



الجرائم المعلوماتية

#وعيك_يحمينا



إلكترونية

خطر تهدد حياة أطفالنا)

أضرار

حسب الدوافع

مسمياتها
حسب التنفيذ

طول مقترحة

عوامل مؤثرة

الأضرار الاسرية

الانتماء الإلكتروني

حرب على القيم والمبادئ

الأعراض

إجراءات

دور الآباء

تعريف

خصائصها

حسب النوع

الجرائم المعلوماتية

السلوكي والأمني

الإلكترونية

الجانب الصحي
خصائص

أساليب مكافحة

تعريف

الالكترونية



الألعاب
الإلكترونية

التنمر
الإلكتروني

الجرائم
المعلوماتية







الجرائم المعلوماتية

الجريمة المعلوماتية قد تكون تغريدة أو صورة أو مقطع فيديو أو رسالة جوال أو رسالة واتس أب أو مقطع سناب أو أي نوع من الوسائط الإلكترونية المستخدمة.

إن جرائم الكمبيوتر والإنترنت أو ما يسمى Cyber Crimes هي ظواهر إجرامية تفرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية وبمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

أي عمل يقصد إيذاء سمعة الضحية أو يسبب أذى مادي أو عقلي للضحية بشكل مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت

التعريف

الجريمة المعلوماتية: عمل إجرامي يتم استخدام وسيلة تقنية أو الشبكة المعلوماتية في ارتكابه كأداة رئيسية.

نقاط تتبع التعريف

أنواع الجرائم المعلوماتية: القرصنة أو الاختراقات الإلكترونية، السب والتشهير عبر الإنترنت، الاحتيال عبر البريد الإلكتروني والمواقع الوهمية، تزوير البطاقات الائتمانية، التصيد عبر الإنترنت.

استخدام أي من وسائل التواصل الاجتماعي في السب أو القذف أو التشهير يعد جريمة إلكترونية يعاقب مرتكبها بالسجن لمدة عام أو غرامة تقدر بمائة ألف ريال أو بهما معاً.

يعد تصوير الوثائق الرسمية وتسريبها عن طريق وسائل التواصل الاجتماعي انتهاك للبيانات الخاصة.

أحد أوجه المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف المزودة بكاميرا هو تصوير مصابي الحوادث المروية ونشر تلك الصور باستخدام الوسائل المختلفة.

التنصت والتجسس والدخول غير المشروع لبيانات شخص بغرض ابتزازه تعد من الجرائم المعلوماتية.

للإطلاع على نظام مكافحة الجرائم المعلوماتية يرجى زيارة الموقع التالي:

www.citc.gov.sa

نظام مكافحة الجرائم المعلوماتية

عرفت نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/17) تاريخ (1428/3/8) بناء على قرار مجلس الوزراء رقم: (79) تاريخ (1428/3/7)

الجريمة المعلوماتية بأنها: أي فعل يُرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

والجرائم المعلوماتية هي « المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية بشكل مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت.

يمكن تعريف الجريمة المعلوماتية أيضاً؛ بأنها استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة، وأمور غير أخلاقية لا يرضيها المجتمع لأنها منافية للأخلاق العامة.





إن هذا التعريف يشمل جميع أنواع الجرائم التي يستخدم فيها الحاسب الآلي أو أحد ملحقاته وبرامجه في تنفيذ أغراض غير شريفة كالتهجس والتسلل إلى أجهزة الآخرين، أو تدمير أو إتلاف مواقع إلكترونية، أو تزوير وقلب الحقائق والوثائق من خلال الدخول إلى أنظمة مستهدفة.

أنواع الجرائم المعلوماتية:

- التسلل والتهجس: حيث أن هناك فئة من الناس يعيشون التهجس على الآخرين بطرق مختلفة؛ فمن استراق السمع في الماضي، إلى تركيب أجهزة تنصت صوتية ومرئية، إلى ابتكار طرق وأساليب حديثة للدخول بها إلى أجهزة الحاسب الآلي الخاصة بالشخص المستهدف للحصول على أكبر معلومات ممكنة.

إن هذه الطريقة وفرت الكثير من المعلومات للأشخاص المتجسسين بحكم أن الحاسب الآلي أصبح المستودع الحقيقي والكبير في هذه الأيام، فالصورة تخزن في الحاسب الآلي وكذلك ملفات الصوت والفيديو، ناهيك عن الوثائق المهمة والمراسلات باختلاف أنواعها الرسمية والمالية والشخصية وغيرها، فجميعها موجودة في



الحاسبات الشخصية، ولذلك فبمجرد دخول المخترق لذلك الجهاز فإنه يكون قد كشف أسرار وخفايا تلك الضحية.

- الإتلاف والتدمير: بإمكان الشخص الذي يستطيع الدخول إلى جهاز شخص آخر من إتلاف محتويات ذلك الجهاز وتدميرها وحذفها أو نقلها إلى مكان آخر داخل ذلك الجهاز أو خارجه، ولك أن تتخيل عزيزي الكريم نوع تلك الوثائق وأهميتها التي من الممكن أن يطولها العبث والتخريب، فمن وثائق رسمية إلى معلومات مالية أو ميزانية شركات مساهمة أو أسرار حربية.

- التزوير والتغيير: إن الدخول إلى حاسوب آخر من قبل شخص له أهداف مريبة؛ يعني أن تلك فرصة عظيمة لذلك المجرم في أن يفعل ما يريد في ذلك الجهاز؛ فبإمكانه أن يغير الحقائق ويغير الأسماء والتواريخ في الوثائق والمستندات الموجودة في ذلك الجهاز، كما أن التزوير وتغيير الحقائق يشمل الصور وتغيير الوجوه والأشخاص الموجودين في تلك الصورة واستخدامها لأهداف مشبوهة، كما أن ملفات الفيديو وتغييرها وتركيب بعض وجوه المشاهير من علماء وفضلاء المجتمع أو من نجوم السينما والرياضة بهدف التشهير وإساءة السمعة،

كل ذلك يعد جريمة من جرائم المعلومات والتي نص النظام الجديد على العقوبة الصارمة بحق من يرتكبونها أو يساعدون على تنفيذها.

- الخداع والتغدير: إن الخداع والتغدير أمر مرفوض شرعاً وعرفاً، مما تسبب في انتشاره هذه الأيام هو تطور التقنية والبرامج الحاسوبية التي استخدمت للاستخدام السيئ من قبل ضعاف النفوس، حيث أنه باستخدام البرامج الاحترافية يستطيع الشخص الحصول على صور محسنة غير الصور الحقيقية وإخفاء العيوب منها ولا يظهر إلا المحاسن والمحسن فقط، كما أنه ومن مظاهر الخداع هو تقمص شخصية غير الشخصية الأساسية كأن يدعي صفة مسئول معين، أو أنه أنثى وهو عكس ذلك تماماً، بل هناك بعض البرامج ساعدت على ذلك منها تغيير الصوت، من ذكر إلى أنثى والعكس مع إمكانية تحسينه وعمل المؤثرات عليه.

أسباب الجريمة المعلوماتية وخصائصها

لا شك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن

شرعي كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

2 - التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

3 - الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.

4 - الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية الخ.

نصائح تهملك لتجنب الوقوع ضحية لجريمة معلوماتية

- توعية الأفراد ونصحهم لماهية الجرائم المعلوماتية وكل ما يترتب عليها من مخاطر.

- الحرص على الحفاظ على سرية المعلومات الخاصة

نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع.

فضلا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تماما عن الخصائص التي تتمتع بها الجرائم التقليدية، كما أن الجاني الإلكتروني (أو المجرم الإلكتروني) يختلف أيضا عن المجرم العادي.

ويأتي في مقدمة أسباب الجريمة المعلوماتية، غاية التعلم والتي تتمثل في استخدام الكمبيوتر والإمكانيات المستحدثة لنظم المعلومات وهناك أمل الربح وروح الكسب التي كثيراً ما تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية.

أهداف الجرائم المعلوماتية

نستطيع تلخيص بعض أهداف الجرائم المعلوماتية ببضعة نقاط أهمها:

1 - التمكن من الوصول الى المعلومات بشكل غير

- كالحسابات البنكية، والبطاقات الائتمانية وغيرها.
- عدم الكشف عن كلمة المرور نهائياً وتغييرها بشكل مستمر، ووضع كلمة المرور بشكل مطابق للمواصفات الجيدة التي تصعب من عملية القرصنة عليه ومن هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف وأن يكون متنوع الحروف والرموز واللغات إلخ.
 - تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.
 - تجنّب تحميل أي برنامج مجهول المصدر.
 - استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها، McAfee، Norton.
 - المسارعة في إبلاغ الجهات الأمنية فور التعرض لجريمة إلكترونية من خلال نظام أبشر www.moi.gov.sa لمكافحة الجرائم المعلوماتية لفرض العقوبات حسب نوعها.





- استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.
- الحرص على تأمين الوصول إلى الملفات السرية عن طريق استخدام الوسائل المختلفة للتشفير مثل Bit locker.
- عدم ترك جهاز الحاسوب مفتوحاً.
- قطع اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.
- أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
- لا تضع معلوماتك الخاصة على الإنترنت وتذكر أنه بمجرد أن تنشر معلومات على الانترنت لن تتمكن أبداً من التحكم بخصوصيتها حتى لو قمت بحذفها.



تجنب تخزين الصور الخاصة على
مواقع التواصل والحاسوب
وتأمين الملفات السرية
والمعلومات الخاصة بالتشفير
مثل Bit locker. تذكر أن ما
تنشره لن تتحكم به حتى لو حذفته



احذر ولا تصدق ما يصل من
إعلانات وتأكد من مصداقيتها
عن طريق محركات البحث



عدم ترك جهاز الحاسوب مفتوحاً
وقطع الاتصال بشبكة الإنترنت
عند عدم الاستخدام



تقنيات متطورة للكشف عن
هوية مرتكب الجريمة



استمرارية تحديث برامج الحماية
الخاصة بأجهزة الحاسوب ومنها،
Norton



مواكبة التطورات المرتبطة
بالجريمة الإلكترونية والحرص
على تطوير وسائل مكافحتها



أساليب مكافحة

الجرائم الإلكترونية



أبلغ الجهات الأمنية عن الجريمة
الإلكترونية من خلال تطبيق كلنا
أمن أو عبر نظام أبشر
www.moi.gov.sa
للمكافحة
ولفرض العقوبة



تجنب تحميل أي برنامج مجهول
المصدر واستخدام برمجيات آمنة
ونظم تشغيل خالية من الثغرات



توعية الأفراد والحفاظ على سرية
المعلومات الخاصة بالحسابات
البنكية، والبطاقات الائتمانية
وغيرها



إخفاء كلمة المرور نهائياً
وتغييرها بشكل مستمر، وتكون
قوية حسب الشروط



التنمر الإلكتروني

يشمل ممارسة التهديد أو إرسال العبارات المسيئة أو التحريض على الكراهية وإثارة السخرية، فلقد أصبح خطراً حقيقياً على الصحة النفسية للأطفال والمراهقين

والتنمر يكون عبارة عن استخدام التكنولوجيا لبث الخوف عن طريق ممارسة التهديد، أو العبارات المسيئة أو المهينة، أو التحريض على الكراهية، وإثارة السخرية، سواء كانت هذه الوسيلة عبر وسائط مرئية، مثل الصور أو الفيديوهات أو الرسائل النصية.

عوامل مؤثرة

الحالة النفسية:

يعتمد الترهيب عبر الإنترنت، أو التنمر، في الأساس على عنصر الحالة النفسية للمتلقى، ومدى ثباته وثقته في نفسه التي تتأثر أمام الرسائل المتكررة السلبية؛ إذ أن تكرار الإهانة والإساءة يضاعف من حدة الحالة، وبخاصة إذا كانت من أشخاص معروفين، مثل أقران المراهق في المدرسة أو النادي.



بدايات بسيطة ونهايات مفاجئة

والمثير أن بعض الدراسات أشارت الى أن بعض التحرشات لا تبدأ بقصد الإيذاء، بل بقصد الدعابة أو السخرية، لكن الأمر يمكن أن يتطور للترهيب فعلا، وذلك حسب الثبات النفسي وعدم وجود ضغوط أخرى على المراهق. وعلى سبيل المثال، يفترض بعض الأصدقاء أن السخرية من المظهر أو التفوق الدراسي لمراهق في الصف الإعدادي أمر ليس بالغ الخطورة، ولا يتعدى كونه مجرد مزحة، ولا يسبب الاكتئاب أو الإحباط في حالة المراهق السوي نفسيا. وهذه الفرضية على الرغم من منطقيتها، فإنها في حالة تكرارها بشكل متواتر وبشكل جماعي مع وجود بعض المشكلات النفسية من الأساس (مثل عدم التقبل وهو شعور يعاني منه الكثير من المراهقين) يمكن لهذا الأمر الذي بدا نوعاً من المزاح أن ينتهي بكارثة ناتجة من تحطم معنويات الضحية ودخوله في اكتئاب حاد.

حجم المشكلة:

ومشكلة الترهيب أكبر مما يظن الآباء، حيث إن معظم الأطفال في الأغلب لا يعترفون بتعرضهم للترهيب

لذويهم، إما بسبب الخوف أو الخجل من الإهانات التي يتلقونها. وهناك بعض الدراسات تشير إلى أن هناك واحداً من كل 4 أطفال تعرّض للترهيب من خلال الإنترنت، كما أن هناك إحصائيات تشير إلى أن واحداً من كل 6 أطفال اعترف بتعرّضه للترهيب. وهناك بعض الدراسات تشير إلى أن نسبة تقترب من 50 في المائة من المراهقين تعرّضوا للترهيب مرة واحدة على الأقل. ويعتبر تعدد وسائل التكنولوجيا من أجهزة كمبيوتر وهواتف ذكية وأجهزة لوحية من الأشياء التي تجعل المراهق يشعر بالحصار، وأنه لا مهرب من هذه الضغوط. والمثير في الأمر أن الضغوط النفسية مثل القلق والتوتر لا تحاصر الضحية فقط وإنما يكون الجاني أيضاً عرضةً لهذه الضغوط مما يهدد في انخراطه مستقبلاً في أعمال عنيفة أو إجرامية.

الأعراض

يجب على الآباء ملاحظة بعض الأعراض التي تشير إلى تعرّض المراهق للترهيب حتى لو لم يفصح عن السبب الحقيقي مثل:

- الشعور بالضيق بعد قضاء وقت معين على الكمبيوتر أو الأجهزة الأخرى.



- التحفظ جدا فيما يتعلق بالخصوصية على الهاتف أو الكمبيوتر.

- الانسحاب الاجتماعي من الأسرة والأصدقاء والأنشطة المختلفة المعتادة له.

- تجنب التجمعات من الأقران المحيطين سواء في المدرسة أو النادي.

- التصرف بشكل عنيف تتراوح حدته في المنزل، بمعنى تغيير السلوك وتحوله لنهج عدواني بداية من حدة الحديث ونبرة الصوت، ونهاية بالعنف الفعلي مثل تحطيم الأشياء أو الشجار مع الإخوة الأصغر.

- تغيير المزاج والسلوك، مثل البدء في التدخين لتخفيف حدة التوتر، وأيضا حدوث تغيير في نموذج النوم، سواء بالأرق المستمر أو بالنوم لساعات طويلة.

- تغير الشهية، وفي الأغلب تكون بفقدان الشهية للأطعمة التي كان يفضلها.

- ملاحظة محاولات الابتعاد عن الكمبيوتر أو الهاتف مصدر التوتر، مثل غلق الهاتف لفترات طويلة خلافاً للمعتاد.



لمنع هذا السلوك، ويُفضل أن يقوم الآباء بوضع الكمبيوتر في وسط المنزل، وعدم تركه في غرفة الأبناء، حتى يشعروا بالتعزيب حيال تلقيهم رسالة جديدة (منع استخدام المحمول يصيب الأبناء بالقلق لأنه يتوقع أن هناك المزيد من الرسائل ولا يملك معرفتها).

إجراءات مهمة

هناك الكثير من الإجراءات التي يجب عملها حيال اكتشاف التعرض للترهيب:

* إبلاغ إدارة المدرسة، حيث إن المدرسة تعتبر المجتمع الأكبر الذي يتحرك من خلاله المراهق، وبخاصة أنه في الكثير من الأحيان يكون القائمون بالترهيب من المدرسة نفسها، وعلى علاقة وثيقة بالمراهق.

* يجب الاحتفاظ بالرسائل النصية أو الصور أو الفيديوهات التي يقوم الجناة بإرسالها حتى تكون بمثابة دليل إثبات للتعرض للترهيب.

* في حالة عدم التمكن من معرفة الأشخاص القائمين

- الشعور بالتوتر والقلق في كل مرة يتلقى فيها رسالة إلكترونية، سواء عبر البريد الإلكتروني أو عبر الهاتف.

- تجنب النقاش حول الأجهزة الإلكترونية والهواتف الذكية، سواء بالسلب أو بالإيجاب.

دور الآباء

هناك دوراً مهم للآباء في مواجهة ظاهرة الترهيب عند اكتشاف أن أحد الأبناء يتعرض لها بعد ملاحظة الأعراض السابقة عليه.

1 - يجب أن يقوم الآباء بطمأنة أبنائهم وتعزيبهم نفسياً وعدم السخرية من حجم المشكلة مهما كانت تبدو بسيطة لأن عدم تقدير المشكلة يضاعف من الألم النفسي للمراهق أو الطفل الذي تعرّض للترهيب .

2 - الشعور بالمشاركة يمنح الأبناء الثقة ويجعلهم قادرين على التحدث بشكل كامل وأكثر استعداداً لتقبل النصائح حيال ذلك الموقف.

3 - التأكيد على الوقوف بجانب الأبناء واتخاذ خطوات جادة



بالترهيب يجب محاولة منعهم من إرسال رسائل مرة أخرى، وبخاصة أن معظم الأجهزة الإلكترونية بها خاصية حظر للأشياء غير المرغوب بها Block.

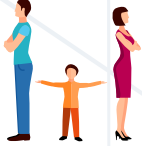
* في بعض الأحيان التي تكون بها تهديدات أو ابتزاز لدفع مبالغ نقدية، أو تعرض فعلي للعنف يجب إبلاغ الجهات الرسمية المسؤولة.

* يجب إجراء ندوات للتوعية بالترهيب وأخطاره، والإبضاء الناتج منه، والتأكيد على أنه عمل غير أخلاقي، ولا يمكن أن يعتبر دعاية أو فكاهة.

* يجب عمل جلسات علاج نفسي للمراهقين الذين يثبت تورطهم في الترهيب لمعالجة الخلل السلوكي لديهم؛ حتى لا يتطور الأمر إلى شكل أكثر عنفا.



عدم السماح للأطفال مصاحبة
أصدقاء أكبر منهم سناً



عدم انشغال الوالدين بالخلافات
النسرية وإهمال البناء



دور المدرسة له أهمية في
التثقيف والتوعية



عدم السماح للأطفال بالخروج
مع الأقارب غير الموثوق بهم
بغرض الترفيه



التمنر

النسرة خط الدفاع الأول
عن براءة أطفالهم



عدم السماح للأطفال بالبيت
خارج البيت



مراقبة سلوكيات الخدم، وعدم
الثقة الزائدة بالخدم



عدم الثقة الزائدة بالأصدقاء



عدم الغياب المتكرر
للوالدين عن المنزل



اعتاد أطفال الأجيال السابقة اللعب بالألعاب المرتبطة ببذل قدراتٍ ذهنية أو حركية أو بذلها معاً، إلا أنه وبعد تطور التكنولوجيا واختراع الحاسوب وتوافره في كل منزل تطوّرت صناعة الألعاب الإلكترونية وحُصّص الكثير منها للأطفال، فتركوا أساليب اللعب التقليدية واتجهوا للألعاب الإلكترونية، فما هي الألعاب الإلكترونية؟ وما هي الأضرار الناجمة عنها؟ وما دور الآباء في ذلك؟



الألعاب الإلكترونية

تُعرّف الألعاب الإلكترونية (Electronic game) بأنها نشاط له قواعد مُحدّدة، ويشترك فيه لاعبون في قضيّة أو نزاع مصطنع، بحيث يكون له نتائج تُقاس بشكلٍ كميّ، وتسمّى اللعبة بأنها (إلكترونية) إذا تواجدت بهيئة رقمية، وعادة ما تُشغّل على منصّات متنوعة كشبكة الإنترنت، والحاسوب، والتلفاز، والهواتف الثّقالة، والفيديو، PlayStation، والأجهزة المحمولة بالكف Palm devices.

تصنيفُ الألعاب الإلكترونية:

تُصنّف الألعاب الإلكترونية من حيثُ فئة مستخدميها والهدف منها إلى ثلاثة أنواعٍ رئيسية هي:

1 - ألعاب الذكاء

2 - ألعاب الإثارة والمتعة

3 - الألعاب التعليمية



أضرار الألعاب الإلكترونية

للألعاب الإلكترونية آثارٌ سلبيةٌ تعودُ على من يلعبها سواءً كان من الكبار أو الصغار بأضرار كثيرة وفي جوانب مختلفة، ومن هذه الأضرار:

الأضرار في الجانب الاجتماعيّ

يُعرّض إدمانُ الألعاب الإلكترونية الأطفال والمراهقين إلى خلل كبير في علاقاتهم الاجتماعية؛ حيثُ يعتادُ الطفلُ السرعة في هذه الألعاب، مما قد يُعرّضه لصعوبة كبيرة في التأقلم مع الحياة الطبيعية ذات السرعة الأقل درجة، الأمر الذي يقوده إلى الفراغ النفسي والشعور بالوحدة سواءً في منزله أو مدرسته.

تُسبب هذه الألعاب العزلة الاجتماعية والميل إلى الانطوائية، إذ أنّ الطفل الذي يقضي في ممارسة هذه الألعاب ساعات كثيرة دون أدنى تواصلٍ مع الآخرين، بعكس الألعاب السّعبة التقليدية التي تتميّز بالتواصل، بالإضافة إلى أنّ الطفل الذي يُسرفُ في قضاء الوقت في الألعاب الإلكترونية سينعزل عن العالم الحقيقي ليجد نفسه مفتقداً

مهارات التّعامل مع الآخرين وإقامة العلاقات والصّداقات، مما يُحوّله طفلاً خجولاً لا يستطيعُ التعبير عن نفسه ومكنونه.

تصنع الألعاب الإلكترونية أطفالاً أنانيّين يُفكّرون في إشباع حاجاتهم من الألعاب فقط، دون أن ينتبهوا لوجود من يشاطرهم اللعب، فتحدثُ الكثير من المشاكل بين الأشقاء على دور اللعب، بعكس الألعاب الشعبية التقليدية التي تتميّز بأنها ألعابٌ جماعية.

الأضرار في الجانب الديني

تحتوي بعضُ الألعاب الإلكترونية على الكثير من الأفكار والعادات التي لا تتوافق مع الدين وعادات المجتمع وتقاليده، وتُساهم في تشكيل ثقافةٍ مشوّهة وغير مناسبة للطفل.

تؤسّس بعض الألعاب الإلكترونية لأفكار الرذيلة والإباحية التي تدمّر عقول المراهقين والأطفال عبر ما يُعرّض من مشاهد فيها.



يؤدّي إدمان الألعاب الإلكترونية إلى إلهاء من يلعبها عن عباداته المفروضة عليه، وبخاصّة الصلوات الخمس، بالإضافة إلى أنّها تلهيه عن صلة الأرحام، وطاعة والديه وتنفيذ طلباتهم.

الأضرار في الجانب الصحي

تقود الألعاب الإلكترونية إلى الإصابة بأمراض الجهاز العضليّ والعظميّ بسبب حاجتها لتفاعل اللاعب معها بحركات سريعة متكرّرة.

تؤدّي الألعاب الإلكترونية إلى آلام أسفل الظهر نتيجة الجلوس لساعات طويلة أمام أجهزة الحاسوب والتلفاز.

تؤدّي الألعاب الإلكترونية إلى حدوث أضرار كبيرة لمفصل الرسغ وإصبع الإبهام؛ بسبب الحاجة لثنيهما باستمرار. تؤثّر الألعاب الإلكترونية بشكل مباشر وسلبيّ على نظر الأطفال؛ إذ إنّ هناك احتمالية لأنّ يُصاب الطفل بضعف في البصر نتيجة تعرّضه بشكل مستمر للأشعة الكهرومغناطيسية قصيرة التردد القادمة من شاشات التلفاز والحواسيب.



الأضرار في الجانب السلوكي والأمني

تعتمد نسبة كبيرة من الألعاب الإلكترونية على عنصر الاستمتاع بقتل الناس، وتخريب ممتلكاتهم، والاعتداء عليهم دون حق. وتُعلم نسبة كبيرة من الألعاب الإلكترونية الأطفال والمراهقين طرق ارتكاب الجرائم وجلبها؛ مما يُنمّي في عقولهم أفكاراً ومهاراتٍ حول العنف؛ حيثُ يكتسبون هذه الأفكار والمهارات عبر الاعتياد على ممارسة هذه الألعاب.

الأضرار في الجانب الأكاديمي أو التحصيل العلمي

تؤثّر الألعاب الإلكترونية بشكلٍ سلبيٍّ على الأداء الأكاديميِّ لمن يلعبها؛ إذ أنها تقوده لإهمال واجباته المدرسية.

وتقوّد الألعاب الإلكترونية الأطفال والمراهقين الى سهر الليل لفتراتٍ طويلة والتأخر في النوم، مما يؤثّر بشكلٍ مباشر على تركيزهم وتفكيرهم، فتجعلهم غير قادرين على الاستيقاظ للذهاب للمدرسة صباحاً، وإن ذهبوا فإنهم سيستسلمون للنوم عوضاً عن التركيز والاستماع، مما يؤثّر على تحصيلهم الدراسي.

الأضرار الأسرية

عدم إدراك أولياء الأمور ما تحمله تلك الألعاب من سلبيات، فيقتني أولياء الأمور تلك الألعاب غير مباشرين بالأوقات الطويلة التي يقضيها أبنائهم أمام تلك الشاشات. وبالتالي لا يمكن حصر السلبيات والأضرار الناجمة عنها. فلا بد من وجود إدراك وحسن تربية وشعور بالمسؤولية عند التعامل مع الألعاب الإلكترونية.

حلول مقترحة لتجنب أخطار الألعاب الإلكترونية والمواقع والأفلام الإباحية عن الطفل والمراهق

يقدم الخبراء عدة نصائح مفيدة وسليمة لتساعد في تجنب أخطار تلك الألعاب والسيطرة على أضرارها:-

التحدث مع الطفل عن اللعبة التي يحبها، واكتشاف سبب تعلقه بها ومن ثم مشاركة الطفل تلك اللعبة لإحياء روح الصداقة بداخله من جديد وبذلك تستطيع مراقبة تلك اللعبة والسيطرة عليه في أي وقت.

انظر على غلاف كل لعبة قبل شرائها لطفلك، واطرأ إرشادات السلامة المكتوبة عليها حول نوع اللعبة وكيفية



استخدامها وأيضا العمر المناسب لها كي لا تؤذي طفلك دون قصد.

تخصيص وقت للعب بالألعاب الإلكترونية، على ألا يتجاوز ذلك مدة ساعة يوميا، ثم يقوم الطفل بلعب أي نوع من الرياضة مهما كان بسيطاً.

يمكنك تفعيل جهاز المراقبة والتحكم الأبوي بالأجهزة على تطبيقات الألعاب الإلكترونية مثل:

- تحميل برنامج (ourpact) للتحكم بتطبيقات جهاز الطفل.

ويكون تحميل البرنامج بجهاز أولياء الأمور وجهاز الأطفال.

جهاز الطفل بعد التحميل يتم تسجيل اسم الطفل وكتابة الایمیل وكلمة السر المستخدمة بجهاز ولي الأمر.

يظهر رابط pair.ourpact.com يتم نسخه ومن ثم فتح المتصفح ثم لصق الرابط والضغط على دخول وكتابة الایمیل السابق.

كتابة اسم الطفل ثم pair ثم install ثم كتابة password ثم install ثم Trust.



تغيير إعدادات اللغة من فاضحة إلى مقيد.

لمحتوى الويب اختيار مقيد.

مواقع الويب اختيار مواقع الويب المحددة فقط.

شجع طفلك بشراء لعبة لتنمية الذكاء أو لتعليم نشاطات جديدة بدلاً من اللعب دائماً بمثل تلك الألعاب، فبيدأ في التخيل والإبداع والاستفادة من اللعبة عن كونها شيئاً ترفيهياً فقط.

. ابدأ بمشاركة طفلك مع أصدقائه في الألعاب الجماعية وحاول قدر المستطاع إبعاده عن الألعاب الفردية، ليتكون لديه حب المجتمع والأصدقاء والبعد عن العزلة والاكنتاب.

. يجب تعويد الطفل منذ الصغر على ممارسة التمارين الرياضية التي تحافظ على رشاقة جسمه كما تخرج الطاقة الكامنة بداخله في شيء مفيد بعيداً عن استهلاك طاقته في لعبة عدوانية.

اقرأ لطفلك ليلاً قصصاً مسلية، لغرس حب القراءة بداخله، فبيدأ بالانجذاب لها ولا يقتصر وقت الترفيه على الألعاب غير المفيدة فقط.

جهاز ولي الأمر اختيار block وتحديد الساعة ثم schedule للتحكم بالوقت والأيام متى يبدأ ومتى ينتهي.

ملاحظة: إذا كان هناك أكثر من طفل يمتلكون أجهزة يتم اختيار Add من جهاز ولي الأمر وإضافة اسم الطفل بنفس الخطوات السابقة.

يمكن حجب المواقع والأفلام الغير مرغوب بها من خلال الإعدادات العامة للجهاز باختيار الإعدادات واختيار القيود واختيار رمز يضعه ولي الأمر باستخدام الخطوات التالية:

- التصنيفات تغيير الولايات المتحدة الى السعودية.

الموسيقى وبودكاست تغيير من فاضح الى إغلاق (غير فاضح).

الأفلام اختيار PG13 ثم تعطيل الخيارات الباقية.

لبرامج التلفاز اختيار عدم السماح.

لتغيير المحتوى "جنسي صريح" وإغلاق المحتوى.

للتطبيقات تحديد سن الطفل 12 سنة.



شارك طفلك في رسم لوحة، فالرسم يخرج طاقة الطفل الكامنة كما يساعده على التخيل والإبداع، أو اشتراكه في مركز ثقافي لممارسة الهواية التي يفضلها، مع إمداده بالأدوات والتشجيع المستمر.

بناء الحصانة في نفس الطفل دائماً، ليباعد ذاتياً عن كل ما هو ضار ومخالف للعادات والتقاليد.

لا يجب أن يتم منع الطفل نهائياً من استخدام الأجهزة الإلكترونية حتى لا يصبح الطفل بعيداً عن عالمه وأبناء جيله ومتأخر فكرياً عنهم.

يجب على أولياء الأمور أن لا يسمحوا للأطفال الأقل من ثلاث سنوات بممارسة هذه الألعاب، وتوجيههم نحو الألعاب التي تناسب سنهم من الألعاب التقليدية.



S سرية: تجنب الإفصاح عن أي معلومات شخصية



M مقابلة: لا تقابل شخصاً لا تعرفه من خلال الإنترنت



الألعاب الإلكترونية

علم أبنائك خمس أساسيات ذكية Smart



A القبول: لا تقبل رسائل وصور من أشخاص لا تعرفهم



T تواصل: أعلم والديك أو ولي أمرك إذا انتابك شعور بالقلق تجاه شيء ما أو شخص لا تعرفه



R راقب: قد يخبرك الشخص بمعلومات خاطئة عن نفسه والمعلومات عبر الإنترنت مضللة

ختاما .. اتصل لنساعدك

لذلك تهدف مبادرة «وعيك يحمينا» إلى توعية الأسرة من مخاطر الجرائم المعلوماتية، والتعريف بهذه الجرائم عن طريق شرحها وتحليلها للناس وأهدافها، وبيان وسائل وطرق الوقاية منها، وزيادة الرصيد المعرفي ومدى تأثيرها على الفرد والمجتمع.

المواقع التي يمكن الرجوع لها لمعرفة المزيد:

برنامج التعاملات الإلكترونية الحكومية
yesser.gov.sa

الإدارة العامة لتقنية المعلومات - جامعة الملك خالد
it.kku.edu.sa

أمن المعلومات - جامعة الملك خالد
infosec.kku.edu.sa

النيابة العامة

pp.gov.sa

هيئة الاتصالات وتقنية المعلومات
citc.gov.sa

مدينة الملك عبد العزيز للعلوم والتقنية
kacst.edu.sa/arb

في الختام نذكر أنه في حالة تعرضك للمضايقة أو التهديد لجريمة إلكترونية من قبل الآخرين فلا تتردد في المسارعة في إبلاغ الجهات الأمنية من خلال نظام أبشر www.moi.gov.sa ..

وقد صدر نظام مكافحة الجرائم المعلوماتية بقرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/17 وتاريخ 1428/3/8هـ وتحقيقاً لقرار مجلس الوزراء رقم (81) وتاريخ 1430/3/19هـ البند الخامس الفقرة الثالثة، القاضي بتوجيه كل جهة حكومية بإعداد برامج توعية للمستخدمين في مجال أمن المعلومات. وقامت الإدارة العامة لتقنية المعلومات بجامعة الملك خالد <http://it.kku.edu.sa> بمبادرة «وعيك يحمينا» التي تتماشى مع إرشادات هيئة الاتصالات وتقنية المعلومات www.citc.gov.sa وتقديم نصائح مهمة للحماية من التصيد الإلكتروني Phishing وشرح طريقة إنشاء كلمة مرور «قوية» ويسهل عليك تذكرها.



اعداد : أ.عائشة موسى محمد الشهراني
تدقيق : عبداللطيف القحطاني - علي الضمراتي

إشراف عام الدكتور سالم فائز العلياني - المشرف العام لتقنية المعلومات



الجرائم المعلوماتية
#وعيك_يحمينا



الالعاب الإلكترونية

الديني

الإلكترونية

أساليب مكافحة
تعريف

أنواع

(بعضها خطر تهدد حياة أطفالنا)
تصنيف

أضرار

حسب النوع

الجانب الصحي

الإلكترونية

حسب الأهداف الجانب السلوكي والأمني

حسب الدوافع

الجرائم المعلوماتية

مسمياتها
حسب التنفيذ

حسب النوع

تعريف

أهم طرق أسباب وخصائصها

دور الآباء

فوائد الألعاب
التنمر الإلكتروني

طول مقترحة

عوامل مؤثرة

حرب على القيم

الأعراض

الأضرار



#وعيلك - يحمينا