق في الواقعة وإعداد محضر بها ومن ثم إرسالها إلى هيئة التحقيق والادعاء العام التي تباشر التحقيق لتكييف الواقعة وإعطائها الوصف المقرر لها بالنظام وبناء عليه توجيه الاتهام لإعداد لائحة اتهام ودعوى عامة تحيلها للمحكمة الجزائية للنظر والحكم فيها حسب الشرع والنظام.

34- ما هي معوقات إثبات الجريمة الإلكترونية؟

أ- اختفاء آثار الجريمة، وغياب الدليل المرئي، لأن الجناة في الجرائم الإلكترونية يتمتعون بقدرة فائقة على إخفاء أي آثار مادية ملموسة على جرائمهم.

ب صعوبة الوصول إلى الدليل، للإحاطة بوسائل الحماية الفنية مثل: كلمات السر التي تمنع الوصول إليه.

ج- سهولة محو وتدمير الدليل في زمن قصير جدا من قبل الجاني.

د- ضخامة حجم المعلومات التي يجب فحصها واحتمال خروجها عن نطاق إقليم الدولة.

هـ- الجناة في الغالب لا يستخدمون في دخولهم على شبكة الإنترنت أجهزتهم، بل يعتمدون على مقاهي الإنترنت المنتشرة في الدولة، ولا يمكن معرفة مستخدميها.

و- أغلب البيانات والمعلومات المتداولة عبر الحاسب الآلي هي رموز مخزنة على وسائط ممغنطة، لا يمكن الوصول إليها إلا عن طريق الحاسب الآلي، من قبل أشخاص مؤهلين لذلك.

35- هل العاملون في وحدة مكافحة الجرائم الإلكترونية أشخاص مؤهلون للتعامل مع قضايا الجرائم الإلكترونية؟

إن وحدة مكافحة الجرائم الالكترونية في الأردن من الوحدات المميزة والمدربة على التعامل مع كافة الجرائم الالكترونية بشكل عام، حيث لها خبرة تقنية طويلة في التعامل ومعالجة القضايا الإلكترونية في الأردن، والسيطرة عليها، فهي تعالج قضايا الابتزاز الالكتروني وقضايا النصب والاحتيال والسب والتشهير والقضايا التي تتعلق بتقنية المعلومات وأي قضية الكترونية أخرى. وهناك شرطة

إلكترونية تابعة لوحدة مكافحة الجرائم الالكترونية في الأردن تعمل على التعامل مع الإبلاغ والشكوى المقدمة بكل سرية مع عدم الإفصاح عن هوية المشتكي، فعلى سبيل المثل، تقوم بتتبع الرسائل التي تصل إلى هاتف الضحية من المبتزين في جرائم الابتزاز الإلكتروني حتى يتمكنوا من تحديد هوية المبتز ومتابعته إلى حين القبض عليه وتسليمه للعدالة.

36- هل هناك عقوبات رادعة لمرتكبي الجريمة الإلكترونية؟ وما هي هذه العقوبات؟

غلّظ مشروع القانون العقوبات على مختلف الجرائم الواردة فيه، فرفع عقوبة الحبس في الفقرة (أ) من المادة (3) إلى مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة أو بغرامة لا تقل عن 500 دينار ولا تزيد عن 1000 دينار، بدلاً من الحبس أسبوع الى ثلاثة أشهر أو الغرامة من 100 الى 200 دينار، وذلك في جرائم الدخول الى الشبكة المعلوماتية أو نظام معلومات دون تصريح أو بما يخالف أو يجاوز التصريح. كما رفع مشروع القانون العقوبات في الفقرتين (ب) و (ج) من المادة الثالثة، إذا أدى الدخول الى إحداث تغيير في عمل الشبكة أو نظام معلومات الشبكة أو موقع الالكتروني لتصبح "الحبس مدة لا تزيد عن سنتين وبغرامة لا تقل عن 500 دينار ولا تزيد عن 1000 دينار."

37- ما هي عقوبة القرصنة بأنظمة الكمبيوتر في الأردن؟

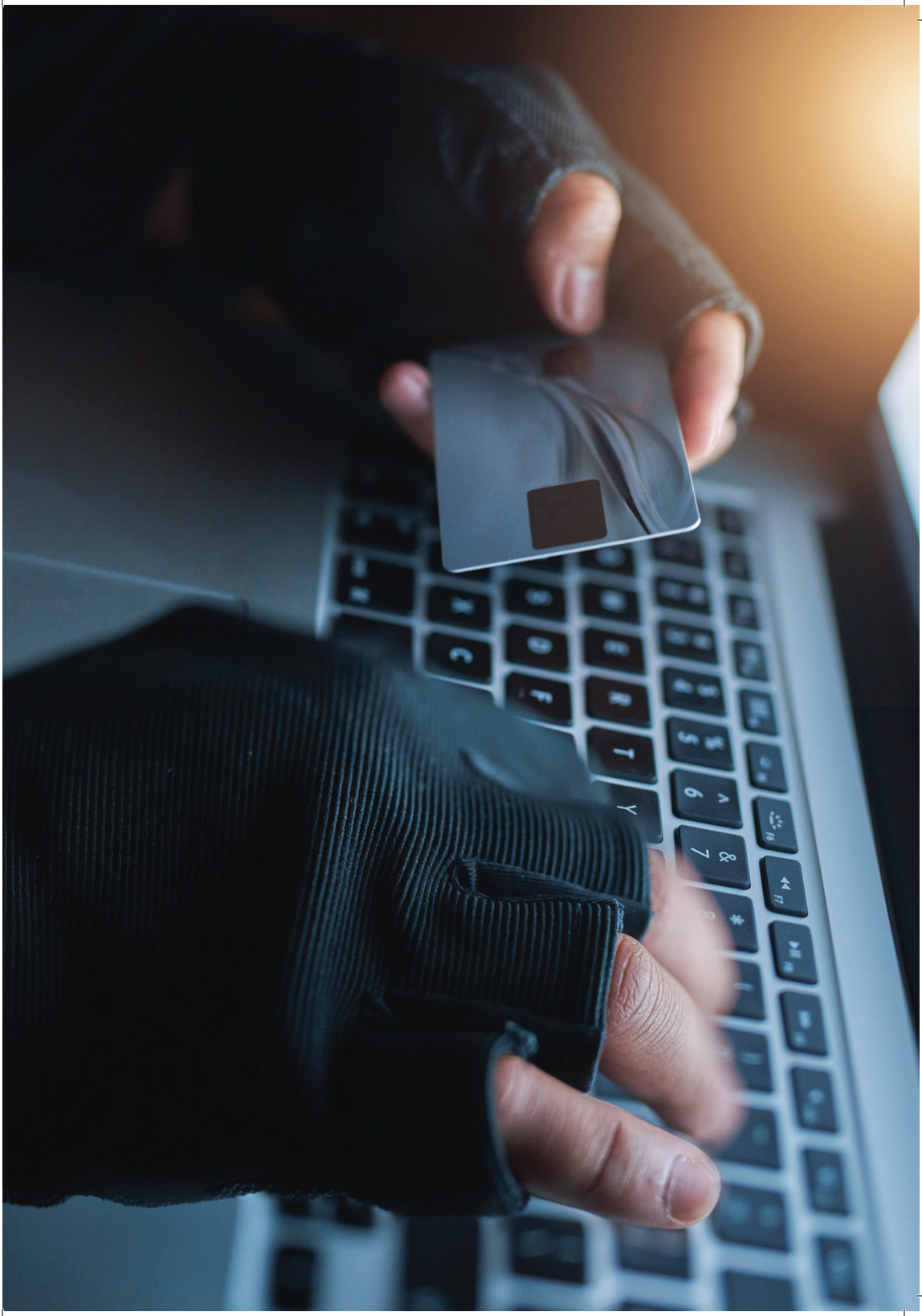
يعاقب كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

38- ما هي الحوسبة السحابية؟ وما هي فوائدها؟

الحوسبة السحابية هي تقنية كمبيوتر حديثة تعتمد على الإنترنت وتستخدم السحابة (عبارة عن مجموعة من الشبكات والأجهزة والخدمات والتخزين والواجهات التي يمكن أن توفر كخدمة حوسبة) لتقديم الخدمات أينما يريدها العميل وتوفر آلية للوصول إلى الخوادم المختلفة حول العالم.

الفوائد الرئيسية للحوسبة السحابية هي:

١. النسخ الاحتياطي للبيانات وتخزين البيانات.
٢. قدرات فعالة للخادم.
٣. زيادة الإنتاجية؛
٤. فعالة من حيث التكلفة، وتوفر الوقت.



39- ما الفرق بين الحوسبة السحابية والحوسبة المتنقلة؟

في التعريف، الحوسبة المتنقلة والحوسبة السحابية متشابهة إلى حد ما. تتبع الحوسبة المتنقلة مفهوم الحوسبة السحابية. وتوفر الحوسبة السحابية للمستخدمين البيانات التي يحتاجون إليها عند العمل على السحابة البعيدة للحوسبة المتنقلة، والتي تتيح للمستخدم الوصول للبيانات المخزنة وتعديلها.

40- ما المقصود بـ VPN ؟ ماذا يحتوي؟

VPN اختصار لـ (Virtual Private Network) وتعني الشبكة الافتراضية الخاصة وهي سحابة خاصة تدير أمن البيانات في البيئة السحابية عند التفاعل. ويمكنك بناء شبكة عامة باستخدام VPN كشبكة خاصة.

41- ما هي الفوائد الأمنية للحوسبة السحابية؟

خدمة التطبيق مرخصة من الحوسبة السحابية، لذلك يتم استخدامها في إدارة الهوية ويُمنح المستخدمون أذونات للتحكم في وصول مستخدم آخر يدخل بيئة السحابة.

42- ما هو عنوان بروتوكول الإنترنتIP؟

Internet Protocol Address

عنوان بروتوكول الإنترنت (بالإنجليزية: IP address) هو المعرف الرقمي لأي جهاز (حاسوب، هاتف محمول، آلة طابعة، موجه انترنت) مرتبط بشبكة معلوماتية تعمل بحزمة بروتوكولات الإنترنت، سواء أكانت شبكة محلية أو شبكة الإنترنت الواسعة. يقابل عنوان الآي بي مثلا في شبكات الهاتف رقم الهاتف.

43- ما هو السطو الإلكتروني؟

هو استخدام اسم نطاق بشكل غير قانوني، وهناك اختلاف بين أنواع السطو، إلا أن الهدف الأساسي منه هو سرقة اسم المجال أو إملائه بشكل خاطئ من أجل الاستفادة من زيادة عدد زيارات موقع الويب، ويعتبر السطو الإلكتروني أحد الجرائم الإلكترونية.

44- ما هو التجسس السيبراني (الإلكتروني)؟

هو فعل أو نشاط لجمع الأسرار باستخدام أساليب التلاعب غير القانونية على الإنترنت من الأفراد أو المنافسين أو الجماعات أو الحكومات أو الأعداء من أجل منفعة عسكرية أو سياسية أو اقتصادية.

45- ما هو التشهير السيبراني (الإلكتروني)؟

التشهير في معناه الاصطلاحي هو شهرة ما كان خفي أي نشر البيانات أو المعلومات التي تحدث من خلف الستار وإظهارها إلى العلن، وفي غالبية الأحيان يحمل التشهير هدفا سيئا يؤدي إلى فضح شخصية معينة أو مجموعة من الأفراد.

تعريف التشهير على الانترنت

تبعا لذلك فإن التشهير الإلكتروني هو نشر أمر ما أو لفت نظر الرأي العام نحو قضية معينة هي حادثة تحتمل أكثر من تفسير وأكثر من وجهة نظر، فالقانونيون على سبيل المثال، وصفوا التشهير الالكتروني على أنه أداة ردع خاصة في الحديث عن المجتمعات التي تقضي أوقاتا مضاعفة في الحياة الافتراضية مقارنة بالحياة الواقعية، فيما الرأي العام الذي يوظف أكثر من نصف جهده في التركيز على القضايا المطروحة على المنصات الإلكترونية أكثر من الموثقة بالأوراق على أرض الواقع، وذلك ليس من شأنه أن يخلق نوعا من التعجب، فالمجتمعات في كل العالم تستخدم الانترنت بنسبة تفوق الـ 90 بالمئة.

وحتى الأخبار التي تتشكل على أرض الواقع صارت تتناقل عبر شبكة الإنترنت أسرع إضافة إلى الحسابات الرسمية التابعة لأصحاب اتخاذ القرار ورؤوس السلطات المسيطرة في العالم ومحليا.

كل هذه المؤشرات تزيد من احتمالية تقبل فكرة التشهير بظاهرة معينة أو سلوك غير مقبول اجتماعيا وضمنيا حسب بروتوكولات المجتمع، وبين نقد هذه الظواهر ومراعاة فكرة الحريات والديمقراطية التي تضمن حق الخصوصية والتعبير عن الاختلاف دون الانصياع إلى الركائز التي ليس بالضرورة تنفيذها.

46- ما هو فيروس حشرة الحب؟

أحد أنواع البرامج الخبيثة التي تقوم بنسخ نفسها على أجهزة المستخدمين من غير معرفتهم وتسعى إلى إحداث خلل أو تدمير في ملفات أو جهاز المستخدم.

47- ما هي المطاردة عبر الإنترنت؟

تعتبر عملية المطاردة عبر الإنترنت ممارسة إجرامية حيث يستخدم الفرد الإنترنت لمضايقة شخص ما أو تهديده بشكل منهجي. ويمكن ارتكاب هذه الجريمة من خلال البريد الإلكتروني أو وسائل التواصل الاجتماعي أوغرف الدردشة أو عملاء المراسلة الفورية أوأي وسيلة أخرى عبر الإنترنت. يمكن أن يحدث المطاردة الإلكترونية أيضًا بالتزامن مع الشكل الأكثر تقليدية للمطاردة ، حيث يتحرش الجاني بالضحية خارج الإنترنت. ويشار إلى المطاردة عبر الإنترنت أحيانا باسم "التسلط عبر الإنترنت" أو "المطاردة الإلكترونية".

48- ما هي القنبلة المنطقية؟

القنبلة المنطقية عبارة عن برامج ضارة يتم تشغيلها بواسطة استجابة لأحد الأحداث، مثل إطلاق تطبيق أو عند الوصول إلى تاريخ أو وقت محدد. يمكن للمهاجمين استخدام القنابل المنطقية بطرق متنوعة، حيث يمكنهم تضمين كود تعسفي ضمن تطبيق مزيف، أو حصان طروادة، ويتم تنفيذه عند تشغيل البرنامج الاحتيالي.

ويمكن للمهاجمين أيضًا استخدام مزيج من برامج التجسس والقنابل المنطقية في محاولة لسرقة هويتك. على سبيل المثال، يستخدم مجرمو الإنترنت برامج التجسس لتركيب برنامج ولوج لاسلكي سرا على جهاز الكمبيوتر الخاص بك. وتستطيع هذه البرمجية التقاط ضربات المفاتيح، مثل أسماء المستخدمين وكلمات المرور. ويتم تصميم القنبلة المنطقية للانتظار حتى تقوم بزيارة موقع ويب يتطلب منك تسجيل الدخول باستخدام بيانات الاعتماد الخاصة بك، مثل موقع مصرفي أو شبكة اجتماعية. وبالتالي، فإن هذا سيؤدي إلى استخدام القنبلة المنطقية لتنفيذ برنامج الولوج اللاسلكي والتقاط أوراق الاعتماد الخاصة بك وإرسالها إلى مهاجم بعيد .

49- ما هي الفيروسات الضارة وبرامج الويب؟

فيروس الكمبيوتر هو برنامج مخفي في برامج أخرى، وعادة ما يكون غير ضار. والفيروسات قادرة على إنشاء نسخ عن نفسها وإدراجها في الملفات القابلة للتنفيذ من البرامج الأخرى. وعادة ما يقوم الفيروس ببعض الإجراءات الخبيثة – على سبيل المثال ، سرقة البيانات أو إتلافها.

50- ما هو التزوير والتزييف الحاسوبي؟

التزوير الإلكتروني : هو تغيير للحقيقة يرد على مخرجات الحاسوب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة، كتلك التي تتم عن طريق الطابعة، أو كانت مرسومة عن طريق الرسم.

كما يُعرف التزوير الإلكتروني على أنه" تغيير الحقيقة في المحررات الإلكترونية بأي وسيلة وذلك بغية استعمالها.

51- ما هو غسيل الأموال الإلكترونية؟

غسل الأموال عبر الإنترنت جريمة ناتجة عن أعمال وأنشطة إجرامية حققت عوائد مالية ضخمة من الأموال القذرة الناتجة عن أعمال غير شرعية يعاد ضخها في الاقتصاد العالمي عبر شبكة الإنترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاماً سرية بالشراء عبر الإنترنت، أو تداول الأسهم، وغيرها من الأنشطة التجارية والمالية التي تتم عبر شبكة الإنترنت.

52- ما هو الإرهاب السيبراني/ الإلكتروني؟

غالبًا ما يتم تعريف الإرهاب السيبراني على أنه أي هجوم متعمد وذو دوافع سياسية ضد أنظمة المعلومات والبرامج والبيانات التي تهدد بالعنف أو تؤدي إلى العنف. يتم توسيع التعريف أحيانًا ليشمل أي هجوم إلكتروني يخيف أو يولد الخوف لدى السكان المستهدفين.

53- ما هي الأنواع العشرة الشائعة للهجمات السيبرانية/الإلكترونية؟

1) البرامج الضارة
2) الحرمان من الخدمة
3) رجل في الوسط
4) التصيد
5) حقن SQL
6) استغلال يوم الصفر
7) أنفاق DNS
8) التنصت
9) الوصول المباشر
10) البرمجة النصية عبر المواقع

بإمكانك معرفة المزيد عن أبرز الهجمات السيبرانية خلال عام 2021 بالعربية من خلال زيارة الموقع التالي:

https://www.rmg-sa.com

54- ما المقصود بالـ HTTP و HTTPS وأيهما أكثر أمانا؟

HTTP هي اختصار لـ Hypertext Transfer Protocol وتعني بروتوكول نقل النص التشعبي وهو الطريقة الرئيسة والأكثر انتشاراً لنقل البيانات في الشبكة العنكبوتية العالمية (الإنترنت)؛

أما HTTPS فهي اختصار لـ Hypertext Transfer Protocol Secure وتعني بروتوكول نقل النص التشعبي الآمن وهو مزيج من بروتوكول نقل النص التشعبي مع خدمة بروتوكول لتوفير الاتصالات المشفرة وتحديد تأمين شبكة خادم الويب. HTTPS أكثر أمانا من HTTP كما يظهر من التعريف.

55- ما فائدة برنامج مكافحة الفيروسات (Anti-Virus)؟

1) أمن البيانات.
2) الحماية من الفيروسات وبرامج التجسس والبرامج الضارة.
3) الحماية من الجذور الخفية، وأحصنة طروادة، وهجمات التصيد، وهجمات البريد العشوائي.
4) الحماية من التهديدات السيبرانية.

56- ما هو خرق البيانات؟

يحدث خرق البيانات عندما يتم اختراق تدابير الأمن السيبراني لفرد ما أو شركة مما يسمح بالوصول غير المصرح به إلى المعلومات.

يمكن أن يكون ضارًا بشكل لا يصدق بسمعة الشركات وكذلك الأفراد إذا تم أخذ معلوماتهم.

يتعين على الشركات قانونًا اتخاذ تدابير لحماية البيانات الشخصية ويجب عليها إخطار أي شخص قد يتأثر بانتهاك محتمل.


Telegram
Google
Linkedin
Spotify
3
Twitter
Facebook
2
Instagram
Pinterest
Pinterest
1
Whatsapp
Tik Tok
Behance

57- ما هي البرمجيات الخبيثة؟

هي برامج ضارة بمجرد دخولها إلى نظام الهاتف أو الحاسوب، يمكن أن تتسبب في حدوث ضرر أو تعطيل أو سرقة للمعلومات. ويمكن للبرمجيات الخبيثة الوصول إلى نظامك إذا نقرت على رابط إلكتروني أو فتحت مرفقًا ضارًا في رسالة بريد إلكتروني على سبيل المثال.

58- كيف تعرف أنك تعرضت للاختراق الإلكتروني؟

لسوء الحظ ، فإن التهديدات الإلكترونية شائعة وليس من الواضح دائمًا أنه تم اختراق أمنك الإلكتروني. ومع ذلك، قد يشير ما يلي إلى تعرضك للاختراق ويجب عليك اتخاذ إجراء على الفور لمنع أي سوء استخدام أو ضرر آخر.

1) عدم القدرة على تسجيل الدخول إلى حساب (ليس نتيجة نسيان كلمة المرور الخاصة بك).

2) بدء تشغيل البرامج غير المعروفة عند تشغيل الكمبيوتر.

3) الرسائل الإلكترونية التي يتم إرسالها من حسابك إلى آخرين، والتي لم ترسلها.

4) منشورات على وسائل التواصل الاجتماعي من حسابك لم تقم بإنشائها.

5) ظهور النوافذ المنبثقة (التي قد تشجعك على زيارة موقع معين أو تنزيل برنامج).

6) جهاز الكمبيوتر الخاص بك لا يعمل كما هو معتاد – على سبيل المثال يبدو أنه أبطىء أو يتعطل بشكل متكرر.

59- كيف يمكنني تعزيز الأمن السيبراني/الإلكتروني؟

1) إعطاء الأولوية للأمن السيبراني.
2) لا تهمل حماية بيانات وخصوصية عملائك.
3) اتباع سياسة حماية صحية ومناسبة.
4) كلمات السر ليست كافية.
5) لا تثق بأحد.
6) احذر من الرسائل الخادعة للدعم الفني.
7) إعطاء الأولوية لأمن شبكات الجيل الخامس.
8) العمل عن بعد ومتطلبات الحماية.
9) بناء علاقات أوثق بين المطورين وفريق الأمن السيبراني.
10) الاستعانة بمصادر خارجية للأمن السيبراني.

60- ما هي برامج التجسس وأحصنة طروادة؟

أحصنة طروادة وبرامج التجسس هي الأدوات الخبيثة التي يمكن لمجرم الإنترنت استخدامها كجزء من هجومه للحصول على وصول غير مصرح به وسرقة المعلومات من الضحية.

61- ما هو التصيد الاحتيالي؟

التصيد هو ممارسة إجرامية تستخدم للوصول إلى المعلومات الحساسة مثل بيانات بطاقة الائتمان من الضحايا، والأكثر شيوعًا هو استخدام الميزات التي يسمح بها الصوت عبر بروتوكول الإنترنت (VoIP) وهي من أكثر الطرق شيوعًا لسرقة الهوية.

62- ما هي طرق الوقاية من الجرائم الإلكترونية؟

- أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
- تجنب فتح أي رسالة الكترونية مجهولة المصدر بل المسارعة إلى إلغائها.
- وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تُصعّب من عملية القرصنة.
- الحرص على المعلومات الشخصية والحاسب الشخصي وذلك بوضع برامج الحماية المناسبة.
- للوصول إلى معلوماتك الشخصية، اقرأ أحدث الطرق التي يبني بها المتسللون حيل التصيد الاحتيالي.
- لتقليل التهديدات والهجمات غير المرغوب فيها إلى الحد الأدنى، قم بتثبيت جدار حماية على جهاز الكمبيوتر الخاص بك.
- عند فتح رسائل البريد الإلكتروني والنقر فوق الروابط، كن حذرًا.
- عند تنزيل محتوى من مصادر لم يتم التحقق منها، يجب أن تقرأ بعناية.
- بالنسبة لأي موقع ويب يتم فيه تخزين المعلومات الشخصية، قم بإنشاء كلمات مرور قوية.

63- هل الدعم والترويج للجماعات الإرهابية عبر أنظمة المعلومات جريمة يعاقب عليها القانون؟

نعم، إن وضع إعجاب أو إعادة نشر أو مشاركة منشورات لجماعات أو تنظيمات إرهابية أو متطرفة قد يعرضك للحبس سنتين في السجن كحد أدنى بتهمة الترويج لجماعات إرهابية.

64- كيف نحمي الأطفال من المواد الإباحية عبر الإنترنت؟

- استخدام أدوات الأمان الخاصة بالعائلات: تتوفر هذه الأدوات في إعدادات جهاز الكمبيوتر الشخصي وفي أي جهاز إلكتروني آخر يستخدمه الأطفال.
- تثبيت أدوات الرقابة على جميع الأجهزة التي يستخدمها الطفل أو المراهق للدخول إلى الإنترنت.
- البحث بين الحين والآخر في سجل التصفّح (History).
- مراجعة التطبيقات الموجودة على الهاتف أو الجهاز اللوحي.
- اعتماد السرية في الصفحات الشخصية.
- مراقبة سلوك الطفل أو المراهق.
- متابعة الأهل الحثيثة لأطفالهم.

65- ما هو العمر المناسب للسماح للأطفال باستخدام وسائل التواصل الاجتماعي بحيث يكونوا قادرين على التمييز بين النافع والضار؟

لا زال العمر المثالي الذي يسمح عنده للأطفال بإمكانية استخدام مواقع التواصل الاجتماعي موضوعا مثيرا للجدل.

في العديد من البلدان، الحد الأدنى لسن الشخص الراغب في الانضمام إلى مواقع وسائل التواصل الاجتماعية مثل الفيس بوك، سناب شات..إلخ هو 13 عاماً.

66- كيف نحمي الأطفال من الجرائم الإلكترونية؟

- قم بتوعية الطفل بالإجراءات الأكثر موثوقية للحفاظ على الأمن الإلكتروني.
- تحاور معه، وتحدث إليه حول السلامة الافتراضية وتصفّح الإنترنت معه لزيادة التوعية.

إن كنت لا تجيد استخدام الوسائل التكنولوجية، لا تستسلم! يمكنك أن تلعب لعبة الأب الفطن. اجلس بكل بساطة مع طفلك واطلب منه تعليمك. أطلب منه أن يعلّمك كيفية استخدام البرامج التي يدخل إليها. بهذه الطريقة، يمكنك الاتّصال بصميم الأنشطة التي يقوم بها الطفل يوميًا على الإنترنت وتوجيهه في الوقت عينه.

- قم بتوعية الطفل لناحية عدم مشاركة أي معلومات خاصة بطبيعتها مثل الصور الشخصية. قل له ألا يشارك معلومات مثل اسمه الكامل، وعنوانه، واسم مدرسته، ورقم هاتفه، وكلمات المرور الخاصة به، لأسباب أمنية. انصحه بعدم نشر مثل تلك المعلومات أو تقديمها كردّ على الأسئلة التي يتلقاها عبر الإيميل أو الرسائل الخاصة، أو غرفة الدردشة، أو المنتديات. ساعد طفلك على فهم ما تقصده بجهات الاتّصال غير المناسبة.
- ابقَ على اطلاع. تعرّف إلى المواقع التي يرتادها طفلك والجهات التي يتواصل معها.
- استخدم برامج فلترة أو مراقبة. جهّز نفسك بالحرص على أن تحمي طفلك على الإنترنت حتّى لو لم تكن موجودًا لمراقبته.
- استخدم أدوات مراقبة أبوية. معظم المواقع الإلكترونية الموثوقة تتيح خيار الرقابة الأبوية التي يمكنك استخدامها.
- طبّق جميع الإعدادات المتعلّقة بالخصوصية.
- تعامل مع حساباتك، وأسماء المستخدمين، وكلمات المرور الخاصة بك على أنها معلومات حسّاسة. اختر اسم المستخدم الخاص بك بعناية بالنسبة للحسابات والإيميلات.
- لا تتردّد أبدًا في الاتّصال بالشرطة. في حال صادف طفلك أو أطفالك جهة اتصال غير مناسب، بلّغ وحدة الجرائم الإلكترونية فورًا بذلك.

67- كيف استخدم كلمة سر قوية جدا لحماية حساباتي الإلكترونية؟ وما هي التوصيات؟

تتميز كلمة المرور القوية بأنك الشخص الوحيد الذي يُمكنه تذكّرها ويستحيل على أي شخص آخر تخمينها، ويمكن ذلك من خلال:

- استخدام كلمة مرور مختلفة لكل حساب.
- استخدام كلمات مرور طويلة لكن يسهل تذكرها بربطها مع أمور تعرفها.
- تجنب استخدام المعلومات الشخصية والكلمات الشائعة.
- قم بتغيير كلمة السر بين الحين والآخر ولا تستخدمها لفترة طويلة.

68- ما هي المصادقة الثنائية؟ وكيف تعزز حماية حساباتك الإلكترونية؟

هي إجراء أمني يتمثل بطلب المصادقة مرتين لتأكيد هوية المستخدم. وعندما يتم تضمين البيانات الحساسة، مثل المعاملات المالية عبر الإنترنت غالبًا ما تكون المصادقة الثنائية مطلوبة. تتطلب المصادقة ذات العاملين إجراء أمان ثان لتأكيد هويتك. قد يكون الإجراء الأمني الثاني هو التعرف على الصوت أو الوجه أو بصمة إصبعك، أو قد تكون كلمة مرور لمرة واحدة (OTP) وهي رمز يتم إرساله إما إلى تطبيق مصادقة آمن على جهازك أو جهاز الكمبيوتر أو يتم إرساله عبر رسالة نصية إلى هاتفك الذكي. يجب إعادة الرمز مرة أخرى لمصادقة معاملتك. يتم إنشاء كلمة المرور لمرة واحدة بشكل عشوائي في الوقت الذي تكون فيه مطلوبة، وهي صالحة للاستخدام مرة واحدة فقط وعادة ما تنتهي المهلة إذا لم يتم استخدامها خلال فترة زمنية محددة وقصيرة.

69- كيف أقوم بعمل المصادقة الثنائية لحسابي على تطبيق واتساب؟

يدعم تطبيق التراسل الفوري واتساب ميزة التأمين التي تُعرف باسم المصادقة الثنائية Two–Factor Authentication على نظامي التشغيل آي أو إس iOS وأندرويد Android، والتي يمكنك من خلالها جعل حسابك أكثر أمانًا خلال بضع دقائق فقط.

تعتبر طريقة المصادقة الثنائية Two–Factor Authentication من أهم الطرق المُستخدمة في تأمين حساباتك، حيث أنها تضيف خطوة تحقق إضافية إلى عملية تسجيل الدخول الخاصة بحساباتك، فبدلاً من إدخال اسم المستخدم وكلمة المرور فقط لتسجيل الدخول إلى أحد الحسابات يتم إرسال كود جديد مختلف إلي هاتفك لتستخدمه في كل مرة تقوم فيها بالدخول إلي حسابك، حيث يُعد الحفاظ على أمان تطبيقات الاتصالات أمرًا مهمًا في هذه الأيام.

إليك كيفية تفعيل ميزة المصادقة الثنائية على واتساب:

يعد أمر تفعيل ميزة المصادقة الثنائية على تطبيق واتساب أمر سهل للغاية، ولكن في البداية تأكد من أنك تستخدم أحدث إصدار من التطبيق، يمكنك القيام بذلك عن طريق الذهاب إلى متجر جوجل بلاي Google Play بالنسبة لمستخدمي نظام أندرويد أو آب ستور بالنسبة لمستخدمي نظام آي أو إس ومعرفة ما إذا كان هناك أي تحديثات جديدة للتطبيق لم تقم بتثبيتها، ثم اتبع الخطوات التالية لتفعيل ميزة المصادقة الثنائية:

- انتقل إلى تطبيق واتساب.
- انقر على رمز القائمة في الجانب العلوي الأيمن من الشاشة ستفتح لك قائمة خيارات.



* اضغط على الإعدادات Settings.
* اضغط على الحساب Account.
* ثم اضغط على خيار المصادقة الثنائية Two–step verification.
* اضغط على زر التفعيل Enable الموجود أسفل الشاشة.
* بعد ذلك ستتم مطالبتك بإدخال رمز مرور مكون من ستة أرقام، ثم تأكيده عن طريق إدخال الرقم مرة أخرى، من المهم جدًا أن تتذكر هذا الرقم لأنه سيكون كلمة المرور الجديدة التي ستفتح من خلال حسابك على واتساب بشكل أساسي.
* ستتم مطالبتك بإدخال عنوان بريد إلكتروني، سيستخدمه تطبيق واتساب لإرسال رابط يمكنك استخدامه لتعطيل المصادقة الثنائية إذا فقدت أو نسيت رمز المرور.
* بعد الانتهاء من هذه الخطوات ستتمكن من تأمين حسابك على واتساب، وعندما تريد استخدام تطبيق واتساب بعد ذلك ستحتاج إلى إدخال رقم رمز المرور.
* تجدر الإشارة إلى أنه ما لم يُطلب منك من خلال رسالة بريد إلكتروني مباشرة تعطيل ميزة المصادقة الثنائية فيجب عليك عدم الضغط على أي روابط في رسائل البريد الإلكتروني التي قد يتم إرسالها، لأنها قد تكون مزيفة، وهدفها اختراق حسابك.

70- كيف أقوم بعمل المصادقة الثنائية لحسابي على فيسبوك؟

يمكن عمل المصادقة الثنائية على فيسبوك كالتالي:

1) قم بتسجيل الدخول إلى حساب فيسبوك الخاص بك.
2) اضغط على خيار المثلث المقلوب في أعلى يسار مع الانتقال إلى "الإعدادات".
3) انتقل إلى "الأمان وتسجيل الدخول".
4) ضمن "الأمان وتسجيل الدخول" سيكون خيارات مثل "تغيير كلمة المرور" و "تسجيل الدخول باستخدام صورة ملفك الشخصي" وتوجد أدناه "المصادقة الثنائية".
5) اضغط على "استخدام المصادقة الثنائية".

ويوجد خيارين يمكن من خلالهم عمل المصادقة الثنائية، الأول هو خيار "الرسالة النصية" والثاني هو المصادقة باستخدام تطبيق، يمكن اختيار ما يناسبك منهما.

71- كيف أقوم بعمل المصادقة الثنائية لحسابي على الجيميل (Gmail)؟

تفعيل ميزة "التحقّق بخطوتين" أو المصادقة الثنائية يتم كالتالي:

1) افتح حساب Google.

2) في لوحة التنقل، اختَر الأمان.

3) ضمن "تسجيل الدخول إلى Google"، اختَر التحقّق بخطوتين البدء.

4) اتّبِع الخطوات التي تظهر على الشاشة.

بعد تفعيل "التحقّق بخطوتين"، عليك إكمال خطوة ثانية لإثبات هويتك عند تسجيل الدخول. وللمساعدة في حماية حسابك، ستطلب منك Google إكمال خطوة ثانية محدّدة.

72- ماذا أفعل إذا كان طفلي متورطا في التنمر عبر الإنترنت؟

- كن داعمًا ومستجيبًا لجميع الأطفال الذين شاركوا في مواقف التنمر، سواء كانوا يتعرضون للتنمر أو يتنمرون على الآخرين (أو كلاهما).
- احصل على القصة الكاملة: استمع جيدًا وخذ الأمر على محمل الجد. قد لا يكون الأمر بسيطًا، وقد يكون الطفل أو المراهق هدفًا للتنمر أو ربما يتنمر على شخص ما أيضًا.
- ضع خطة لمعالجة الموقف مع طفلك. اسأل عما يمكنك فعله للمساعدة، واجعل إجابات الطفل أساس الخطة. ناقش ما سيفعله كل واحد منكم. احصل على مساعدة. ابحث عن مستشارين أو خبراء آخرين مدربين على التعامل مع الأطفال الذين تعرضوا للتخويف أو التنمر على الآخرين.

بالنسبة لطفل يتعرض للتنمر عبر الإنترنت:

- لا تقم بلوم الشخص المستهدف من التنمر – حتى لو كان هو من بدأها. لا أحد يستحق أن يتعرض للتنمر.
- نصح الأطفال بعدم الرد أو الانتقام.
- احتفظ بالمواد في حالة احتياج السلطات المعنية إليها.
- أبلغ عن التنمر الإلكتروني إلى موقع الويب أو الشركة التي حدثت فيها الإساءة.
- إذا شعرت أن طفلك معرض لخطر جسدي، فاتصل بالشرطة على الفور.

بالنسبة لطفل يتنمر على شخص ما عبر الإنترنت:

- حاول أن تفهم مصدر سلوك التنمر. (لكن لا تدع الأسباب تصبح أعذارًا).

- كن داعما. إنه السلوك، وليس الطفل، هذا ما تود أن تعالجه.
- ناقش كيف يمكن للطفل أو المراهق التعويض، مثل تقديم اعتذار أو القيام بعمل صالح للشخص الذي يتعرض للتنمر.

73- كيف أحمي نفسي من التحرش الإلكتروني؟

أولاً– رفع مستوى الحماية الذاتية على الإنترنت.

ثانياً– اكتساب المعرفة اللازمة بالاستخدام الآمن للإنترنت.

ثالثاً– اللجوء إلى القانون لمحاسبة المتحرش.

رابعاً– تثقيف الضحايا والفئات المحتمل تعرضها للتحرش الجنسي الإلكتروني.

خامساً– تثقيف المتحرشين أنفسهم.

74- ما هي الخطوات التي يجب اتباعها إذا كنت مضطرا لبيع هاتفك الذكي؟

1) نزع شريحة الهاتف

أول شيء يجب القيام به هو إخراج شريحة الهاتف حتى لو كنت ستحصل على شريحة جديدة؛ لأن الشريحة القديمة تحتوي على الكثير من أرقام تليفونات المعارف، وبالطبع لا تريد تركها في الهاتف القديم.

2) التخلص من بطاقة الذاكرة

لا تنسَ إلقاء نظرة على الفتحة الخاصة ببطاقة الذاكرة؛ لأنك لا تريد بيع الهاتف ببطاقة الذاكرة التي تحتوي على ملفاتك المهمة.

3) محو البيانات

يمكنك حذف البيانات الخاصة بك على الهاتف بطريقتين:

إما عن طريق الإعدادات ثم النسخ الاحتياطي Settings > backup/restore، ثم اختيار "إعادة ضبط المصنع". لكن قبل هذه الخطوة، تأكَّد من حماية بياناتك ومنع استعادتها مرة أخرى عبر تشفير الهاتف من الإعدادات ثم الأمن وتشفير الهاتف Settings > Security > Encrypt Phone.

أو القيام بعملية المسح يدوياً من خلال الوصول لكل ملف وتطبيق واختيار أمر الحذف، لكن هذه الطريقة لن تؤمّن بياناتك كلياً من خطر الاستعادة.

4) تنظيف الهاتف

بمجرد تنظيف الهاتف داخلياً من البيانات الخاصة بك، نأتي للخطوة التالية وهي تنظيفه من الخارج وإزالة بصمات الأصابع، وربما تزويده بِواقٍ لحماية الشاشة.

وللتخلص من البيانات المخزنة، نقوم بتشغيل "إعادة ضبط المصنع"، ثم محاولة ملء ذاكرة الهاتف بملفات عديمة الأهمية من الفيديوهات وغيرها. ويمكن تشغيل كاميرا الهاتف فترات طويلة حتى يتم استهلاك الذاكرة بالكامل، وعند محاولة الآخرين استرجاع ملفات هاتفك، يحصلون على بيانات وهمية لا قيمة لها. ويبقى الحل الآمن تماماً والمثالي الذي توصل إليه الباحثون هو: إما تدمير الجهاز وإما الاحتفاظ به وعدم بيعه.

75- هل هناك مخاطر من بيعي هاتفي الذكي الذي استعملته على الرغم من قيامي بحذف جميع الصور والفيديوهات والبيانات الخاصة بي؟

كشفت دراسة أجراها باحثون في جامعة كامبريدج البريطانية، أنَّ وضع "إعادة ضبط المصنع" لا يحذف جميع البيانات والحسابات وكلمات المرور من جهاز الأندرويد.

واختبر الباحثون مجموعة من أجهزة الأندرويد المستعملة، التي تعمل بنظام أندرويد 2.3 وحتى الإصدار 4.3.، وجدوا أنهم في جميع الحالات كانوا قادرين على استعادة رمز الأمان الخاص، الذي يتم إرساله للتصديق عند إدخال كلمة المرور للمرة الأولى لخدمات مثل واتساب وفيسبوك وجوجل، كما استطاعوا استعادة الرمز الرئيسي لـ 80% من تلك الهواتف.

والرمز الرئيسي للهاتف يُعتبر بمثابة مفتاح الباب الأمامي لبيتك، ومن خلاله يمكن استرجاع ملف اعتماد المستخدم (اسم المستخدم/كلمة المرور)، وحينها يصبح الأمر سهلاً لإعادة مزامنة جميع بياناتك للجهاز؛ ما يعني استعادة رسائل البريد الإلكتروني والصور المخزنة على الخدمات السحابية، إلى جانب جهات الاتصال.

76- كيف يمكننا بناء عالم إلكتروني أكثر أماناً؟

كل ذلك يتعلق بالتعليم والعمليات والتكنولوجيا. تحتاج المجتمعات والشركات إلى الاستثمار في تثقيف الموظفين والأفراد حول أفضل ممارسات الأمن السيبراني. بالإضافة إلى ذلك، تحتاج المجتمعات أو الشركات إلى تأمين البيانات بشكل فعال. يجب على المستخدمين اتخاذ قرارات أكثر استنارة عند التفاعل مع التكنولوجيا.

77- (للمؤسسات) ماذا أفعل إذا اشتبهت بتعرضي لهجوم إلكتروني؟

يجب أن يكون لدى مؤسستك عملية معالجة للهجمات الإلكترونية. إذا لم تكن متأكدًا ، فاسأل موفر تكنولوجيا المعلومات لديك أو أي

شخص في قسم تكنولوجيا المعلومات الداخلي لديك – فقد يوفر ذلك أموال نشاطك التجاري وسمعته في حالة حدوث هجوم إلكتروني.

78- ما هي الأدلة اللازمة التي يجب الاحتفاظ بها لإثبات الجريمة الإلكترونية؟

يتوجب عليك كشخص تعرض لجريمة إلكترونية الاحتفاظ بكافة المراسلات المكتوبة والتسجيلات الصوتية والجهاز أو الأجهزة المستخدمة أثناء وقوع الجريمة الإلكترونية وأي دليل رقمي آخر يساهم في إثبات وقوع الجريمة.

79- ما هي وسائل إثبات الجرائم الإلكترونية؟

يمكن إثبات الجرائم الإلكترونية بواسطة وسائل الإثبات التقليدية غير أن التطور التكنولوجي أدى إلى ظهور وسائل إثبات جديدة.

أولا: وسائل الإثبات التقليدية

تتمثل في الإقرار والشهادة والمعاينة والتفتيش والحجز والاختبار.

ثانيا: وسائل الإثبات الحديثة

ظهرت وسائل إثبات حديثة سهلت الكشف عن الجريمة الإلكترونية، وتتمثل في وسائل مادية ووسائل إجرائية.

1) **الوسائل المادية الحديثة:** يقصد بالوسائل المادية تلك الأدوات الفنية التي تستخدم في نظم المعلومات والتي تثبت وقوع الجريمة وتحدد الجاني. فالوسائل المادية عبارة عن أدوات او برامج ذات طبيعة تقنية يتم استخدامها بغرض إثبات وقوع الجريمة و تحديد مرتكبيها أو بالأحرى وسائل فنية تعهدف إلى جمع مختلف الأدلة الجنائية الرقمية التي يمكن من خلالها الكشف عن ملابسات الجريمة الإلكترونية. ومن بين هذه الوسائل إستخدام بروتوكول IP/ TCP والبروكسي Proxy والمعلومات التي تحتويها ملفات الكوكيز Cookies وبرامج التتبع وكشف الإختراق.

2) **الوسائل الإجرائية الحديثة:** يقصد بالوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية الإجراءات التي تستعمل أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، فالوسائل الإجرائية عبارة عن أساليب محددة قانونا تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وذلك باستخدام تقنيات وبرامج إلكترونية مختلفة. وتتمثل هذه الوسائل الإجرائية في اعتراض الاتصالات والمراقبة الالكترونية.



80- ماذا أفعل إذا كنت مضطراً لبيع هاتفي الذكي الذي كانت عليه ملفات حساسة خاصة بي وبعائلتي؟

يجب التخلص منها بشكل آمن للتأكد من أنه من المستحيل استرداد أي بيانات تحملها. قد تحتاج إلى استخدام خدمة احترافية للتخلص من البيانات للقيام بذلك نيابة عنك.

تشمل أجهزة التخزين أجهزة الكمبيوتر المحمولة والهواتف الذكية وأجهزة USB والتخزين المحمول والخوادم والمسجلات الرقمية على سبيل المثال.

81- ما هي أهم وأنفع خطوات العلاج من إدمان استخدام مواقع التواصل الاجتماعي؟

- الاعتراف بالمشكلة والإصرار على التخلص منها.
- تنظيم الوقت وجدولة أوقات محدّدة قصيرة لتصفح الانترنت.
- تَعلّم شيء جديد.
- حذف بعض الأشخاص من قائمة الأصدقاء.

82- ما هو دورك كفرد في مكافحة الجريمة الإلكترونية؟

- وعي الفرد لماهية الجرائم الالكترونية وكل ما يترتب عليها من مخاطر والحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها، وتسليط الضوء على موضوع الجرائم المتصلة بالكمبيوتر و سبل مكافحتها، للحيلولة دون المزيد من انتشارها.
- عدم الكشف عن كلمة السر نهائيا وتغييرها بشكل مستمر، مع تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.
- تجنب تحميل أي برنامج مجهول المصدر واستمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب.

83- ما هو دور الأسرة في توعوية الأبناء بخطر الجرائم الإلكترونية؟

1) على الأسرة غرس الأخلاق والقيم والوعي اللازم لاستخدام الإنترنت وتعرفتهم أصول التنشئة الصحيحة في مواجهة مخاطر شبكة الإنترنت .

2) ضرورة توعية الأبناء بالمخاطر بين الحين والأخر مع تعليمهم الاستخدام الصحيح بالتطبيق المباشر.

3) يجب على الأسرة تنظيم إستخدام أفرادها للإنترنت.

4) تشجيع الأبناء على التحدث عن أي شيء يشاهدونه أو يطلعون عليه أو يحصل معهم .

5) على الأسرة تنبيه أبنائهم بعدم إعطاء أي معلومات شخصية وتنبيههم على عدم تصديق أي شخص أو أي معلومة لأن الكثير من الأشخاص يتنكرون بأسماء وهمية لأغراض فاسدة أو منحرفة.

84- ما هي خطورة إدمان استخدام ومشاهدة المواقع الإلكترونية؟

مخاطر استخدام الإنترنت:

العزلة الاجتماعية يؤدي الإفراط في استخدام الإنترنت إلى البعد عن العالم المحيط، الأمر الذي يؤدّي إلى فقدان الأصدقاء، كما أنّ الاعتماد عليه في كل شيء يحدث سوءاً في التواصل بين الأشخاص، علماً أنّ التواصل المباشر يعتبر أفضل وسيلة للتواصل الاجتماعي مع الآخرين، كما أنّ الاستمرار في استخدامه يؤدّي إلى التفكك الأسري.

الأمراض يؤدّي الإكثار من استخدام الإنترنت إلى تدهور الحالة الصحية والإصابة ببعض الأمراض، مثل تصلّب العمود الفقري، والسمنة المفرطة، وآلام الرقبة، ومشاكل البصر، إضافةً إلى المشاكل النفسية، والشعور المستمرّ بالاكتئاب والقلق، والتوتر، وعدم الثقة بالآخرين، خاصةً في حال تكوين علاقات يظهر في نهاية المطاف أنها مع أشخاص غير حقيقيين.

سرقة المعلومات الشخصية يحتاج التفاعل على مواقع التواصل الاجتماعي إلى تدوين المعلومات الشخصية، التي من الممكن أن يصل إليها قراصنة الشبكة العنكبوتية، فيستخدمونها لأغراض غير أخلاقية، مما يضيع حق أصحاب هذه المعلومات ويعرضهم للمساءلة القانونية، وأحياناً قد يصل الأمر إلى اعتقالهم وسجنهم.

تعرض الأطفال إلى المواد الإباحية والعنف يعتبر الإنترنت من أكثر الوسائل الحديثة خطراً على الأطفال، علماً أنّ الوصول إليه أصبح سهلاً، وغير مقيّد بشروط أو أسس للتعامل معه، الأمر الذي يزيد من احتمالية دخول الأطفال إلى المواقع الإباحية المخلّة بأخلاقهم، وبالتالي التأثير على قيمهم التي تربّوا عليها، كما من الممكن دخولهم إلى مواقع تعرض مشاهد عنيفة، الأمر الذي يؤثر على المجتمع بشكلٍ غير مباشر كونهم هم لبنة هذا المجتمع، وأساس بنائه.

الإدمان يؤدّي الإفراط في استخدام الإنترنت إلى الإصابة بالإدمان عليه، الأمر الذي يؤثر على مجرى حياة الشخص، كونه يصبح غير قادر على الابتعاد عن الإنترنت، ولا يتخيّل حياته من دونه، كما لا بد من الإشارة إلى أنّ ذلك يؤثر على الإنتاجية العامة للأشخاص، وبالتالي يؤثر على تقدّم المجتمع وتطوّره.

تهديد الثقافة المحلية يؤدّي الانفتاح على العالم الخارجي إلى دخول ثقافات أخرى تؤثر على الثقافة المحلية للمجتمعات، خاصةً إذا كانوا ذوي ثقافة ووعي محددوين، علماً أنّ بعض هذه الثقافات قد تكون غير مناسبة.

تهديد الأمن الاجتماعي تؤثّر بعض مواقع التواصل الاجتماعي على الأفراد تأثيراً سلبياً، علماً أنها تستهدف فئة الشباب على وجه الخصوص، فيتم تجنيدهم ضد المصلحة العامة لبلدانهم الأمر الذي يؤثر على قوّة هذه البلدان، ويعرّضها للخطر.

85- ما هي الحلول لمكافحة الابتزاز الإلكتروني على النطاقين الشخصي والمؤسسي؟

مكافحة الابتزاز الإلكتروني على النطاق الشخصي:

- التأكد من محو جميع الصور والملفات الحساسة قبل بيع الهاتف المحمول إما باستخدام أحد تطبيقات محو الملفات في الجهاز نهائيًا مثل تطبيق Super Easer للأندرويد، أو عن طريق إعادة تهيئة الجهاز ثم تخزين ملفات غير مهمة فيه مرة أخرى، ثم إعادة التهيئة مرة أخرى ويفضل التكرار لعدد من المرات.
- عدم إرسال الصور الشخصية إلى أفراد غير معروفين على وسائل التواصل الاجتماعي حتى لغرض التعارف.
- تجنب إرسال الصور الخاصة على حسابات التواصل، لأن اختراقها قد يتسبب في حدوث الابتزاز الالكتروني.
- تفعيل دور الرقابة في الأسرة.
- اتباع الطرق الآمنة في استخدام الإنترنت وذلك بعدم فتح الروابط مجهولة المصدر قبل فحصها من التهديدات، وكذلك عدم فتح البرامج من أي مصدر غير معروف ما عدا تنزيلها من المتاجر المعروفة.
- الإهتمام بتحديث النظام والبرامج المشهورة على الجهاز وذلك لتجنب امتلاك تطبيق يحتوي على ثغرات يمكن استغلالها.

مكافحة الابتزاز الإلكتروني على النطاق المؤسسي:

- إخطار الموظف للإدارة في حال حدث له ابتزاز متعلق بالشركة أو المؤسسة.
- تدريب الموظفين على كيفية التعامل مع التقنية بالشكل الصحيح وبالتالي تجنّب الوقوع في الاختراق مثل التعامل مع رسائل البريد الإلكتروني بأمان.
- التخلّص السليم من القمامة وأجهزة الحاسوب القديمة حتى لا يتم استغلالها في كشف أسرار الشركة أو المؤسسة.
- تفعيل التوعية الأمنية لدى المجتمع بمختلف أطيافه بالنسبة للمؤسسات الاجتماعية.

86- كيف يمكنني منع التنمر الإلكتروني؟

كيفيّة الاستجابة للتنمُّر الإلكتروني

افعل ما يلي:

- التكلُّم مع شخص موثوق، والّذي قد يكُون المُدرّس أو أحد الوالدين أو مُقدّم الرعاية أو الصّديق. تقع المسؤوليّة على عاتق المَدارس للتأكُّد من عدم تعرُّض الطُّلاب للتسلُّط، ويُمكِنُه اتّخاذ إجراءاتٍ مُعيّنةٍ حتّى وإن حدَثَ التنمر خارج سُور المدرسة.
- تبليغ حادثة التنمُّر الإلكتروني إلى مُزوّد خدمة الانترنت (ISP) إن حدَثَ التنمر على الانترنت. وطلب المُساعدة من الوالدين أو المُدرّس.
- تبليغُ شركة الهاتف النقّال عن التنمُّر الإلكتروني إذا تمَّ تلقّي رسائلَ واتصالات التنمر على الهاتف النقّال. ربّما يتوجّب على المرء تغيير رقمه إذا حدَثَ التنمر بشكلٍ مُتكرّر.
- حظر الرّسائل الفوريّة ورسائلَ البريد الإلكتروني. وطلب المُساعدة من المُدرّس أو الوالدين.
- إخبار الشُّرطة بالتنمُّر الإلكتروني الخطير، مثل التهديدات الجسديّة أو الجنسيّة.

لا تفعل ما يلي:

- لا تحذِف الرّسائل أو مُراسلَات البريد الإلكتروني المُزعِجة أو تعليقات الفيسبوك.. إلخ. حافِظ على الدّليل. من المُمكن أن يُفيد في تَعيين هويّة الشخص المُتنمر إذا كانَ التنمُّر الإلكتروني من قبل شخصٍ مجهول. حتّى الأشخاص الّذين يستخدمُون اسماً أو بريداً إلكترونياً مُزيَّفاً يُمكنُ اقتفاء أثرهم.
- لا تَرُدّ. فهذا ما يُريده الشّخص المُتنمر، وربّما يجعل الأمرَ أسوأ.

كيف يُمكن تجنُّب التعرُّض للتنمُّر الإلكتروني؟

إنّ أفضلَ طريقة لتجنُّب التعرُّض للتنمُّر الإلكتروني هي باستخدام الإنترنت والهواتف النقّالة بحَذَر:

- عدم نشر تفاصيل شخصيّة، مثل رقم الهاتف الخاص أو العنوان.
- التّفكير بحذرٍ قبل نشر الصُّور أو مقاطع الفيديو الخاصّة بالمرء أو بأصدقائه على الإنترنت.
- إعطاء رقم الهاتف النقّال إلى الأصدقاء المُقرّبين فقط.
- حماية كلمة المُرور، وعدم إعطاء الأصدقاء حقّ الوُصول إلى الحِسابات الشخصية.
- استخدام إعدادات الخصوصيّة على مواقع التّواصل الاجتماعي.

* عدم تمرير رسائل البريد الإلكتروني السيئة.
* تعلُّم كيفيّة حظر التّراسُل الفوري أو استعمال فلاتر الرَّسائل لحظر رسائل البريد الإلكتروني.
* معرفة كيفيّة التبليغ عن التنمُّر الإلكتروني في مواقع التّواصل الاجتماعي أو مُزوّد خدمة الإنترنت أو مُدراء المواقع الإلكترونيَّة. وطلبُ المُساعدة من الآباء أو المُدرّس.

87- كيف يمكنني التواصل للاستفسار عن الأمور المتعلقة بالجرائم الإلكترونية؟

خصصت وحدة مكافحة الجرائم الإلكترونية في إدارة البحث الجنائي الرقم 065633404 للإجابة على جميع استفسارات المواطنين المتعلقة بالجرائم الإلكترونية.

البريد الإلكتروني: ecrimes@psd.gov.jo

88- ما هي إجراءات الإبلاغ عن الجريمة الإلكترونية؟

الجهة المختصة في تلقي الشكاوى المتعلقة بالجرائم الإلكترونية هي وحدة مكافحة الجرائم الإلكترونية – إدارة البحث الجنائي، وتتعامل الوحدة بمطلق السرية والخصوصية مع جميع الحالات التي تصلها.

ماذا أفعل؟

1) التوقف عن الحديث مع المجرم تماما وتجنب الرد.

2) توثيق كافة المراسلات المكتوبة أو الصوتية بينك وبينه.

3) إحضار لائحة شكوى إلى المدعي العام الأقرب إلى مكان سكنك، ومن ثم الذهاب إلى إدارة البحث الجنائي، وموقعها: عمان – العبدلي – بجانب شرطة وسط عمان. وفي إقليم الشمال: قفقفا (موقع السجن القديم).
أو الإتصال على الرقم: 196 – ثم اختيار الرقم الفرعي: 812594 أو 812595

89- ما مدى تأثير معرفتي بشخص يعمل داخل وحدة مكافحة الجرائم الإلكترونية على سرية المعلومات؟

تتعامل وحدة الجرائم الإلكترونية بمطلق السرية والخصوصية مع جميع الحالات التي تصلها.

90- هل بإمكان اللاجئين في الأردن الإبلاغ عن الجرائم الإلكترونية وتلقي الخدمة المطلوبة؟

نعم، بإمكان اللاجئين من مختلف الجنسيات الإبلاغ عن الجرائم الإلكترونية وتلقي الخدمة.

91- أين تقع وحدات مكافحة الجرائم الإلكترونية في الأردن؟

عمان – العبدلي – بجانب شرطة وسط عمان.
وفي إقليم الشمال: قفقفا (موقع السجن القديم).

92- هل تستطيع وحدة مكافحة الجرائم الإلكترونية الكشف عن الجاني المقيم خارج الأردن؟

نعم، فمن مهام وحدة الجرائم الإلكترونية التعاون الدولي مع الجهات الدولية في مجال مكافحة الجرائم الإلكترونية.

93- هل لوحدة مكافحة الجرائم الإلكترونية صفحة على فيسبوك بإمكاني متابعتها لأطلع على كافة التحذيرات والتوصيات الأمنية أولا بأول؟

نعم، لوحدة الجرائم الإلكترونية صفحة رسمية على فيسبوك بإمكانك متابعتها وتأكد من أنها مميزة بعلامة زرقاء بجانب اسمها "وحدة مكافحة الجرائم الإلكترونية".

المصدر/المرجع

موقع وحدة مكافحة الجرائم الإلكترونية، الأردن
https://psd.gov.jo/ar-jo

مطر، كامل. (2016). الجريمة الالكترونية.

بلغيث, جغلولي, & يوسف. (2021). صعوبات التحقيق في الجرائم الالكترونية. مجلة الر سالة للدراسات والبحوث الإنسانية 83–70, 6(3), .

نتائج المسح الميداني لمنظمة سايرن. 2020–2021.

المملكة. 2021.
https://www.almamlakatv.com

شاهين خضر–رضوان سعادة. (2021). الجريمة الإلكترونية وإجراءات مواجهتها. جامعة المسيلة.

البداينة، ذياب. (2014). الجرائم الإلكترونية: المفهوم والأسباب. كلية العلوم الاستراتيجية.

المنظمة العالمية للملكية الفكرية (WIPO)، اللجنة الاستشارية المعنية بالإنفاذ، جنيف، 2014.

JorJordan laws https

العجمي، عبد الله (2014). المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة. جامعة الشرق الأوسط. ص 45.

أشـــرف القواقزة، (2020). دور التشريع الأردني في مواجهة الجريمة الإلكترونيـــة وأثرهـــا في أمن معلومات المكتبات. دراسات، علوم الشريعة والقانون.

العجمي، عبد الله (2014). المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة. جامعة الشرق الأوسط. ص 75

غنيمات، طلال. 2020. ناشرو الإشاعات عبر مواقع التواصل الاجتماعي.. آن أوان تشديد العقوبات. الغد.
https://alghad.com

شبلوط، عصام. (2020). ما هو التصيد الصوتي Vishing؟ تعرف على مخاطره وطرق الحماية منه.
https://www.arageek.com

https://www.phptpoint.com

العجمي، عبد الله (2014). المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة. جامعة الشرق الأوسط. ص 47

Unicef. https://www.unicef.org

Childnet. https://www.childnet.com

رائد الأعمال العربي. 2022
https://the-arabic-entrepreneur.com

شركة حماة الحق للمحاماة
https://jordan-lawyer.com

مباركـــي، منال. (2017/2016). رسالة ماجستير بعنوان أشكال الجريمة الإلكترونية المرتكبـــة عبر الفيس بوك. جامعة العربي بن المهيدي – أم البواقي–. ص 59–61.

المحامون العرب
https://bestlawfirmjo.com

https://lawyermonem.com

https://jordan-lawyer.com

https://www.sawaleif.com

https://www.phptpoint.com

https://www.gkgigs.com

المركز العربي للبحوث والدراسات https://ar.theastrologypage.com
http://www.acrseg.org

https://ar.theastrologypage.com

https://ar.eyewated.com

https://www.bezpeka.com

جريمة التزوير الالكتروني في التشريع الاردني (دراسة مقارنة). عمر عبد السلام حسين الحبوري
https://meu.edu.jo

جرائم غسل الأموال على شبكة الإنترنت : دراسة مقارنة / عبد اللّه عبد الكريم عبد اللّه
http://librarycatalog.bau.edu.lb

https://www.techtarget.com

https://www.ihasco.co

"تقرير"10 نصائح لتحقيق الأمن السيبراني لك ولشركتك عام 2022
https://www.aljazeera.net
نصائح–من– ذهب–لتحقيق–الأمن–السيبراني

مركز العدل للمساعدة القانونية
http://www.jcla-org.com

https://www.lebarmy.gov

https://www.albawaba.com

الجرائم الإلكترونية وحقوق أطفالي
Retrieved from: https://www.safespace.qa/topic

https://support.google.com

https://aitnews.com

الصور التوضيحية مرفقة من خلال نفس الرابط

https://www.youm7.com

https://support.google.com

https://support.microsoft.com

https://www.google.com

https://arabicpost.net

https://arabicpost.net
https://hightouchtechnologies.com

https://www.annajah.net

بحث ودراسة حول الجرائم الإلكترونية وأنواعها والإجراءات القانونية لمكافحتها – استشارات قانونية مجانية (mohamah.net)

دور الأسرة في حماية الأبناء من مخاطر شبكة الإنترنت: دراسة ميدانية في مدينة سوهاج بصعيد مصر / محمود عبد العليم محمد سليمان
JiL.Center | Home (jilrc.com)
https://mawdoo3.com

https://faharas.net

مواجهة التنمر الإلكتروني
Retrieved from https://www.webteb.com

https://www.petra.gov.jo

الدكتور جابر غنيمي، 2020، رابطة القضاة العرب



التوعية الوطنية





مكالمات الفيديو الخاص بالصم



للتبليغ عن طريق رسائل الواتس آب



الرقم الموحد للطوارئ والتبليغ عن الحوادث المختلفة

مبادرة اللجنة التوعوية بجمعية التكافل الخيرية

#معاً.نُحدث.التغيير