2020-2021

مدرسة الكمال الأمريكية الدولية – العزرة
Al Kamal American International School – Al Azra

IT Policy & Technology Rules AR .

Mr.Osama Yasser

It Administrator

- التهديد الإلكتروني 4
- التهديدالإلكتروني 6
- مؤشرات التهديد الإلكترونى 7
- نصائح لإدارة التهديد الإلكتروني 8
- تبادل المحتويات الجنسية:(SEXTING) 11
- الإتصال الجنسي الغير مرغوب فية 13
- الأمن الإلكترونى و التجارة الإلكترونية 17
- •النصائح الأساسية للآباء والأمهات 17
- ما يجب القيام به قبل إجراء المعاملات التجارية عبر الإنترنت: 18
- ما الذي يمكنك القيام به لحماية نفسك؟ 19
- النصائح التالية يمكن أن تساعد على ضمان معاملة آمنة على الانترنت 19
- تحديد القضايا عند إجراء المعاملات التجارية عبر الإنترنت 20
- •لاحتيال الأكثر شيوعا على بطاقات الائتمان 20
- حماية جهاز الكمبيوتر الخاص بك 22
- •الفيروسات والديدان وأحصنة طروادة 22
- الحماية ضد المخاطر الأمنية للإنترنت 23
- •الجدران النارية(FIREWALLS) 23
- التحميل الأكثر أمانا للملفات والموسيقى والفيديو 24
- SECURING A WIRELESS NETWORK 27
- حماية المعلومات الشخصية 28
- السمعة الرقمية 31
- سرقة الهوية 33
- الشبكات الاجتماعية الأكثر أمانا 35
- المحتوى غير اللائق 40
- •كيفية وصول الأطفال إلى المحتويات غير اللائقة؟ 40
- •ما هي المحتويات المحظورة عبر الإنترنت؟ 40
- الإفراط في استخدام الإنترنت 44
- الهواتف المحمولة 47
- الشبكات الإجتماعية والأصدقاء على الإنترنت 52
- الألعاب على الإنترنت 53

AKAIS-AZRA

AKAIS-AZRA

التهديد الإلكتروني

ما هو التهديد الإلكتروني؟

التهديد الالكتروني هو عندما يستخدم شخص التكنولوجيا (مثل الانترنت أو الهاتف المحمول) للتهديد أو الضغط على الآخرين.

أن تكون ضحية التهديد الالكتروني شيء مؤلم خصوصا للأطفال الصغار الذين لا يعلمون من يقوم بتهديدهم، يتضمن التهديد الإلكتروني إرسال رسائل نصية قبيحة أو رسائل بالبريد الإلكتروني أو إنشاء مجموعة هدفها الكراهية على مواقع التواصل الإجتماعي.

ماذا يمكنك أن تفعل بصفتك مدرس؟

1. **فهم الأدوات:** يكون على دراية بآليات الإبلاغ عن المواقع والخدمات المختلفة حتى تتمكن من دعم ومساعدة تلاميذك في عمل تقرير بالحالة.
2. **مناقشة التهديد الإلكتروني:** كن إستباقياً في مناقشة التهديد الإلكتروني مع تلاميذك. كيف يحدث، لماذا يحدث، والنتائج المترتبة على مثل هذا السلوك.
3. **معرف الشخص المناسب لتقديم البلاغ:** تأكد من أنك على بينة من الأشخاص المسؤولين في مدرستك لتبليغهم في حالة التهديد الإلكتروني.

ما هي النصائح التي يمكن إعطائها لطلابك

1. **عدم الرد:** معظم الوقت المتنمر يحاول إغاظتك ويبحث عن رد فعل لدعوتك بأسماء سيئة، قم بتذكير الطلاب بعدم الرد على التهديد الالكتروني واذا لم يفعلوا فإنهم يعطون المتنمر ما يريد.
2. **حفظ الأدلة:** تشجيع الطلاب على حفظ الأدلة كالرسائل النصية ورسائل البريد الإلكتروني التي يتلقونها، وهذا دليل يقدمونه عند التبليغ عن التهديد الإلكتروني.
3. **أخبر شخص بالغ تثق به:** تشجيع الطلاب على تبليغ شخص بالغ يثقون به بالتهديد الإلكتروني، والقيام بذلك بأسرع وقت ممكن لتقليل أضرار التهديد الإلكتروني.

أفضل نصائح للآباء للإستخدام الآمن على الإنترنت

الآباء

يلعب الآباء دورا حاسما في ضمان تجربة آمنة وإيجابية لأبنائهم خلال تعاملهم مع الانترنت ولكن من أجل القيام بذلك، يجب على الآباء أن يكونوا على علم كيف يستخدم الأبناء للإنترنت. ويرتبط الشباب اليوم في العديد من الطرق المختلفة، ولكن أساس تجربتهم عبر الإنترنت يبدأ عادة مع التكنولوجيا المكتسبة لديهم في المنزل. برنامج سايبر سى C3 يشجع الآباء على وضع قواعد ورصد استخدام ومناقشة ممارسات السلامة مع ابنائهم باعتبارها أفضل وسيلة لمساعدتهم على أن يصبحوا فى وضع آمن ومدركين لإستخدام وسائل الاعلام.

أفضل نصائح للآباء للإستخدام الآمن على الإنترنت

1. تحدث مع ابنك عن السلامة على الإنترنت عند بدأ إستخدامه / إستخدامها الإنترنت.
2. قم بممارسة المراجعة المناسبة حسب الأعمار، لمنع ومراقبة البرامج على كافة الأجهزة التي تدعم خدمة الانترنت التي يستخدمها طفلك، بما في ذلك الهواتف وأجهزة الكمبيوتر المحمولة اللاسلكية وألعاب الفيديو.
3. ضع مقدارا للوقت المسموح به لأبنائك بإستخدام الإنترنت وتعرف على المواقع الأكثر زيارة لطفلك على شبكة الإنترنت. وحاول التعرف بنفسك عن أنشطة أبنائك على الانترنت.
4. إشرح لأبنائك أنه يجب عدم إعطاء معلومات شخصية عبر الإنترنت على سبيل المثال، ينبغي أن يفهم ابنك أنه لا يجوز إعطاء معلومات مفصلة حول مكان تواجده / تواجدها.
5. تأكد من أن ابنك يدرك دائما أن لقاءه وجها لوجه بأحد الذين تعرف عليهم على الانترنت يتم بموافقتك.
6. اشرح لطفلك أنه ينبغي عدم تبادل كلمات المرور(السر) الخاصة بهم مع أي شخص بما في ذلك الأصدقاء.
7. ضع ملاحظاتك على استخدام طفلك للهاتف المحمول وقم بإستعراض الرسائل النصية وغيرها من وقت لآخر بما في ذلك أي صور قام بإرسالها أو إستلامها.
8. تابع بنفسك أحدث التهديدات التي تواجه الاطفال على الانترنت (على سبيل المثال، التهديد الإكترونى ، وإثارة الغرائز الجنسية وتبادل الصور الفاضحة ، الخ.)

التهديدالإلكتروني

التهديد الإلكتروني

التهديد الإلكتروني للشباب هو نتيجة لاستمرار المضايقة وسوء المعاملة والسخرية عن طريق:

1. رسائل البريد الإلكتروني
2. الشبكات الاجتماعية
3. الرسائل النصية
4. الهواتف المحمولة
5. الفيديو
6. المدونات
7. أي شكل آخر من أشكال الاتصال الإلكتروني

هذا السلوك المتكرر والعدائى يمكن أن يكون مدفوعا من قبل أفراد أو جماعات.

يشمل التهديد الإلكتروني الأنشطة التالية

1. نشر الرسائل افتراء على مواقع الشبكات الاجتماعية
2. نشر الشائعات عبر الإنترنت
3. إستثناء شخص من جماعة على الانترنت
4. إرسال الرسائل غير المرغوب فيها من عبر الرسائل والنصوص الفورية أو البريد الإلكتروني

يحدث هذا النوع من الإحتيال عادة في أي مكان أو في أي وقت بحيث لم يعد الضحية يشعر بالأمان حتى في وطنه، ويسبب هذا بدوره ضيقا عظيما وأثرا سلبيا تجاه إحترام الشخص لذاته وثقته بنفسه.

إذا تركت لحالها ولم يتم مراجعتها، يمكن أن تؤدي الآثار السلبية للتهديد الإكترونى الى درجات سيئة، وعواطف لولبية ، واكتئاب، والغياب المدرسي وفي بعض الحالات الانتحار. للأسف يحدث التهديد الإلكترونى عالميا وحاليا فإن حالاته فى تزايد وارتفاع!

تأثير التهديد الإلكتروني

يمكن أن يحدث التهديد الإلكترونى لأي شخص، وليس فقط الأطفال الضعفاء والشباب. ومع ذلك، فإن حدوث التهديد الإلكترونى أكثر إحتمالا للأطفال حتى فى حال خروجهم من شبكة الإنترنت.

كما هو فى حال خروجهم من شبكة الإنترنت يمكن أن يكون للتهديد الإلكترونى عواقب طويلة الأمد يحتاج خلالها الأطفال إلى الدعم.

مؤشرات التهديد الإلكترونى

مؤشرات التهديد الإلكترونى

تشمل المؤشرات الدالة على تأثر طفلك بالتهديد الإلكترونى تغييرات في سلوكهم العام أو المزاج، وانخفاض في الصحة البدنية، والتغيرات تجاه مجموعات الأصدقاء ، والتغيرات في أنماط النوم أو التغيب عن المدرسة أو النوادي.

فى حال ظهور أي من هذه المؤشرات على طفلك ، خاصة إذا هذا السلوك جديد وخارج عن طابعهم العادى ، حاول التحدث معهم عن مخاوفك وراقب سلوكهم على الانترنت وخارجه عن كثب. وحافظ على معرفة تواصلهم وعدم تواصلهم عبر الانترنت مع الأصدقاء والعائلة على حد سواء.

AKAIS-AZ

نصائح لإدارة التهديد الإلكتروني

نصائح لإدارة التهديد الإلكتروني

بأدناه نقدم النصائح العملية التالية لمساعدة الآباء فى إدارة مخاطر التهديد الإلكترونى مع الأطفال صغار السن ، الأطفال الأكبر سنا والمراهقين.

الأطفال الصغار:

التهديد الإلكترونى أقل شيوعا بين الأطفال الصغار مع احتمال تورطهم فيه مع تقدم العمر.

يمكن أن يكون للتهديد الإلكترونى نتائج أكاديمية واجتماعية ونفسية سلبية لدى الأطفال، لذا فإن توفير الدعم للأطفال المتورطين في التهديد الإلكترونى أمر بالغ الأهمية.

نصائح السلامة العامة للانترنت هي نقطة انطلاق جيدة لمساعدة الأطفال الصغار على تطوير آداب الإنترنت المناسبة لتعلم والاستجابات الملائمة لسلوكيات التهديد الإلكترونى. وتعتبر النصائح التالية ذات أهمية خاصة:

1. في هذا العمر ينبغي مراقبة استخدام الأطفال الإنترنت عن كثب. للمساعدة في ذلك يجب محاولة الحفاظ على جهاز الكمبيوتر في مكان مشترك أو مرئ للجميع بالمنزل.
2. حافظ على وضع طفلك متصلا كان أوغير متصل بالأصدقاء والعائلة الذين يثقون به عبر الانترنت ، مما يساعد على حمايته من النتائج السلبية المحتملة.
3. ساعد طفلك على فهم أن ما يقولونه ويفعلونه على الانترنت هو المهم. شجع طفلك على استخدام نفس الخلق، والتواصل مع الآخرين في نفس الطريق تماما كما يفعلون في حال عدم إتصالهم بالإنترنت.
4. تقديم النصح لطفلك عدم الرد على أي رسائل سلبية والإبلاغ عن أي رسائل سلبية تصل لك أو شخص آخر موثوق به.
5. إذا كان لدى طفلك كلمات مرور يستخدمها لأنشطة الإنترنت إنصحه بعدم تبادلها مع أصدقائه ، حيث أن تلك الصداقات قد لا تستمر في هذه السن أما الأصدقاء السابقين فيمكنهم إساءة استخدام كلمات المرور والقيام بتهديدات إلكترونية.
6. إذا تورط طفلك في تهديدات إلكترونية وبدأت عليه علامات الأسى أو أظهر تغيرات في سلوكه أو مزاجه فمن المستحسن التعامل مع الموضوع بمهنية،
7. يمكن أن يكون لرفقاء طفلك القدرة على توفير الدعم والتوجيه.
8. إذا كان هناك تهديد لسلامة طفلك يمكن أن تساعد الشرطة فى تقديم الدعم اللازم.

الأطفال الأكبر سنا :

تحدث التهديدات الإلكترونية أكثر شيوعا بين الأطفال الأكبر سنا والمراهقين.

يمكن أن تكون للتهديدات الإلكترونية نتائج أكاديمية واجتماعية ونفسية سلبية ، لذا فإن توفير الدعم للأطفال والشباب المتورطين فى التهديدات الإلكترونية يعتبر أمر بالغ الأهمية.

مساعدة الأطفال على التعامل مع السلوك السلبي عبر الإنترنت والاحتفاظ بتوصيلهم عبر الانترنت بالأصدقاء والعائلة الذين يثقون بهم حيث تعتبر تلك التدابير هامة لحمايتهم من النتائج السلبية المحتملة. النصائح التالية ذات أهمية خاصة:

1. ينبغي مراقبة طفلك عن كثب في هذا العمر خلال استخدامه الإنترنت. وللمساعدة في هذا يجب محاولة الحفاظ على جهاز الكمبيوتر في مكان مشترك أو أماكن مرئية في المنزل.
2. تحدث مع طفلك عن التهديدات الإلكترونية قبل وقوعها. ضع استراتيجيات لمعالجة التهديدات الإلكترونية التي ترى أنها معقولة ، لذا يعرف طفلك ما يمكن توقعه إذا رفعوا لك تقرير حول المخاوف أو لأى شخص آخر موثوق به.
3. طمأنة طفلك بأنك لن تمنع وصوله إلى شبكة الإنترنت إذا تم إبلاغك عن مخاوف بشأن التهديدات الإلكترونية. وحاول مساعدته على البقاء متصلا عبر الإنترنت أوغير متصل بالأسرة والأصدقاء.
4. ساعد طفلك لمنع أي شخص يرسل له محتويات هجومية. تسمح معظم خدمات الشبكات الاجتماعية للمستخدمين منع والإبلاغ عن أى شخص يتصرف بشكل غير لائق.
5. تشجيع الأطفال على دعم أصدقائهم ومساندتهم والإبلاغ عن الأصدقاء الذين قد تكون لهم علاقة بالتهديد الإلكترونى.
6. ساعد طفلك على تطوير المهارات التي يحتاجها للتفاعل بأمان واحترام عبر الإنترنت. وقم بتوجيه أنشطته عبر الإنترنت ومساعدته على تعلم كيفية التواصل بشكل مناسب مع الأصدقاء والعائلة.
7. تقديم النصح لطفلك بعدم تبادل كلمة المرور الخاصة بهم مع الأصدقاء ، نظرا لأن عمر الصداقات قد تكون قصيرة فى هذا العمر والأصدقاء السابقين يمكنهم إساءة استخدام كلمات المرور من خلال عمل التهديدات الإلكترونية.
8. فى حال تورط طفلك في التهديدات الإلكترونية ويبدو عليه القلق أو يظهر تغيرات في السلوك أو المزاج قد يكون من المستحسن الحصول على الدعم المهنى.
9. إذا كان هناك تهديد على سلامة طفلك فإن الشرطة يمكن أن تساعد في الحالات الحرجة التى تهدد الحياة والوقت.

المراهقين

تحدث التهديدات الإلكترونية أكثر شيوعا بين الأطفال الأكبر سنا والمراهقين.

يمكن أن تكون للتهديدات الإلكترونية نتائج أكاديمية واجتماعية ونفسية سلبية ، لذا فإن توفير الدعم للأطفال والشباب المتورطين فى التهديدات الإلكترونية يعتبر أمر بالغ الأهمية.

يعتبر العديد من الشباب أن حياتهم على الانترنت هى جزء مهم من هويتهم الاجتماعية. ويخشى العديد من المراهقين أن الآباء قد يقدمون على قطع الإنترنت منهم وعزلهم من أصدقائهم كحل لمواجهة التهديدات الإلكترونية، مما يمنع بعض المراهقين من الإبلاغ عن قضايا التهديدات الإلكترونية . ويعتقد بعض المراهقين أيضا أن الآباء سيجعلون التهديدات الإلكترونية أكثر سوءا. لذا تعتبر النصائح التالية ذات أهمية خاصة:

1. تحدث مع ابنك المراهق حول التهديدات الإلكترونية قبل وقوعها ، وضع استراتيجيات لمعالجة التهديدات الإلكترونية المعروفة لديك ، مما يجعل طفلك يدرك ما يمكن توقعه من مخاوف فى حال تبليغك الأمر أو تبليغ شخص آخر موثوق به. ويمكن طمأنتهم بأنك سوف تقدم لهم الدعم اللازم ولن تفصل بينها وبين العالم على شبكة الإنترنت.
2. قم بتشجيع ابنك المراهق لأن يخبرك أو يخبر أى شخص عاقل آخر موثوق به إذا كان يتلقي أو يستمع لرسائل سلبية، أو أنهم مبعدين من قبل الآخرين. مساعدتهم على البقاء على تواصل مع الأصدقاء والعائلة الموثوق بهم على الانترنت فى حال الإتصال وغيره. وهذا تدبير وقائي مهم ضد النتائج السلبية المحتملة من التهديدات الإلكترونية.
3. تقديم النصح والإرشاد للأبناء فى سن المراهقة بعدم الرد على أي رسائل سلبية ولكن بإمكانهم حفظ الرسائل وتفاصيل الراسلين. قد ترغب في حفظ الرسائل لابنك المراهق بحيث لا يقوم بقراءتها ويشعر بالقلق.
4. يمكنك أن تساعد ابنك المراهق للإبلاغ عن أي مخاوف لمدير الخدمة المستخدمة، بما في ذلك للهاتف الجوال) إذا كان الأمر يتضمن SMS)، ومسؤول الموقع (إذا تم إشراك الشبكات الاجتماعية أو خدمات الدردشة)، أو مزود خدمة الإنترنت.
5. فهم سياسة مدرستك حول التهديدات الإلكترونية، هل لديهم سياسة وما هي النتيجة المحتملة لشكوى عن التهديدات الإلكترونية إذا كان الأمر يتضمن طالب آخر.
6. قم بتشجيع ابنك المراهق لدعم ومساندة أصدقائه والإبلاغ عن الأصدقاء الذين قد تكون لهم علاقة بالتهديدات الإلكترونية.
7. قم بتقديم النصح لطفلك بأن لا يتبادل كلمة المرور الخاصة به مع أصدقائه، لأن فترة الصداقات قد تكون قصيرة مع أصدقاء عصره السابق والأصدقاء القدامى قد يسيئون استخدام كلمات المرور خلال التهديدات الإلكترونية.
8. إذا تورط طفلك في التهديدات الإلكترونية وبدأ عليه القلق والأسى أو ظهرت عليه تغييرات في السلوك أو المزاج قد يكون من المستحسن للحصول على دعم مهنى.
9. إذا كان هناك تهديد على سلامة طفلك يمكن أن تساعد الشرطة تجاه ذلك خاصة الحالات الحرجة التى تهدد الحياة والوقت.

تبادل المحتويات الجنسية:(SEXTING)

تبادل المحتويات الجنسية:(sexting)

ويشار عموما لمتبادل المحتويات الجنسية على أنه شخص بالغ في سن المراهقة أو الشباب تقاسم صور عارية أو بذيئة النص على الهواتف المحمولة أو من خلال الدردشة على شبكة الإنترنت. يمكن أن تكون لهذه الممارسة عواقب قانونية وفسيولوجية إضافة للضرر المهنى والأسرى على المدى الطويل.

ممارسة تبادل المحتويات الجنسية عمل غير قانوني! لا تأخذ أو ترسل صورا عارية أو إيحاءات جنسية لنفسك أو لأي شخص آخر بما في ذلك الرسائل النصية التى تحمل إيحاءات جنسية. من خلال ذلك أو المرور على صور شخص آخر أو رسائل تصبح عرضة لخطر الإتهام بإنتاج المواد الإباحية. وإذا إحتفظت بهذه الرسائل على هاتفك الخليوي الخاص بك أو جهاز الكمبيوتر فإنك ستتحمل تهمة حيازة المواد الإباحية للأطفال. إذا تم إرسال الرسائل عبر حدود الدولة يصبح ذلك جريمة فدرالية تُعرض لعقوبات أكبر في المحكمة.

هناك أيضا آثار غير قانونية لمثل ذلك السلوك. الضرر العاطفي لسمعة سيدة هو أمر شائع. وهناك صداقات لا تدوم كثيرا لذا فإن تبادل الصور والنصوص الحميمة مع مثل ذلك الصديق أمر ربما يعرضك للخطر لعدم تمكنك من السيطرة على معلوماتك فى حال إنتهاء تلك الصداقة ،ويمكن إنتقال هذه الرسائل وتبادلها مع العديد من الناس أو فى حال وضعت على شبكة الانترنت بمثابة سجل دائم. فبمجرد حدوث ذلك يصبح من المستحيل عمليا التراجع عن الأضرار التي لحقت بسمعة أو إزالة كل آثار البيانات الشخصية.

هناك أسباب كثيرة لهذا السلوك المعروف بتبادل المحتويات الجنسية (sexting) وعادة ما يكون نتيجة لضغط الأقران (شكل من أشكال الهجمات الإلكترونية) أو الضغط من صديق / صديقة. في بعض الأحيان يمكن أن يكون سلوك اندفاعي متهور، بغرض المزح أو الإبتزاز وتعتبر تلك المشاركة فكرة سلوكية سيئة.

الآباء بحاجة إلى التحدث مع أطفالهم حول تبادل المحتويات الجنسية (sexting) لتحديد ما يعرف طفلهما عن ذلك، وكذلك لاطلاعهم على النتائج المحتملة لهذا النوع من تقاسم المعلومات الحميمة. الآباء بحاجة إلى التعبير عن مشاعرهم بطريقة حوارية غير تصادمية. ويمكن للحوار في إتجاهين أن يقطع شوطا طويلا نحو مساعدة أطفالك على فهم كيفية تقليل المخاطر القانونية والاجتماعية ومخاطر السمعه.

كن حذرا عند إستخدام وسائل الإعلام الرقمية وتبادل المعلومات. ليس الناس دائما على ما يبدو لك وفي بعض الأحيان فالتغيرات في الظروف يمكن أن تؤدي إلى نتائج محرجة وضارة. وتصبح الحماية فى التفكير النقدي حول ما نقوم تحميله هو أفضل حماية.

أولياء الأمور

1. إذا أرسل أطفالك أي صور عارية لأنفسهم، تأكد من أنهم أوقفوها على الفور ، وأشرح لهم أنهم سيصبحون عرضة لخطر إنتاج وتوزيع المواد الإباحية عنهم . وإذا تحصلوا على صور عارية، تأكد من أنهم لم يرسلوها إلى أي شخص آخر.

2. وفي كلتا الحالتين، فإن الشيء التالي الأكثر أهمية هو أن يكون هناك نقاش جيد. بهدوء، كن متعاونا وحاول التعرف بقدر ما تستطيع عن الحالة. على سبيل المثال، حاول معرفة ما إذا كان ذلك السلوك متهورا، أو أنه "رومانسية" سن المراهقة ، أو أنه شكل من أشكال التحرش.
3. محاولة التحدث مع المراهقين والآباء المعنيين، بناء على ما علمته.
4. ينصح بعض الخبراء بإرسال الصورة للشرطة المحلية، ولكن عليك معرفة أنه بينما تحاول حماية طفلك، ربما تجرم طفل آخر – وربما يكون طفلك نفسه. لهذا فإنه من الأفضل التحدث أولا مع الأطفال والآباء والأمهات. إذا كان الأمر ينطوي عن خبث أو قصد جنائي، قد يتطلب الأمر إستشارة محام، والشرطة، أو غيرهم من خبراء القانون في ولايتكم، ولكن كن على بينة من إمكانية أن تقدم المواد الإباحية للأطفال والتهم الموجهة ضد أي شخص متورط.

الشباب

1. فى حال إستلامك صورة إباحية sexting على هاتفك، لا ترسلها إلى أي شخص آخر (حيث يمكن إعتبارها توزيع مواد إباحية).
2. تحدث مع أحد الوالدين أو شخص بالغ موثوق به. إسرد لهم القصة الكاملة لأنهم يعرفون كيفية دعمك. ولا تفزع إذا قرر ذلك الشخص الحديث مع آباء الأشخاص المشاركين الآخرين – التي ربما تكون أفضل وسيلة لحمايتكم من الدخول في مشاكل خطيرة.
3. إذا كانت الصورة مرسلة من صديق أو شخص تعرفه، فربما يحتاج ذلك الصديق للتوجيهات حتى يدرك أن التعامل فى الصور الإباحية sexting مخالف للقانون. لذا تكون قد قدمت له خدمة كبيرة بسبب نصحه قبل تدخل الشرطة.
4. فى حال إستمرار إستلام الصور يتحتم عليك مرافقة أحد والديك والتحدث مع والدي صديقك، وإدارة المدرسة أو الشرطة.

كيف يمكنني التعامل معها؟

1. فكر قبل أن تحفظها أنها يمكن أن تكون على الانترنت إلى الأبد.
2. إضبط خصوصيتك حيث أن بعض الأشياء يجب أن لا تكون مشتركة.
3. قم بإدارة الصور الفوتوغرافية أو الصور ذات الكلمات الدلالية مع اسمك.
4. حذف أي صورة إباحية sexting تتلقاها ولا ترسل أي شيء منها.
5. إدرس الآخرين قبل أن ترسل لهم أو تستلم منهم صورة.
6. تحدث إلى شخص بالغ تثق به.

الإتصال الجنسي الغير مرغوب فية

الإتصال الجنسي غير المرغوب فيه

يمكن للأطفال والشباب التواصل مع أشخاص لا يعرفونهم أو لم تكن لديهم سابق معرفة بهم وذلك عبر الإنترنت. في حين يمكن أن يكون الإتصال بأشخاص جدد مثيرا ، ويوفر إمكانية عدم الكشف عن الهويه التي توفرها شبكة الإنترنت وتسمح هذه الاتصالات الجديدة لتغطية هوياتهم الحقيقية. على سبيل المثال، يمكن القول أن فتاة فى عمر الـ 10 عام يمكنها أن تتعامل على أساس أنها رجل فى الـ40 سنة من العمر. عدم الكشف عن الهويه هذا يعني أن الطلب الجنسي والإستمالة يمكن أن يحدث على الانترنت وبمخاطر كبيرة.

الطلب الجنسي هو المكان الذي يطلب فيه شخص ما الدخول في محادثة جنسية أو نشاط أو إرسال صورة جنسية فاضحة أو معلومات. الاستمالة وشراء الأطفال عبر شبكة الانترنت هو عمل غير قانوني من شخص بالغ أو أشخاص بالغين يقومون بالاتصال عبر الإنترنت على طفل دون السادسة عشرة من العمر بهدف تسهيل إقامة علاقة جنسية.

مخاطر الإتصال الجنسي غير المرغوب فيه:

يمكن للأطفال والشباب زيادة مخاطر الإتصال الجنسي غير المرغوب فيه من خلال الأساليب التالية.

1. نشر الصور والرسائل الاستفزازية أو باستخدام أسماء إستفزازية على الشاشة. العديد من الأطفال يعتقدون أنهم أصبحوا ناضجين عند إستخدام اللغة المضحكة والمثيرة جنسيا والصور ولا يعتبرون أنها قد تجذب بعض الناس غير مرغوب فيهم على المعلومات الخاصة بهم.
2. نشر معلومات شخصية على مواقع متاحة للجمهور. على سبيل المثال، إذا قام الأطفال بنشر أسمائهم وعناوينهم أو مكان المدرسة / العمل على موقع شبكة الانترنت والشبكات الاجتماعية دون إستخدام ضوابط الخصوصية، يمكن أن يظهر بذلك لكثير من الناس لم يعرفوه من قبل. الكثير من الأطفال ليسوا على بينة من المخاطر في مشاركة معلوماتهم الشخصية علنا، لذلك يسعدهم أن يجعلوا كل ما لديهم من معلومات مرئية.
3. قبول الإتصالات أو "الأصدقاء" غير المعروفين على مواقع الشبكات الاجتماعية أو مواقع الألعاب، يسمح للأشخاص الغرباء من الوصول إلى معلوماتهم الشخصية وصورهم. قد تكون هذه الاتصالات غير مؤذية، ولكنها يمكن أيضا أن تؤدى إلى إقامة علاقة مع طفل لأغراض جنسية.
4. الإنخراط في الشبكات الاجتماعية أو مواقع الألعاب المصممة للمراهقين أو الكبار، يمكن أن يزيد من إحتمالات الإتصال بهم من قبل المراهقين الأكبر سنا أو البالغين لأغراض جنسية.

ونقدم النصائح العملية التالية لمساعدة الآباء إدارة مخاطر الاتصال الجنسي غير المرغوب فيه مع أطفال صغار، والأطفال الأكبر سنا والمراهقين.

صغار الأطفال

يقيم بعض البالغين علاقات صداقة مع الأطفال على الإنترنت لأغراض جنسية وهذا ما يسمى بالاستمالة وهو سلوك غير قانوني وينبغي إبلاغ الشرطة بذلك. في كثير من الحالات يمكن للشرطة مقاضاة البالغين الذين يسعون وراء الأطفال لأغراض جنسية حتى لو لم يقم إتصال وجها لوجه مع الطفل.

صغار الأطفال عادة لا يستخدمون المواقع التي تمكن التفاعل المباشر مع الآخرين من دون رقابة. النصائح التالية سوف تساعد على مراقبة الذين يمكنهم الاتصال بطفلك عبر الإنترنت واستجابتهم للإتصال غير اللائق.

1. يجب مراقبة استخدام الأطفال للإنترنت عن كثب في هذا العمر. للمساعدة في هذا يجب محاولة الحفاظ على جهاز الكمبيوتر في مكان مشترك أو مرئى في المنزل.
2. كن على علم بطفلك وكيفية إيستخدمه الإنترنت،وشاركهم فى عملية الإستكشاف واستكشف معهم مرجعية القائمة المفضلة لك وأشرح لهم كيفية الوصول إلى هذه القائمة.
3. إذا كان طفلك في سن حيث كنت قد بدأت توعيتهم وتعريفهم بالغرباء وحماية أجسامهم، قد يكون من المفيد توسيع تلك الدروس لتغطية المعرفة بالإنترنت. العمر المناسب لهذا التعليم تحدده أنت وعائلتك.
4. إذا كنت مستمرا فى تثقيف طفلك بالحديث عن جسمه وكيفية الحفاظ عليه آمنا قد يكون من المفيد وضع قاعدة حول ما هو مقبول وما هو غير مقبول لمناقشته على الكمبيوتر وما ينبغي الإبلاغ عنه لك أو لشخص آخر بالغ موثوق به. على سبيل المثال، هناك قاعدة واحدة "إذا سألك شخص عن ملابسك الداخلية أو" أجزاء خاصة "عندما كنت على الكمبيوتر ، هنا يمكنك إستدعاء أمك للتأكد من أن ما يقولونه صحيحا.'
5. هناك قاعدة أخرى جيدة لطفلك وهو أن يبلغ عن أي شيء يجعله يشعر بعدم الراحة أو مضحك لهم.
6. إذا أظهر طفلك تغييرات في السلوك أو المزاج التي تشمل بما في ذلك السلوكيات الجنسية زيادة أو نقصان، تماسك أو انسحاب قم باستكشاف مخاوفك معهم وإذا لزم الأمر إطلب الدعم الفني.

كبار الأطفال

يقيم بعض البالغين علاقات صداقة مع الأطفال على الإنترنت لأغراض جنسية وهذا ما يسمى بالاستمالة وهو سلوك غير قانوني وينبغي إبلاغ الشرطة بذلك. في كثير من الحالات يمكن للشرطة مقاضاة البالغين الذين يسعون وراء الأطفال لأغراض جنسية حتى لو لم يقم إتصال وجها لوجه مع الطفل.

كبار الأطفال عادة تكون لديهم رغبة أكبر فى إستخدام مواقع الويب والألعاب التي تمكن التفاعل المباشر مع الآخرين من الكبار والصغار.

النصائح التالية سوف تساعد على حماية طفلك من الأتصال الجنسي غير المرغوب فيه.

1. يجب مراقبة استخدام الأطفال للإنترنت عن كثب في هذا العمر. للمساعدة في هذا يجب محاولة الحفاظ على جهاز الكمبيوتر في مكان مشترك أو مرئى في المنزل.
2. استكشف المواقع المفضلة طفلك. بشكل عام فإنه من المفيد أن تنظر فيما إذا كنت مرتاحا مع المحتوى من المواقع وإمكانية الاتصال مع الآخرين بما في ذلك المراهقين والبالغين. هل طفلك مستعد اجتماعيا للاتصال بالغرباء ؟
3. إذا وافقت لطفلك بالوصول إلى المواقع التي تسمح بالاتصال المباشر مع الآخرين في هذه الحالة فكر فى إنشاء قواعد حول كمية المعلومات التي يمكن أن توفرها، بما في ذلك عدم توفير المعلومات الخاصة باللقب أو العنوان أو المدرسة، وعدم تحميل أو إرسال الرسائل النصية أو الصور أو مقاطع فيديو دون إذن الوالدين.
4. إذا كان طفلك في سن حيث بدأت توعيته وتوجيهه حول الغرباء وحماية الجسم، قد يكون من المفيد أيضا توسيع هذه الدروس لتشمل الحديث حول الإتصال عبر الإنترنت.
5. تختلف السن العمرية المناسبة لهذا التعليم وهو قرار خاص بالنسبة لك ولعائلتك.
6. قد يكون من المفيد وضع قاعدة حول ما هو مقبول وما هو غير مقبول لمناقشته على الكمبيوتر وماذا ينبغي الإبلاغ عنه لك أو لشخص بالغ موثوق به. على سبيل المثال، هناك قاعدة واحدة "إذا سألك شخص عن ملابسك الداخلية أو" أجزاء خاصة "عندما كنت على الكمبيوتر ، هنا يمكنك إستدعاء أمك للتأكد من أن ما يقولونه صحيحا.'
7. بعض الأطفال يشعرون بالقلق حول رد الوالدين على أشياء قالوها أو قاموا بها على الانترنت، مما يمنعهم الإبلاغ عن مسائل هامة . يلعب هؤلاء المخالفون على هذا القلق والخجل لعزل الأطفال. للتغلب على ذلك يجب طمأنة طفلك أن تقول له أنهم يخبرونه دائما بأنهم يشعرون بعدم الارتياح أو القلق حول شخص ما وردت فعلهم على ذلك.
8. إذا أظهر طفلك تغييرات في السلوك أو المزاج التي تشمل بما في ذلك السلوكيات الجنسية زيادة أو نقصان، تماسك أو انسحاب قم باستكشاف مخاوفك معهم وإذا لزم الأمر إطلب الدعم الفني.

المراهقين

يقيم بعض البالغين علاقات صداقة مع الأطفال على الإنترنت لأغراض جنسية وهذا ما يسمى بالاستمالة وهو سلوك غير قانوني وينبغي إبلاغ الشرطة بذلك. في كثير من الحالات يمكن للشرطة مقاضاة البالغين الذين يسعون وراء الأطفال لأغراض جنسية حتى لو لم يقم إتصال وجها لوجه مع الطفل.

عادة ما تكون لدي معظم المراهقين رغبة أكبر فى إستخدام مواقع الويب التي تمكنهم من التفاعل المباشر مع أشخاص غير معروفين لديهم. هناك مخاطر تتمثل في أن الأفراد الذين يتواصل معهم المراهقون غير مناسبين لأعمارهم ، أو أنهم يعتزمون إقامة علاقة جنسية مع ابنك المراهق. النصائح التالية سوف تساعد على حماية طفلك من الأتصال الجنسي غير المرغوب فيه.

1. المشاركة في استخدامات التكنولوجيات الجديدة التى يستخدمها أطفالك فى سن المراهقة ، بغرض مواكبة المواقع التي يزورونها وقم بتعريفهم ببعض ممن تثق بهم إن كان ذلك ممكنا. بشكل عام فإنه من المفيد أن تنظر فيما إذا كنت مرتاحا لمحتوى المواقع وإمكانية الاتصال مع الآخرين بما في ذلك البالغين.
2. قم بتذكير طفلك المراهق بإنشاء قوائم تعريفية لا توضح الجنس والعمر والإسم أو الموقع وليست مثيرة جنسيا.
3. قم بتوجيه طفلك المراهق لإستخدام إعدادات الخصوصية الخاصة بهم لتقييد معلوماتهم على الانترنت لعرضها علي أصدقائهم المعروفين فقط.
4. قم بتشجيع إبنك المراهق للحفاظ على أصدقائه متصلين على الإنترنت. إذا كانوا يريدون أن يلتقوا بأحد ما لم يلتقوا به شخصيا من قبل شجعهم على طلب أحد الوالدين أو شخص بالغ آخر موثوق به للذهاب معهم ويفضل دائما اللقاء في الأماكن العامة، وخلال النهار.
5. قم بتشجيع إبنك المراهق أن يكون حذرا تجاه الأشخاص الذين يقابلهم على الانترنت ويشعرونه بعدم الارتياح وأن يغلق عليهم الموقع . كما ينبغي عليه أن يبلغ مدراء الموقع بتلك الإتصالات غير اللائقة.
6. يشعر بعض المراهقين بالقلق حول ردود أفعال والديهم حول الأشياء التي قد قالوها أو قاموا بها على الانترنت، خصوصا إذا كانوا يعتقدون بأنهم يشجعون الاتصال الجنسي عبر الإنترنت ، مما يمنعهم الإبلاغ عن مخاوفهم بشأن الاتصالات عبر الإنترنت. يلعب هؤلاء المخالفون على هذا القلق والخجل لعزل الأطفال من العائلة والأصدقاء، وتشجيعهم على الثقة بهم.
7. وللتغلب على هذه المخاطر يمكنك القيام بطمأنة المراهق بأنك ستدعمه دائما ولا تمنعهم الدخول إلى الإنترنت فى حال قيامهم بالإبلاغ عن أى مضايقات غير مريحة أو أنهم قلقون حول أقوال بعض الأ شخاص عبر الإنترنت.
8. كن يقظا ومنتبها للتغييرات التى تحدث في سلوك أو مزاج إبنك المراهق أو التي تتعلق بالسلوكيات الجنسية زيادة أو نقصان و / أو إظهار الثقة، والإلتصاق أو الانسحاب، والقلق أو الحزن وتغيير التفاعلات مع الأصدقاء. حاول استكشاف مخاوفك معهم وإذا لزم الأمر إطلب الدعم الفني.

الأمن الإلكترونى و التجارة الإلكترونية

التجارة الإلكترونية

التجارة الإلكترونية (التجارة الإلكترونية) أو التسوق عبر الإنترنت يعني ممارسة الأعمال التجارية على شبكة الإنترنت ويشمل بيع وشراء السلع أو الخدمات عبر الإنترنت. في الوقت الحاضر، العديد من الشركات ذات السمعة الطيبة مقبلون على هذا النمط من ممارسة الأعمال التجارية لتغطية سوق أوسع.

يغطي الأمن الإلكتروني أو أمن الإنترنت مجموعة واسعة من الأنشطة للحفاظ على المعلومات الإلكترونية آمنة. وتجرى عمليات الشراء والأعمال التجارية عبر الإنترنت أكثر وأكثر كل يوم لذلك من المهم بالنسبة للآباء فهم كيفية حماية أجهزة حواسيبهم ومعاملاتهم المالية إذا أرادوا المشاركة في التجارة الإلكترونية وشراء إحتياجاتهم عبر الإنترنت.

توفر مواقع التسوق على الانترنت ذات السمعة الحسنة لعملائها معاملات تجارية آمنة عبر الإنترنت. فقط ومن خلال الجلوس أمام الكمبيوتر، يمكن للمشتري تأكيد مشترياته / مشترياتها والدفع عبر الإنترنت. وسيتم شحن البضاعة التى تم شراؤها وإرسالها مباشرة إلى عنوان المشتري. لسوء الحظ ، فإن الشراء عبر الإنترنت يمكن أن يسبب في بعض الأحيان متاعبا مثل تأخر تسليم السلع، ونوعية السلع قد لا يطابق الوصف على الموقع أو عدم وصول السلع للمشترى!

- **النصائح الأساسية للآباء والأمهات**

1. يمكن أن يؤدى الأمن أو أمن الإنترنت الضعيف إلى فساد فى الملفات وتمكين المجرمين وغيرهم للوصول إلى المعلومات الشخصية والمالية. توفر تدابير الأمن الإلكترونى الحماية من التطفل غير المرغوب فيه المتعمد وغير المتعمد لإفساد أجهزة الكمبيوتر و الملفات وفقدان البيانات.تأكد أن لديك أحدث برامج الكمبيوترمثل فاحص الفيروسات وأحدث متصفحات الويب وكاشفات البرامج الضارة قبل ان تشارك في التجارة الإلكترونية.
2. يغطي الأمن الإلكترونى أو أمن الإنترنت مجموعة واسعة من الأنشطة للحفاظ على المعلومات الإلكترونية آمنة. وينصح الآباء والأمهات أن يطلعوا على أفضل الممارسات للتأكد من أنها ليست ضحية لخرق الأمن الإلكتروني.
3. يمكن أن يؤدى الأمن أو أمن الإنترنت الضعيف إلى فساد فى الملفات وتمكين المجرمين وغيرهم للوصول إلى المعلومات الشخصية والمالية.

ما يجب القيام به قبل إجراء المعاملات التجارية عبر الإنترنت:

تقدم مواقع الانترنت معلومات محددة ومهمة يجب الإنتباه إليها قبل إجراء المعاملات التجارية عبر الإنترنت، وتشمل الآتى:

1. اسم البائع وعنوانه ورقم الهاتف
2. البريد الإلكتروني للبائع (إن وجد)
3. وصف السلع أو الخدمات
4. السعر الإجمالي وبيان مفصل لشروط الدفع
5. تاريخ توريد السلع أو الخدمات
6. العملة التي بموجبها يتم دفع المبالغ المستحقة
7. شرح كيفية شحن البضائع لك
8. سياسة سعر الصرف لدى البائع ، إن وجدت
9. يجب أن تحصل على نسخة من العقد
10. يجب أن يكون للموقع بروتوكول آمن.

1. كن حذرا وحريصا بشأن النقاط الساخنة فى خدمة الواي فاي. النقاط الساخنة غير المعروفة غير آمنة وتسمح للقراصنة بإلتقاط وجمع أي بيانات تتدفق من وإلى النقطة الساخنة، وتمكينهم من سرقة المعلومات الشخصية والسرية (تسجيلات الدخول وكلمات المرور ورسائل البريد الإلكتروني والوثائق المرفقة) المخزنة على الجهاز المحمول الخاص بك.
2. ابحث عن المواقع التي توفر الدفع الآمن (المعروفة باسم التشفير) – سيظهر رمز قفل على الشاشة أثناء تعبئتك لتفاصيل الدفع.
<=="" li="" style="margin: 0px; padding: 0px;"><=="" li="" style="margin: 0px; padding: 0px;">
3. احذر من رسائل البريد الإلكتروني التى تقول "يا أنت، تحقق من تخفيضات العطلات القائمة هنا!" أو "فى هذا المكان تبلغ تخفيضات العيد 50% في المائة!" يمكن للكمبيوتر المرسل أن يصاب من قبل برمجيات خبيثة المبرمجة من خلال إرسال روابط خبيثة على عناوين البريد الإلكتروني للجميع.
4. قم بحماية خصوصيتك. لا تكشف عن التفاصيل الشخصية الخاصة بك بكل بساطة.
5. قم بعمل فحص مزدوج وتحقق ما إذا كان لدي الشركة بيان الخصوصية الذى يخبرك ماذا سيفعلون مع المعلومات الشخصية الخاصة بك.
6. تأكد من معرفة تفاصيل التاجر الكاملة. ويمكن استخدام تلك المعلومات تفاصيل عن النسخ الاحتياطي في حاجتك لتقديم تقرير الاحتيال. إذا لم يكشف البائع عن المعلومات الضرورية، وما عليك إلا أن تعمل على إيجاد بائع آخر.

ما الذي يمكنك القيام به لحماية نفسك؟

1. قم بفحص المنتج من خلال الهاتف أو البريد الإلكتروني.
2. الدفع عن طريق بطاقة الائتمان وتتبع جميع المعاملات.
3. إذا كنت تدفع عبر الإنترنت، تأكد من أن الموقع آمن. عليك التأكد من وضع الختم الأمنى للشركة.

النصائح التالية يمكن أن تساعد على ضمان معاملة آمنة على الانترنت

1. ابحث عن رمز القفل قبل إدخال المعلومات الشخصية على موقع شبكة الانترنت، والبحث عن أيقونة "القفل" في المتصفح الخاص بك. القفل المغلق قفل يشير إلى أن الموقع آمن. ميزة أخرى من موقع على شبكة الانترنت هو آمن عندما يبدأ.'https://'
2. Uاستخدام جدار الحماية: تثبيت أحدث برنامج جدار حماية على الكمبيوتر الخاص بك لتتبع عمليات الاقتحام.
3. تثبيت تحديثات الأمان للكمبيوتر. تمكن معظم أنظمة تشغيل أجهزة الكمبيوتر المستخدمين من تحديث نظام أمن الكمبيوتر الخاص بهم لحماية البيانات من برامج التجسس والفيروسات وغيرها من التهديدات.

AKAIS-Az

تحديد القضايا عند إجراء المعاملات التجارية عبر الإنترنت

الغش فى بطاقة الائتمان

يستخدم معظم الناس اليوم بطاقات الائتمان والخصم لإجراء عمليات الشراء. ليس فقط أنها تساعد على إجراء المعاملات بطريقة أسهل بكثير وأسرع، بل أنها تستبدل أيضا الحاجة إلى حمل النقود. بالإضافة إلى ذلك، فإن بطاقات الائتمان والخصم هي طريقة الدفع المفضلة للشراء عبر الإنترنت.

على الرغم من الميزات الأمنية المختلفة التي أدخلتها شركات بطاقات الائتمان، يبقى مستخدمو بطاقات الائتمان في خطر تزوير بطاقات الائتمان. في الواقع، حتى أولئك الذين ليس لديهم بطاقات الائتمان يصبحون ضحايا، نظرا لإمكانية إستخدام معلوماتهم الشخصية لطلب بطاقات ائتمان جديدة من قبل المحتالين.

- **لاحتيال الأكثر شيوعا على بطاقات الائتمان**

هناك عدة أنواع من الاحتيال على بطاقات الائتمان شائعة جدا في الوقت الحاضر، مثل:

1. **سرقة البطاقة** :عندما يأخذ شخص بطاقة ائتمان لشخص آخر ويستخدمها من دون الحصول على إذن منه.
2. **التزوير** :عندما يستخدم شخص معلومات حساب حقيقي لإنشاء بطاقة مزورة تبدو حقيقية ومشروعة.
3. **تزوير بطاقات وليس إلى الوقت الحاضر** :عندما يأخذ شخص تفاصيل الائتمان لشخص آخر ويستخدمها / تستخدمها لمصلحته الخاصة.

من المهم جدا للجميع الذين يملكون بطاقات الائتمان الإحتفاظ ببطاقاتهم آمنة. وستحسب كل معاملة على حدة . وهنا بعض النصائح الجيدة حول كيفية تجنب الاحتيال على بطاقات الائتمان:

4. **الحفاظ على بطاقات الائتمان الخاصة بك آمنة** :حمل بطاقة ائتمان واحدة فقط أو اثنين ، لأن القيام بحمل أكثر من بطاقتى ائتمان في محفظتك ليس آمنا / لأنها ستكون عرضة للضياع أو الفقدان.
5. **قم بتمزيق جميع الوثائق التى تحتوى على تفاصيل بطاقة الائتمان الخاصة بك** :تدمير جميع الوثائق والرسائل، والفواتير حيث يتم طباعة تفاصيل بطاقات الائتمان الخاصة بك.
6. **لا توقع إيصالات لبطاقات ائتمان فارغة** :دائما تحقق من المبلغ المذكور في الإيصال قبل التوقيع عليه.
7. **تجنب اعطاء معلومات بطاقة الائتمان الخاصة بك** :إذا سأل شخص ما عن تفاصيل بطاقات الائتمان الخاصة بك، لا تعطيه لها بسهولة.
8. **توخي الحذر عند استخدام بطاقة الائتمان الخاصة بك على الانترنت** :لا تقم بمتابعة المعاملات عبر الإنترنت ببساطة حتى لو تلقيت الدعوة من شخص يدعي أنه ضابط بطاقة الائتمان عبر (البريد الإلكترونى / أو مكالمة هاتفية).
9. **الإبلاغ الفورى عن بطاقات الائتمان المفقودة أو المسروقة** :إذا فقدت بطاقة الائتمان الخاصة بك، قم بإبلاغ البنك وشركة بطاقات الائتمان فورا.
10. **تكون ذكيا بارعا عند دفع فواتير بطاقات الائتمان** :تحقق من كشف بيان بطاقة الائتمان الخاصة بك جيدا القيام بالدفع.

الإندفاع فى الشراء

تعرف عملية الإندفاع فى الشراء بأنها عملية شراء عفوية أو غير مخطط لها. يشار إلى الشخص الذي يقوم بإجراء مثل هذه العملية بالمشتري المتسرع. وهنا بعض النصائح الجيدة حول كيفية تجنب الإندفاع فى الشراء:

1. **كن على بينة من حجم الاموال التي تنفقها** :خذ نظرة فاحصة على كل درهم واحد تنفقه. قد لا تريد أن تنفق كثيرا على الأشياء التي ليست ضرورية. أفضل شيء تفعله هو العمل على ميزانيتك والتشبث بها.
2. **التفكير مرتين قبل إجراء عملية الشراء** :إذا كان لديك ميل إلى الاندفاع فى الشراء، كن على بينة من أي إعلانات قد تؤثر عليك.
3. **ضع أهداف واضحة عند التسوق**:ضع أهدافك الخاصة في كل مرة تذهب للتسوق والتزم بها. قد تكون بحاجة لتذكير مثل مذكرة صغيرة حيث يمكنك ترتيب قائمة بجميع المنتجات التي تحتاج إليها في وقت مبكر.

AKAIS-AZR

حماية جهاز الكمبيوتر الخاص بك

فهم المخاطر الأمنية للإنترنت

يمكن أن يؤدي ضعف الأمن الإلكتروني إلى فساد فى الملفات والبيانات، وفقدان الخصوصية وتمكن المجرمين وغيرهم من الوصول إلى المعلومات الشخصية والمالية. يوفر الأمن الإلكترونى تدابير الحماية من التطفل غير المرغوب فيه المتعمد وغير المتعمد لإفساد أجهزة الكمبيوتر والملفات، وفقدان البيانات.

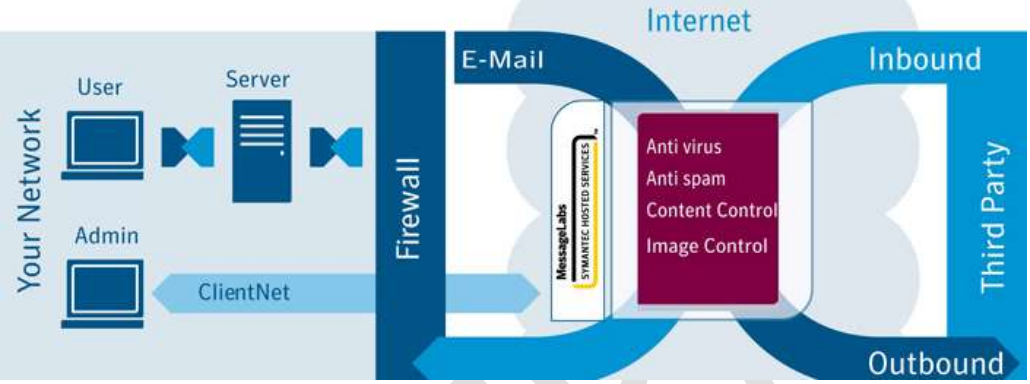
- **الفيروسات والديدان وأحصنة طروادة**

الفيروس هو مجموعة من التعليمات البرمجية الضارة التي تنتقل للكمبيوتر عن طريق البريد الإلكتروني، من خلال إصابة التنزيلات والتى تشمل البرامج الجديدة والصور وملفات الموسيقى، وأجهزة الكمبيوتر المصابة مثل USB أو عند تصفح الانترنت. بإمكان الفيروسات تدمير أجهزة الكمبيوتر، وسرقة المعلومات والإنتشار بأنفسهم إلى أجهزة الكمبيوترات الأخرى.

حصان طروادة هو برنامج يمكنه إتلاف جهاز كمبيوتر، وسرقة البيانات الخاصة، وإعطاء الآخرين الوصول إلى الكمبيوتر أو انتشار الفيروس.

الدودة هى برنامج ذاتي التكرار يمكنه أن ينتشر من دون تدخل المستخدم. تم تصميم الديدان بغرض إصابة أجهزة الكمبيوتر بالمزيد من أنواع أخرى من البرامج الضارة، مثل البرامج التي تعمل على إرسال البريد المزعج. ويمكن للدودة أن تنتشر عن طريق إرسال نفسها إلى جميع جهات الاتصال في دفتر العناوين في برنامج البريد الإلكتروني، أو عن طريق ثغرة أمنية في برنامج أو في نظام تشغيل الكمبيوتر

الحماية ضد المخاطر الأمنية للإنترنت



يوما بعد يوم لا تدور إستخدامات الإنترنت فقط حول الشبكات الاجتماعية، والتجارة الإلكترونية أو تصفح الإنترنت، بل أنه من وقت لآخر نجد أنه من المستحسن تبادل البيانات مع الآخرين، وتحميل محتوى من شبكة الإنترنت أو الاشتراك في الخدمات التي ترسل الملفات إلى جهاز الكمبيوتر الخاص بك. من المهم أن نفهم ما هى الآثار المترتبة على هذه الأنشطة وأفضل الطرق لحماية نفسك ضد الوصول غير المرغوب لجهاز الكمبيوتر أثناء تنزيل وتبادل بيانات الكمبيوتر.

- **الجدران النارية(FIREWALLS)**

يمكن للجدار الناري منع كل حركة المرور بين شبكة الانترنت وجهاز كمبيوتر غير مسموح صراحة بدخوله، ومنع الدخول غير المصرح به إلى البيانات. يوفر الجدار الناري الحماية من الفيروسات وبرامج التجسس، والبريد المزعج ، إضافة إلى حماية المعلومات والبيانات الشخصية المخزنة على جهاز الكمبيوتر.

وجود جدار الحماية المتحول بشكل دائم هو خط الدفاع الأول ضد الفيروسات وبرامج التجسس والمتسللين.

توفر معظم انظمة التشغيل جدار حماية كجزء من انشاء الأمن الأساسي. قد تتوفر تجاريا البرمجيات الأمنية مثل مكافحة الفيروسات والبرامج المضادة للفيروسات قد تشمل أيضا خيارا من خيارات جدار الحماية الشخصية.

تبادل الملفات الأكثر أمانا

تبادل الملفات هو تبادل المعلومات الرقمية مثل برامج الكمبيوتر، الملفات الصوتية أو الفيديو أو الوثائق أو الكتب الإلكترونية مع الآخرين عبر الإنترنت. أكثر الملفات المشتركة والمقرصنة عادة الموسيقى والأفلام وبرامج الكمبيوتر. ويجري تبادل الملفات عبر الإنترنت باستخدام الشبكات بين الند للند.(P2P)

الند للند (P2P) هى تطبيقات برامجية تعمل على أجهزة الكمبيوتر الشخصية فى تبادل الملفات، مثل ملفات الموسيقى، مع مستخدمين آخرين عبر الإنترنت. تعمل شبكات الند للند P2P من خلال ربط أجهزة الكمبيوتر الفردية معا لمشاركة الملفات مباشرة بدلا من الاضطرار إلى اللجوء إلى جهاز خادم مركزي. شبكة الند للند P2Pشعبية ومعروفة للأطفال نظرا لمجانية البرنامج عادة، وسهولة تركيبه ويتيح الوصول إلى العديد من الملفات التي من شأنها أن يكون الحصول عليها من الصعب جدا أو مكلفا للغاية. بعض البرامج وتبادل الملفات تمكن الناس من الدردشه على الانترنت خلال مشاركتهم.

يمكن أن تكون مشاركة الملفات آمنة إذا تم استخدام الخدمات القانونية وتدابير الأمن الإلكتروني المناسبة.

يتيح تبادل ملفات الند للند P2P للمستخدمين الوصول إلى أنظمة بعضهم البعض. ويختلف مستوى الوصول وفقا لعلم المستخدم من استخدام وإعدادات الأمان المناسبة. يمكن للمستخدمين الأقل معرفة الوصول إلى جميع جوانب نظام أجهزة الكمبيوتر الخاصة بهم، وليس فقط ملفات الموسيقى أو الفيلم التى يتشاركونها أصلا.

لبعض الملفات في شبكات الند للند P2P مسميات مختلفة لإخفاء وتضليل الطبيعة الحقيقية للمحتوى. يعني هذا أن الأطفال قد يحملوا شيء يظهرهم أبرياء، فقط لتجد أنه من غير المناسب بالنسبة لهم. ويمكن أيضا استخدام شبكات الند للند P2P لتوزيع مواد الاعتداء الجنسي على الأطفال أو محاولة السعى لاجراء اتصالات مع الأطفال. يجب على الآباء أن يكونوا حذرين خاصة من البرمجيات التي تمكن الأطفال من الدردشة مع أشخاص آخرين خلال تبادل الملفات.

التحميل الأكثر أمانا للملفات والموسيقى والفيديو

التحميل هو عملية حفظ ملف من الإنترنت على جهاز الكمبيوتر. الطريقة الأكثر شيوعا للتحميل هى الضغط على الرابط الذى يبدأ عملية التحميل تلقائيا. سوف يظهر مربع حوار يُظهر مطالبة المستخدم لاختيار موقع الكمبيوتر إلى "حفظ" الملف، وباختيار الحفظ تبدأ العملية.

التحميل هو النشاط الأكثر شيوعا والمتزايد على شبكة الانترنت لكثير من الناس ، وتحميل الموسيقى والفيديو هي نقطة الجذب الرئيسية لاستخدام شبكة الإنترنت. يقوم العديد من الطلاب بتحميل وثائق مثل صحائف الواجبات المدرسية وكذلك الموسيقى والأفلام.

ليس من الضروري أن يكون تحميل الملفات والموسيقى والفيديو غير قانوني. هناك العديد من المصادر القانونية التي تقدم الموسيقى والأفلام وغيرها من المعلومات للتحميل. بعضها خدمات مجانية في حين أن للبعض الآخر رسوم لكل خدمة أو رسوم الاشتراك المستمر.

من القضايا الهامة التى يتحتم على المرء معرفتها قضية حدود التحميل المحتملة بعقد الإنترنت الخاص بك. من المهم قبل التحميل التحقق من حد تحميل الانترنت الخاص بك ، وما هو مستوى التحميل الحالي وما هى تكلفة التحميل الإضافى أي كم ستكون الرسوم الإضافية.

التحميل فى العديد من المواقع غير القانونية يحمل أيضا خطر الفيروسات. يمكنك أن تسأل الأصدقاء أو العائلة عن المواقع الموثوقة والقانونية للتحميل.

تساعد النصائح التالية الوالدين على إدارة مخاطر عملية التحميل.

الأطفال الصغار

من غير المرجح أن يمثل التحميل مشكلة للأطفال الأصغر سنا الذين قد لا تتاح لهم الفرصة، أو المعرفة لتحميل وسائل الاعلام مثل الموسيقى أو الفيديو. إذا كان الأطفال على الانترنت تمثل النصائح العامة التالية نقطة انطلاق جيدة لمساعدتهم على أن يكونوا فى وضع آمن ويمكنهم تحمل المسؤولية. لذا فإنه من المفيد النظر في النصائح التالية.

1. فكر في استخدام الفلاتر، والعلامات والمناطق الآمنة للمساعدة في إدارة أساليب وصول طفلك ودخوله على الانترنت.
2. تثبيت وتحديث برامج مكافحة الفيروسات وغيرها من برامج الأمن الإلكتروني لمنع الوصول غير المصرح به إلى البيانات الموجودة على الكمبيوتر المنزلي وحماية تلك البيانات من الفساد.
3. تأكد من تشغيل ميزات الأمان بما في ذلك جدار الحماية على المسح التلقائي وأنه قد تم تحديثها بانتظام لحمايتها ضد أحدث المخاطر.

الأطفال الكبار

يمكن أن يمثل التحميل خطورة للأطفال الأكبر سنا الذين يرغبون في تنزيل ملفات الوسائط مثل الموسيقى والبرامج التلفزيونية والأفلام ونغمات الرنين. النصائح التالية تساعدتك على توجيه طفلك.

1. تحدث مع طفلك عن الأخطار المحتملة لاستخدام مواقع غير آمنة لتحميل ومشاركة الملفات، بما في ذلك التعرض لخطر اصابة جهاز الكمبيوتر في المنزل بالفيروسات، والتكاليف المحتملة والجوانب القانونية لخرق حقوق النشر.
2. إذا كنت تريد تعليم طفلك تحميل الوسائط الإعلامية قم باستخدام المواقع الموثوق بها والقانونية ، والتى تكون واضحة من شروطها وأحكامها أو يمكن العثور عليها من خلال البحث على شبكة الإنترنت أو غيرها من المصادر.
3. إذا كنت لست متأكدا من مواقع أخرى آمنة أو قانونية يمكنك طلب ذلك من الأهل والأصدقاء ويمثل ذلك وسيلة جيدة للتعرف على مصادر تحميل موثوق بها.
4. إذا كنت مرتاحا مع طفلك لاستخدامه مواقع تضع رسوما مقابل الدخول إليها ، فإنك ربما تفكروتنظر في زيارة المواقع المفضلة لديك معهم والتحقق من الرسوم. وقد يكون من المفيد وضع قواعد تطلب من طفلك الحصول على إذنك قبل تنزيل الملفات، لمنع إضافة تكاليف غير متوقعة. وضع ميزانية الأسرة الأسبوعية لتنزيل الوسائط المساعدة قد يُساعد كثيرا.
5. إذا كان طفلك يستخدم موقع التحميل الذي يفرض الرسوم تأكد من أن للموقع تسهيلات دفع آمنة عبر الإنترنت. ابحث عن https://في حقل العنوان ورمز القفل المغلق في أسفل الشاشة. وتشير https:// ورمز القفل إلى أن البيانات المالية مشفرة ومحمية من الوصول إليها بصورة غيرمصرح بها.
6. تحدث إلى طفلك عن حد التحميل بعقد الإنترنت الخاص بك. ما هو الحد وما هي التكلفة إذا تم تجاوز ذلك؟ أي نوع من الاستخدام يحدث مع كل تحميل، وكيف يمكنك التحقق من الاستخدام الحالي مع طفلك؟
7. فكر في استخدام الفلاتر، والعلامات والمناطق الآمنة للمساعدة في إدارة وصول ودخول طفلك على الانترنت.
8. قم بتثبيت وتحديث برامج مكافحة الفيروسات وغيرها من برامج الأمن الإلكتروني لمنع الوصول غير المصرح به إلى البيانات الموجودة على الكمبيوتر المنزلي وحماية تلك البيانات من الفساد. تأكد من تشغيل ميزات الأمان بما في ذلك جدار الحماية على المسح التلقائي وأنه قد تم تحديثها بانتظام لحمايتها ضد أحدث المخاطر.

المراهقين

التحميل من الممارسات المحببة وسط المراهقين الذين يقومون بتحميل ملفات الوسائط الإعلامية مثل الموسيقى والبرامج التلفزيونية والأفلام والنغمات. النصائح التالية يمكن أن تساعد في توجيه إبنك المراهق للتحميل بأمان.

1. تحدث مع ابنك المراهق حول المخاطر المحتملة لاستخدام مواقع غير آمنة لتحميل ومشاركة الملفات، بما في ذلك التعرض لخطر اصابة جهاز الكمبيوتر في المنزل مع الفيروسات، والتكاليف المحتملة والجوانب القانونية لخرق حقوق النشر.
2. إذا كنت تريد تعليم طفلك تحميل الوسائط الإعلامية قم باستخدام المواقع الموثوق بها والقانونية ، والتى تكون واضحة من شروطها وأحكامها أو يمكن العثور عليها من خلال البحث على شبكة الإنترنت أو غيرها من المصادر.
3. إذا كنت لست متأكدا من مواقع أخرى آمنة أو قانونية يمكنك طلب ذلك من الأهل والأصدقاء ويمثل ذلك وسيلة جيدة للتعرف على مصادر تحميل موثوق بها.
4. إذا كنت مرتاحا مع طفلك باستخدام مواقع التحميل هذا الاتهام للاستخدام كنت قد تنظر في زيارة المواقع المفضلة لديك معهم والتحقق من الرسوم. قد يكون من المفيد وضع قواعد تتطلب طفلك للحصول على إذن منك قبل أن تنزيل الملفات، لمنع تكاليف غير متوقعة. وضع ميزانية الأسرة الأسبوعية لتنزيل الوسائط المساعدة قد يُساعد كثيرا.
5. إذا كان طفلك يستخدم موقع التحميل الذي يفرض الرسوم تأكد من أن للموقع تسهيلات دفع آمنة عبر الإنترنت. ابحث عن https://في حقل العنوان ورمز القفل المغلق في أسفل الشاشة. وتشير https:// ورمز القفل إلى أن البيانات المالية مشفرة ومحمية من الوصول إليها بصورة غيرمصرح بها.
6. تحدث إلى طفلك عن حد التحميل بعقد الإنترنت الخاص بك. ما هو الحد وما هي التكلفة إذا تم تجاوز ذلك؟ أي نوع من الاستخدام يحدث مع كل تحميل، وكيف يمكنك التحقق من الاستخدام الحالي مع طفلك؟
7. فكر في استخدام الفلاتر، والعلامات والمناطق الآمنة للمساعدة في إدارة وصول طفلك ودخوله على الانترنت.
8. قم بتثبيت وتحديث مكافحة الفيروسات وغيرها من برامج الأمن الإلكتروني لمنع الوصول غير المصرح به إلى البيانات الموجودة على الكمبيوتر المنزلي وحماية هذه البيانات من الفساد. تأكد من تشغيل ميزات الأمان بما في ذلك جدار الحماية على المسح التلقائي وأنه قد تم تحديثها بانتظام لحمايتها ضد أحدث المخاطر.

SECURING A WIRELESS NETWORK

Wireless networks in the office or at home enable users to share files, printers and internet access between all their computers without cables.

Wireless networking is very useful, but if not password protected, your wireless network may be accessed by others—even people who live next door or across the street. This could lead to you exceeding your download limit without knowing why. It can also enable others to access your personal information.

There are countless public computers offering internet access including computers in libraries, airports and internet cafes. Because these computers are accessible to many people, taking extra precautions to protect personal information and protect against possible virus infection is important.

Remembering not to leave a public computer unattended until fully logging out and not saving any files or any log-in information will help you to be safe when using public computers. Where a website has an automatic log-in checkbox, it's a good idea to uncheck it. This helps to prevent others logging in with your identity later. When you've finished, clear the history, quit the browser, log out and, if possible, reboot the computer.

If using a public wireless network try to avoid online banking or credit card transactions, and ensure that security software, such as anti-virus and anti-spyware software and a firewall, are installed on the laptop.

حماية المعلومات الشخصية

المعلومات الشخصية هي أية معلومات من شأنها التعريف على شخص ما، وتشمل المعلومات الشخصية الاسم الكامل والعنوان وتاريخ الميلاد وأرقام الهواتف وعناوين البريد الإلكتروني، وأسماء المستخدمين وكلمات المرور وتفاصيل الحساب المصرفي وتفاصيل بطاقة الهوية أو جواز السفر.

تستخدم المعلومات الشخصية على شبكة الانترنت من قبل العديد من الشركات للتحقق من هوية المستخدم.ومن الممكن أن يتم الكشف عن المعلومات الشخصية للعديد من الأعمال التجارية المشروعة بشكل آمِن، غير أنَّ هذه المعلومات يمكن الوصول إليها وإساءة استخدامها من قبل المجرمين إذا لم يتم التعامل معها بعناية. ويمكن أيضا أن تستخدم من قبل المسوِّقين من خلال إرسال رسائل غير مرغوبة عن طريق البريد الالكتروني أو من خلال الرسائل النصيَّة القصيرة.

يمكن لكشف المعلومات الشخصية عبر الإنترنت أن يؤثر أيضا على السمعة الرقمية للمستخدم، والسمعة الرقمية هي الرأي الذي يحمله الأشخاص لغيرهم على أساس ما يفعلونه ويقولونه عبر الإنترنت.

سوف تساعد النصائح العامة التالية الوالدين على حماية المعلومات الشخصية لأطفالهم على الانترنت.

الأطفال الصغار

الإرشادات التالية هي نقطة بداية مفيدة لتعليم الأطفال الصغار على التفاعل بأمان ومسؤولية عبر الإنترنت.

1. ينبغي في هذا العمر إبقاء استخدام الأطفال للإنترنت تحت المراقبة الحثيثة، وللمساعدة في هذا ينبغي إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.
2. كن على علم بكيفية استخدام أطفالك للإنترنت، واستكشف معهم المواقع المفضلة لديهم وساعدهم على عمل قائمة بمواقعهم المفضلة وتحقق فيما إذا كانت المعلومات الشخصية مطلوبة للاشتراك بأي من هذه المواقع أو الألعاب المفضلة وساعدهم على القيام بعملية الاشتراك وعلى استخدام إعدادات الخصوصية بأمان إذا كنت تشعر بأنَّ ذلك مناسبا.
3. تحدث مع أطفالك عن المعلومات الشخصية وعن السبب في خصوصيتها إذ يمكن استخدام هذا النوع من المعلومات في تحديد هويتهم أو في تحديد أماكن سكناهم والمدارس التي يرتادونها أو الأنشطة التي يشاركون فيها.
4. ضع مجموعة من القواعد وتأكد من معرفة طفلك بماهية المعلومات التي يمكن مشاركتها مع الآخرين والمعلومات التي يمكن نشرها على الانترنت والمواقع التي يمكن زيارتها ، ومن المفيد أن يقوم الطفل باستشارة شخص بالغ وموثوق به قبل أن يقوم بنشر أية معلومات شخصية على الانترنت حتى وإن كان نشر المعلومات على الشبكة هو لغايات المشاركة في مسابقة معينة.
5. فكِّر في إنشاء حساب بريد إلكتروني عائلي لغايات 'المتعة' يمكن استخدامه للمشاركة في المسابقات وغيرها من الأنشطة. ويكون هذا الحساب منفصلاً عن الحسابات الشخصية الأخرى بحيث يمكن حذفه بسهولة إذا ما تم إساءة استخدامه.

الأطفال الاكبر سناً

المبادئ التوجيهية العامة التالية هي نقطة بداية مفيدة لتعليم الأطفال الأكبر سنا على استخدام معلوماتهم الشخصية بأمان ومسؤولية عبر الإنترنت.

1. ينبغي في هذا العمر إبقاء استخدام الأطفال للإنترنت تحت المراقبة الحثيثة، وللمساعدة في هذا ينبغي إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.
2. كن على علم بكيفية استخدام أطفالك للإنترنت، واستكشف معهم المواقع المفضلة لديهم وساعدهم على عمل قائمة بمواقعهم المفضلة وتحقق فيما إذا كانت المعلومات الشخصية مطلوبة للاشتراك بأي من هذه المواقع أو الألعاب المفضلة وساعدهم على القيام بعملية الاشتراك وعلى استخدام إعدادات الخصوصية بأمان إذا كنت تشعر بأنَّ ذلك مناسبا.
3. تحدث مع أطفالك عن المعلومات الشخصية وعن السبب في خصوصيتها إذ يمكن استخدام هذا النوع من المعلومات في تحديد هويتهم أو في تحديد أماكن سكناهم والمدارس التي يرتادونها أو الأنشطة التي يشاركون فيها.
4. ضع مجموعة من القواعد وتأكد من معرفة طفلك بماهية المعلومات التي يمكن مشاركتها مع الآخرين والمعلومات التي يمكن نشرها على الانترنت والمواقع التي يمكن زيارتها ، ومن المفيد أن يقوم الطفل باستشارة شخص بالغ وموثوق به قبل أن يقوم بنشر أية معلومات شخصية على الانترنت حتى وإن كان نشر المعلومات على الشبكة هو لغايات المشاركة في مسابقة معينة.
5. ذكِّر طفلك بأن الهوية الحقيقية لكل مستخدم للشبكة قد لا تكون هي الهوية التي يدعيها وشجعهم على توخي الحذر عند مشاركة المعلومات.
6. ساعد طفلك على إنشاء "أسماء شاشة" أو "هويات تعريف" لا تتضمن نوع الجنس أو العمر أو اسم المكان الذي يتواجد فيه.
7. فكِّر في إنشاء حساب بريد إلكتروني عائلي لغايات 'المتعة' يمكن استخدامه للمشاركة في المسابقات وغيرها من الأنشطة. ويكون هذا الحساب منفصلاً عن الحسابات الشخصية الأخرى بحيث يمكن حذفه بسهولة إذا ما تم إساءة استخدامه.

المراهقون

يمكن للنصائح التالية مساعدة المراهقين على إدارة معلوماتهم الشخصية بشكل آمِن ومسؤول.

1. ذكِّر ابنك المراهق بأن الهوية الحقيقية لكل مستخدم للشبكة قد لا تكون هي الهوية التي يدعيها على الرغم من أن أنهم قد يستمتعون بوجود العديد من الأصدقاء عبر الإنترنت إذ أنَّ إضافة اشخاص جُدد ومجهولي الهوية الى 'قوائم الأصدقاء "يسمح لهؤلاء الناس بمعرفة كل شيء عنهم. ومن الممكن عندها أن يتم استخدام هذه المعلومات للقيام بعمليات الاحتيال وسرقة الهوية وما هو أسوأ من ذلك.
2. تحدث مع من هم في سن المراهقة حول إدارة المعلومات الشخصية على مواقع الشبكات الاجتماعية.
3. شجعهم على عدم وضع أية معلومات شخصية على ملفاتهم الشخصية. وهذا يشمل رقم الهاتف، عنوان البريد الإلكتروني الشخصي أو عناوين المسكن والمدرسة أو اسمها.
4. تشجيع المراهق على توخي الحذر عند نشر الصور التي قد تقدم عن طريق الخطأ دلائل على معلوماتهم الشخصية مثل الزي المدرسي الخاصة بهم.
5. تشجيع المراهقين على إنشاء حساب بريد إلكتروني مستقل للاستخدام عند الدخول الى الألعاب أو المواقع ويكون هذا الحساب منفصلاً عن أية حسابات شخصية أخرى بحيث يمكن حذف هذا الحساب إذا تعرض لإساءة الاستخدام ولا ينبغي أن يحتوي عنوان هذا الحساب على أسماءهم أو على أية معرفات أخرى.
6. قد يكون من المحبب لهم أيضا إنشاء حساب منفصل للتواصل مع الشبكات الاجتماعية اذا ما أرادوا الترويج لأنفسهم أو لاهتمام ما والتواصل مع أمثالهم من الاشخاص الذين لا يعرفونهم حاليا على أرض الواقع، وينبغي عليهم التأكد من خلو الموقع من معلوماتهم الشخصية.
7. تشجيع المراهقين على قراءة اتفاقات المستخدم وسياسات الخصوصية التي تحدد الكيفية التي يمكن بها استخدام معلوماتهم الشخصية عند اشتراكهم ببعض الخدمات إذ أنَّ العديد من المؤسسات تستخدم معلوماتهم في التسويق لنفسها ويمك لبعضها أن يقوم ببيع هذه المعلومات لبعض الشركات التسويقية الأخرى.
8. تذكير المراهق أنه ينبغي الكشف عن المعلومات المالية فقط على المواقع التي يثقون بها والتي لديها مرافق دفع آمنة يميزها عنوان يبدأ برابط نص تشعبي (https://) ورمز قفل "مؤمن/مغلق" في أسفل الشاشة، يشير إلى قيام المرفق بتشفير البيانات.
9. تذكير المراهق بأن المؤسسات المصرفية لا تقوم بأي حال بإرسال طلبات موجهة للأفراد عبر البريد الإلكتروني تطلب فيها اسم المستخدم أو كلمة المرور الخاصة بهم وأن حدث وتلقى رسالة بريد إلكتروني من منظمة تزعم بأنها تمثل مؤسسة مصرفية عليه القيام بإبلاغ البنك عن هذا البريد الإلكتروني.

السمعة الرقمية

لمستخدمي الإنترنت سمعة رقمية أو سمعة عبر الإنترنت تمكِّن الآخرين من رؤيتهم على الشبكة وتستند هذه السمعة الى الآثار التي يخلفها نشاط المستخدم عبر الإنترنت وهي ما يُطلق عليه "البصمة الرقمية" الخاصة بهذا المُستَخدِم وحفاظاً على الخصوصية والأمان ينبغي أن يعيّ الأطفال والشباب معلوماتهم الشخصية المتاحة على شبكة الإنترنت، وأن يدركوا هوية من يستطيع الوصول إليها، وما يفعله الآخرون بمعلوماتهم الخاصة والانطباع الذي يتركونه ليجده الآخرون.

تساعد النصائح العامة التالية الوالدين على حماية سمعة أبنائهم الرقمية.

الأطفال الصغار

1. ربما يكون مفهوم السمعة الرقمية أمرا بالغ التعقيد ومستعصياً على فهم الأطفال الصغار.
2. تعتبر النصائح العامة المتعلقة بالسلامة على الإنترنت بداية جيدة في مساعدة الأطفال على تطوير آداب الإنترنت المناسبة والملائمة وعلى تعلم طرق الرد عبر الانترنت ولقد تم ذكر هذه الأمورعلى الموقع الإلكتروني لسايبر.C3
3. يمكن أن يكون مفيدا كنقطة انطلاق لمساعدة الأطفال الصغار على فهم ضرورة التصرف عبر الإنترنت بنفس الطريقة التي يتصرفون بها وهم خارج الشبكة، وينبغي مساعدتهم على استيعاب أن الآخرين يمكن لهم أن يروا ما يفعلون على الانترنت. لذا من الطبيعي أن يتوخوا الحذر فيما يقولونه ويفعلونه.

الأطفال الأكبر سنا

1. ينبغي في هذا العمر الاستمرار في مراقبة استخدام الأطفال للإنترنت عن كثب وللمساعدة في هذا حاول إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.
2. بَيِّن لطفلك أن الإنترنت مكان عام وأن المعلومات التي يشارك الغير بها على شبكة الانترنت قد تبقى على الشبكة لفترة طويلة، ولهذا يستوجب الأمر التفكير مليا بعواقب ذلك.
3. ساعد طفلك على تطوير المهارات التي يحتاجها للتفاعل بأمان واحترام عبر الإنترنت. اجلس معهم ووجهم استخدامهم للإنترنت وساعدهم على تعلم كيفية التواصل مع الأصدقاء والعائلة بشكل مناسب.
4. تحقق من أن إذا المواقع التي يستخدمها طفلك تسمح له بنشر المعلومات والصور لأنَّ العديد من مواقع الشبكات الاجتماعية تمكِّن الأطفال من نشر المعلومات الشخصية والتعليقات والصور بإسلوب قد يكون له تأثير على طريقة رؤية الآخرين لها وينبغي أن تراقب استخدامهم لهذه المواقع وأن تكون على بينة من التوجيهات الخاصة بالعمر وسياسات الخصوصية وشروط الاستخدام.
5. إذا كان طفلك مشاركاً في الشبكات الاجتماعية قُم بمساعدته على فهم واستخدام إعدادات الخصوصية للحد مِن عدد من يستطيعون رؤية المعلومات الخاصة بهم.

المراهقون

1. تحدث مع من هم في سن المراهقة حول إدارة المعلومات الشخصية على مواقع الشبكات الاجتماعية.
2. شجعهم على عدم وضع أية معلومات شخصية على ملفاتهم الشخصية. وهذا يشمل رقم الهاتف، عنوان البريد الإلكتروني الشخصي أو عناوين المسكن والمدرسة أو اسمها.
3. شجِّعهم على توخي الحذر عند نشر الصور على الشبكة وعلى التفكير في الكيفية التي يراها الآخرون بها.
4. تحدث معهم حول الآثارالاجتماعية والوظيفية والأكاديمية و القانونية المترتبة على نشر مواد غير لائقة لأنفسهم أو للآخرين عبر الإنترنت وحثهم على التفكير فيمن قد يرى هذا المحتوى والأثر الذي قد يكون لذلك في الحاضر والمستقبل.
5. ذَكِّرهم بأنَّ الكثير مما يفعلونه على الإنترنت قد يصبح متوفرا للعامة، وقد يتجاوز مجموعة الأصدقاء المُراد أن يصل إليهم، لذا فمن المستحسن كقاعدة عامة عدم نشر الصور التي لا يرغبون بأن يراها الغرباء على الشبكة.
6. ساعدهم على فهم أن ما يتشاركون به من معلومات قد ينتشرعبر الإنترنت أو عن طريق الرسائل النصيَّة على نطاق أوسع مما قد يعتقدون حتى وإن تم اختيار اعداد الملف الشخصي بوضعية "خاص" فإن السيطرة على تصرف الأصدقاء بالمعلومات المنشورة غير ممكن، وحثهم على التفكير مليا قبل تبادل مشاركة الصور أو الرسائل المثيرة للجدل عبر الإنترنت أو عبر الهاتف النقال.
7. ذكِّرهم بالعناية بسمعة الآخرين الرقمية إذ لا ينبغي نشر صور الآخرين دون موافقة منهم كما ينبغي توخي الحذر عند نشر التعليقات عن الآخرين.
8. تأكد من فهمهم لميزات وشروط استخدام مواقع الشبكات الاجتماعية وكيفية إعداد الملف الشخصي بوضعية "خاص" على وجه التحديد.

سرقة الهوية

سرقة الهوية هو نوع معين من الغش، الذي ينطوي على سرقة المال أو الحصول على منافع أخرى من خلال انتحال هوية شخص آخر، ويمكن لسرقة الهوية أن تكون مدمرة على النطاق المالي والعاطفي، ويمكن لها أن تحدث بعدة وسائل تتراوح بين استخدام تفاصيل بطاقة الائتمان لشخص ما بطريقة غير مشروعة للقيام بعمليات الشراء وبين انتحال هوية هذا الشخص بشكل كامل لفتح الحسابات المصرفية والحصول على القروض والقيام بالأعمال غير المشروعة تحت هذا الاسم.

وتمكِّن أدوات جمع المعلومات المتطورة مثل البرمجيات الخبيثة وبرامج التجسس الجناة من جمع المعلومات الشخصية للافراد المستهدفين دون علمهم غير أنَّ هناك العديد من التدابير التي توفرالحماية من هذه الأدوات.

تساعد النصائح العامة التالية الوالدين على حماية أطفالهم من سرقة الهوية.

الأطفال الصغار

1. ينبغي في هذا العمر إبقاء استخدام الأطفال للإنترنت تحت المراقبة الحثيثة، وللمساعدة في هذا ينبغي إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.

<=="" li="" style="margin: 0px; padding: 0px;">

2. تحدث مع أطفالك عن المعلومات الشخصية وعن السبب في خصوصيتها إذ يمكن استخدام هذا النوع من المعلومات في تحديد هويتهم أو في تحديد أماكن سكناهم والمدارس التي يرتادونها أو الأنشطة التي يشاركون فيها.
3. ضع مجموعة من القواعد وتأكد من معرفة طفلك بماهية المعلومات التي يمكن مشاركتها مع الآخرين والمعلومات التي يمكن نشرها على الانترنت والمواقع التي يمكن زيارتها ، ومن المفيد أن يقوم الطفل باستشارة شخص بالغ وموثوق به قبل أن يقوم بنشر أية معلومات شخصية على الانترنت حتى وإن كان نشر المعلومات على الشبكة هو لغايات المشاركة في مسابقة معينة.
4. فكِّر في إنشاء حساب بريد إلكتروني عائلي لغايات 'المتعة' يمكن استخدامه للمشاركة في المسابقات وغيرها من الأنشطة. ويكون هذا الحساب منفصلاً عن الحسابات الشخصية الأخرى بحيث يمكن حذفه بسهولة إذا ما تم إساءة استخدامه.
5. فكر في استخدام الفلاتر والعلامات والمناطق الآمنة للمساعدة في إدارة مستوى وصول طفلك الى الانترنت.
6. تثبيت وتحديث برامج مكافحة الفيروسات وغيرها من برامج الأمن الإلكتروني لتقييد محاولات الوصول غير المصرح بها إلى البيانات الموجودة على الكمبيوتر المنزلي وحماية هذه البيانات من الإفساد وينبغي ضمان تشغيل ميزات الأمان بما في ذلك جدار الحماية والمسح التلقائي وتحديث البرامج بانتظام للحماية من أحدث المخاطر.

الأطفال الأكبر سنا

1. ينبغي في هذا العمر إبقاء استخدام الأطفال للإنترنت تحت المراقبة الحثيثة، وللمساعدة في هذا ينبغي إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.
2. كن على علم بكيفية استخدام أطفالك للإنترنت، واستكشف معهم المواقع المفضلة لديهم وساعدهم على عمل قائمة بمواقعهم المفضلة وتحقق فيما إذا كانت المعلومات الشخصية مطلوبة للاشتراك بأي من هذه المواقع أو الألعاب المفضلة وساعدهم على القيام بعملية الاشتراك وعلى استخدام إعدادات الخصوصية بأمان إذا كنت تشعر بأنَّ ذلك مناسبا.
3. تحدث مع أطفالك عن المعلومات الشخصية وعن السبب في خصوصيتها إذ يمكن استخدام هذا النوع من المعلومات في تحديد هويتهم أو في تحديد أماكن سكناهم والمدارس التي يرتادونها أو الأنشطة التي يشاركون فيها.
4. ضع مجموعة من القواعد وتأكد من معرفة طفلك بماهية المعلومات التي يمكن مشاركتها مع الآخرين والمعلومات التي يمكن نشرها على الانترنت والمواقع التي يمكن زيارتها ، ومن المفيد أن يقوم الطفل باستشارة شخص بالغ وموثوق به قبل أن يقوم بنشر أية معلومات شخصية على الانترنت حتى وإن كان نشر المعلومات على الشبكة هو لغايات المشاركة في مسابقة معينة.
5. فكِّر في إنشاء حساب بريد إلكتروني عائلي لغايات 'المتعة' يمكن استخدامه للمشاركة في المسابقات وغيرها من الأنشطة. ويكون هذا الحساب منفصلاً عن الحسابات الشخصية الأخرى بحيث يمكن حذفه بسهولة إذا ما تم إساءة استخدامه.
6. فكر في استخدام الفلاتر والعلامات والمناطق الآمنة للمساعدة في إدارة مستوى وصول طفلك الى الانترنت.
7. تثبيت وتحديث برامج مكافحة الفيروسات وغيرها من برامج الأمن الإلكتروني لتقييد محاولات الوصول غير المصرح بها إلى البيانات الموجودة على الكمبيوتر المنزلي وحماية هذه البيانات من الإفساد وينبغي ضمان تشغيل ميزات الأمان بما في ذلك جدار الحماية والمسح التلقائي وتحديث البرامج بانتظام للحماية من أحدث المخاطر.

المراهقون

1. تشجيع المراهقين على حذف رسائل البريد الإلكتروني القادمة من مصادر غير معروفة وعدم فتح مرفقات رسائل البريد الإلكتروني التي تكون من هذا القبيل إذ أنَّها قد تحتوي على برامج ضارة قد تضر بأجهزة الكمبيوتر.
2. تشجيع المراهقين على إنشاء حساب بريد إلكتروني مستقل للاستخدام عند الدخول الى مواقع الانترنت ويكون هذا الحساب منفصلاً عن أية حسابات شخصية أخرى بحيث يمكن حذف هذا الحساب إذا تعرض لإساءة الاستخدام.
3. فكر في استخدام الفلاتر والعلامات والمناطق الآمنة للمساعدة في إدارة مستوى وصول طفلك الى الانترنت.
4. تثبيت وتحديث برامج مكافحة الفيروسات وغيرها من برامج الأمن الإلكتروني لتقييد محاولات الوصول غير المصرح بها إلى البيانات الموجودة على الكمبيوتر المنزلي وحماية هذه البيانات من الإفساد وينبغي ضمان تشغيل ميزات الأمان بما في ذلك جدار الحماية والمسح التلقائي وتحديث البرامج بانتظام للحماية من أحدث المخاطر.
5. تشجيع المراهقين على عدم تحميل الملفات أو التطبيقات من المواقع التي يشتبه بها إذ قد تحتوي هذه الملفات أو التطبيقات على برامج ضارة يمكن أن تضر بأجهزة الكمبيوتر.

الشبكات الاجتماعية الأكثر أمانا

يصف مصطلح الشبكات الاجتماعية مجموعة متنوعة من الخدمات على الانترنت مثل الفيسبوك ويوتيوب وماي سبيس وتويتر والألعاب التي تُلعَب عبر الإنترنت كعالم الحرب "World of Warcraft" ووحوش موشي "Moshi Monsters" والعوالم الافتراضية كنادي البطريق "Penguin Club" حيث تمكن هذه الخدمات الأشخاص من التواصل مع الآخرين عبر الإنترنت. وهذا يمكن الشباب من البقاء على تواصل مع الأصدقاء والعائلة والمشاركة في عوالم الخيال والمرح والألعاب مما قد ينسى الأطفال توخي الحذر ممن يتواصلون معهم على الانترنت وكشف الكثير عن أنفسهم كما أنَّهم قد يتصرفون أيضا بطرق تختلف عما هم عليه في العادة.

وتشير عبارة "خدمات الشبكات الاجتماعية" هنا إلى طيف واسع من أدوات وممارسات الخدمات التي تنمو بوتيرة سريعة ويمكن تعريف هذه الخدمات بشكل عام على أنها مساحات اجتماعية متوفرة على شبكة الإنترنت أو الهاتف المحمول مصممة لتسهيل التواصل والتعاون وتبادل المحتويات عبر شبكات الاتصالات.

تسمح خدمات الشبكات الاجتماعية للمستخدمين بإدارة وبناء وتمثيل شبكاتهم الاجتماعية على الانترنت، تشمل الخدمات عادة (وليس دائما) أفراد آخرين وقد تشمل أيضا الملفات الشخصية لفعاليات وشركات وحتى لأحزاب سياسية وقد تتيح لك هذه الخدمات إضافة أي شخص ضمن الشبكة كصديق أو وضعة ضمن قائمة المتصلين لديك أو قد تطلب الشبكة من كلا الطرفين الموافقة على كافة اشكال الاتصال.

تدعم خدمات الشبكات الاجتماعية عادة امكانية العرض العام للشبكات مع توفيرها لإمكانية وضع القيود على الخصوصية أو ايجاد مجتمعات مغلقة وتعتبر خاصية "طلب الإذن" ميزة هامة جدا لمعظم خدمات الشبكات الاجتماعية إذ أنها تسمح لأعضاء الجماعات بالتحكم في امكانية وصول الآخرين الى ملفاتهم الشخصية ومعلوماتهم وقوائم اتصالهم ومساحاتهم وتسمح ايضا بتحديد درجات الوصول كما وتختلف مستويات التفاصيل وحدود التحكم من خدمة إلى خدمة ومن الطبيعي أن تتيح إعدادات الخدمة الحفاظ على معلوماتك خاصة وشخصية (أي أنه لا يراها إلا من تم منحه الاذن بذلك) أو تمكنك من جعل امكانية رؤية معلوماتك الخاصة مقصورة على:

1. الأعضاء المسجلون في الخدمة فقط،
2. الأشخاص الموجودون في قائمة جهات الاتصال الخاصة بك.
3. فئات معينة من مستخدمي الخدمة،
4. اجعل المعلومات الخاصة بك "عامَّة" حتى يتمكَّن من رؤيتها الناس من غير الأعضاء أو ممَّن لم يوقعوا حتى لدخول الشبكة كأعضاء.

يمكن للمستخدمين من خلال إعدادات الخصوصية هذه إدارة مجموعة من العلاقات المختلفة عبر الإنترنت وإدارة وجودهم على شبكة الانترنت من حيث الكيفية التي يظهرون بها امام المعارف أو الأصدقاء أو الجمهور العام.

تعتبر إدارة العلاقات عبر الإنترنت وإدارة المظهر الذي نطل به من شبكة الانترنت مفتاح الحصول على المُتعة والأمان في استخدام الشبكات الاجتماعية مع ذلك قد تعني سرعة تطوُّر خدمات الشبكات الاجتماعية احتمال أن يكون الشباب قد طوَّروا استراتيجياتهم الشخصية أو أنَّهم قد تعلَّموا من أقرانهم ما لم يتعلموا من خلال التعليمات الرسمية ومن خلال المساعدة التي يقدمها البالغون لهم.

تختلف مواقع الشبكات الاجتماعية من حيث أنواع الأدوات والوظائف التي تقدمها وتوجد بشكل بديهي ثلاثة عناصر مشتركة بينها:

1. الملف الشخصي للعضو (وفقاً لتعريفها يكون دائما صفحة ويب).
2. القدرة على إضافة أعضاء آخرين إلى قائمة جهات الاتصال.
3. تفاعل مدعوم بين أعضاء قوائم جهات الاتصال (تتعدد أشكال التفاعل بشكل كبير ولكن هناك عادة درجة معينة من التفاعل المتاح بين الأشخاص الغير موجودين على قوائم جهات الاتصال الخاصة ببعضهم البعض).

ينظر في كثير من الأحيان الى مواقع الشبكات الاجتماعية من قبل مستخدميها على أنَّها بيئات مغلقة يتحدث فيها الأعضاء إلى أعضاء آخرين ويقف هذا الانطباع من أنَّ خدمات الشبكات الاجتماعية توفِّر مساحة خاصة وراء السلوكيات والمواد المعروضة التي يمكن أن يساء ترجمتها خارج السياق المغلق الذي وُضِعَت به، وفي الحين الذي يبدو فيه من المهم أن يفهم الأطفال والشباب الطبيعة الجماهيرية للكثير من نشاطاتهم داخل خدمات الشبكات الاجتماعية (ويمكن استخدام الأذونات وضوابط الخصوصية لإدارة المعلومات الشخصية والاتصالات)، نحتاج أيضا الى ضمان أن يفهموا النشاط على الانترنت بشكل كليّ، أي على أنها مجموع النشاط لجميع المواقع والشبكات على الانترنت التي ينتمي الفرد إليها.

القضايا والشكاوى عند استخدام موقع تواصل اجتماعي.

يمكن الإبلاغ عن أية مخاوف بشأن مواقع الشبكات الاجتماعية إلى مسؤول الموقع في المقام الأول، حيث يمكن البحث عن عنوان الاتصال به على الموقع وتحتوي كثير من المواقع على "أزرار إبلاغ" أو مركز اتصال للمساعدة في معالجة قضايا المتعلقة بالسلامة، والمحتويات المُسيئة ومحاولات القرصنة والاحتيال، ويمكن للمستخدمين أيضا السعى بشكل مستقل وراء المشورة القانونية حول الخيارات المتوفرة أمامهم للتعامل مع المواد المعنية.

تساعد النصائح التالية الوالدين على إدارة المخاطر العامة للشبكات الاجتماعية بخصوص الأطفال الصغار والأطفال الكبار والمراهقين.

الأطفال الصغار

بصفة عامة سيكون للأطفال الصغار تداخل مباشر محدود في الشبكات الاجتماعية لعدم تلبيتهم الشروط التوجيهية الموصى بها والمتعلقة بالسِن وهناك بعض مواقع الشبكات الاجتماعية التي تستهدف الأطفال وتدعي الاعتدال في عمليات الاتصال لتوفير مزيد من الحماية للأطفال وقد يطلب طفلك استخدام واحد من هذه المواقع في مرحلة ما، لذا قد تكون النصائح التالية مفيدة:

1. إذا كان طفلك يستخدم خدمات التواصل الاجتماعي، بما في ذلك مواقع الألعاب والعوالم الافتراضية التي تسمح لهم بالاتصال مباشرة مع الآخرين، تحقق من المبادئ التوجيهية المتعلقة بالسِن ومن سياسات الخصوصية لهذه المواقع وتحقق من كيفية فرضها للاعتدال- وهل يقوم الإداريون بفحص جميع الرسائل قبل نشرها؟ هل أنت مقتنع بأن طفلك يتفاعل على الانترنت بشكل آمِن؟
2. ضع قواعد وضوابط وتأكد من أنَّ طفلك يعرف ماهية المعلومات التي يمكن نشرها على الانترنت وماهية المواقع التي يستطيعون زيارتها ويمكن الطلب منهم إبلاغكم قبل إرسالهم أية معلومات شخصية عبر الإنترنت، بما في ذلك الاسم الكامل، واسم الأم أو الأب، أو عنوان المدرسة.
3. ساعد طفلك على إنشاء "أسماء شاشة" أو "هويات تعريف" لا تتضمن نوع الجنس أو العمر أو اسم المكان الذي يتواجد فيه.
4. ضع قواعد حول أنواع المحتوى أو المعلومات التي يمكن تقديمها إلى شخص بالغ. ، قد تكون من القواعد على سبيل المثال: "أبلغ أمك أو أبيك إذا طلب منك شخص عنوان المدرسة أو المكان الذي تعيش فيه" و " أبلغ أمك أو أبيك إذا تحدث أحدهم اليك عن أشياء بذيئة."
5. انصح طفلك باستشارتك قبل النقر على أية وصلات أرسلت اليه من قبل آخرين على مواقع الشبكات الاجتماعية لأنَّ هذه الوصلات قد تؤدي إلى محتوى مخصص للبالغين.
6. ساعد طفلك على فهم أهمية ما يقوله ويفعله على الانترنت وشجعه على استخدام نفس الأخلاقيات التي يستخدمها في الواقع عند التواصل مع الآخرين وشجعه على الإبلاغ عن الاشخاص الذين لا يتصرفون بلياقة.
7. قدِّم المشورة لطفلك حول عدم الاستجابة لأية رسائل سلبية وضرورة إبلاغ شخص بالغ آخر موثوق به عن هذه الرسائل السلبية وضرورة حفظها.

الأطفال الأكبر سنا

1. إذا كان طفلك يستخدم خدمات التواصل الاجتماعي تحقق من المبادئ التوجيهية الخاصة بالعمر والشروط والأحكام الخاصة بالموقع. إن من المفيد بشكل عام أن تنظر فيما إذا كنت مرتاحا للمحتوى ولإمكانية الاتصال مع الآخرين بما في ذلك المراهقين والبالغين.وتسائل فيما إذا كان طفلك مستعداً اجتماعيا لإجراء اتصال مع أشخاص غرباء يحتمل أن يكونوا سيئي النية.
2. ساعد طفلك على إعداد ملفه الشخصي للتأكد من أنه لا يعرض الكثير من المعلومات الشخصية على الانترنت وساعده على إنشاء أسماء الشاشة أو المعرفات التي لا تُخبر بنوع الجنس أو العمر أو الإسم أو موقع السكن والتي لا تكون مثيرة جنسيا.

3. ضع مجموعة من القواعد وتأكد من معرفة طفلك بماهية المعلومات التي يمكن مشاركتها مع الآخرين والمعلومات التي يمكن نشرها على الانترنت واطلب منه إبلاغك قبل ان ينضم الى مواقع جديدة وقبل أن يرسل أية معلومات شخصية عبر الإنترنت، بما في ذلك الاسم على نحو كامل أو عنوان المسكن أو المدرسة.
4. قدِّم المشورة لطفلك على عدم الرد على أي رسائل سلبية وعلى أن يقوم بإبلاغك أو إبلاغ أي شخص بالغ آخر موثوق به عن أي رسائل سلبية يتلقاها.
5. ضع قواعد حول نوع المتصلين الذي ينبغي الإبلاغ عنهم لشخص بالغ، فعلى سبيل المثال قد تكون احدى القواعد "أبلغ أمك أو أبيك إذا سألك متصل عن ملابسك الداخلية أو عن الأجزاء الحساسة من جسمك.
6. طَمئِن طفلك بأنك لن تحرمه من استخدام الإنترنت إذا أفصح عن شعوره بعدم الراحة أو الأمان عند تصفح الإنترنت إذ أن هذا الحرمان يُعَد مصدر قلق حقيقي وكبير للأطفال قد يمنعهم من الحديث إليك بصراحة.
7. انصح طفلك باستشارتك قبل النقر على أية وصلات أرسلت اليه من قبل آخرين على مواقع الشبكات الاجتماعية لأنَّ هذه الوصلات قد تؤدي إلى محتوى مخصص للبالغين.
8. ذَكِّر طفلك بالتواصل مع الآخرين عبر الإنترنت بشكل مناسب و ذَكِّره بأن يقوم بإبلاغك أو إبلاغ أي شخص بالغ أهلٍ للثقة عن أية محاولات بلطجة قد يتعرض لها من الآخرين.
9. تحدث مع طفلك عن وجود خدمات تحديد المكان التي تمكن مستخدمي الشبكات الاجتماعية من تحديد الأماكن الفعلية لتواجد المستخدمين الآخرين من خلال تفعيل هذه الوظيفة فيما تترك بعض الخدمات للناس امكانية تحديد مواقع أصدقائهم عبر وظائف تقوم بتفعيل مزايا تحديد المكان بشكل افتراضي. يمكن لطفلك مراجعة هذه الإعدادات وحجب هذه الوظيفة أو الحَد مِمَّن يستطيع رؤية معلوماته الخاصة بموقع تواجده، ذَكِّر ابنك أن السماح للغرباء بالاطلاع على مكان تواجده أو تواجد أقرانه يُعتَبَر سلوك محفوف بالمخاطر.
10. يمكن أيضا الاتصال بشركة الهاتف المحمول للحصول على المساعدة بشأن حجب خدمة الإنترنت وتقنية البلوتوث ونظام تحديد المواقع من على هاتف طفلك المحمول للحد من قدرته على إخطار الآخرين عن أماكن وجودهم.
11. فكر في استخدام الفلاتر والعلامات والمناطق الآمنة للمساعدة في إدارة مستوى وصول طفلك الى الانترنت.

المراهقون

1. تحدث مع من هم في سن المراهقة حول إدارة المعلومات الشخصية على مواقع الشبكات الاجتماعية.وشجعهم على عدم وضع أية معلومات شخصية على ملفاتهم الشخصية الرئيسية وهذا يشمل رقم الهاتف، عناوين المسكن والمدرسة، ومعلومات عن أماكن العمل أو النوادي.
2. ذكِّره بعدم نشر صور له أو لغيره لا يرتضي بأن يراها الغرباء أو صور قد يكون لها أثر سلبي على طريقة تفسير الآخرين للغاية من عرضها.
3. تأكد من فهمه لمزايا الخصوصية خاصة كيفية إعداد ملفه الشخصي بوضعية "خاص/شخصي" وكيفية الحد من وصول الآخرين إلى معلوماته وشجِّعه على تدقيق الأصدقاء عبر الانترنت.
4. ذَكِّره بأن ليس كل من على الشبكه هم حقا من يدعون أنَّهم هم، فعلى الرغم من المتعة التي قد يشعرون بها عند امتلاك الكثير من الأصدقاء عبر شبكة الإنترنت تسمح إضافة أناس لا يعرفونهم على 'قوائم الأصدقاء" لهؤلاء الناس بمعرفة كل شيء عنهم وقد تُستَخدَم هذه المعلومات في عمليات الغش أو المطاردة الإلكترونية.
5. تحدث معه حول استخدام الخدمات المُعتَمِدة على تحديد المكان كخدمات فورسكواير والفيسبوك والتي تتيح تحديد المكان الفعلي لمستخدمي الشبكات الاجتماعية بمجرد تسجيل الدخول لها فيما تتيح بعض هذه الخدمات للناس امكانية تحديد أماكن أصدقائهم وقد تحتوى على وظائف لتحديد المكان التي يجري تفعيلها بشكل افتراضي. يمكن للمراهق مراجعة إعداداته لحجب هذه الوظائف أو الحد مِمَّن يستطيع رؤية معلوماته الخاصة بموقع تواجده، ذَكِّر ابنك أن السماح للغرباء بالاطلاع على مكان تواجده أو تواجد أقرانه يُعتَبَر سلوك محفوف بالمخاطر.
6. يمكن أيضا الاتصال بشركة الهاتف المحمول للحصول على المساعدة بشأن حجب خدمة الإنترنت وتقنية البلوتوث ونظام تحديد المواقع من على هاتف طفلك المحمول للحد من قدرته على إخطار الآخرين عن أماكن وجودهم.
7. شَجِّعه على إبقاء صداقاته على الانترنت مقصورة على الانترنت، وإذا أراد أن يلتقي أحداً لم يسبق له اللقاء به فينبغي عندها أن يطلب من أحد والديه أو من شخص بالغ آخر موثوق به الذهاب معه وليكن اللقاء دائماً في مكان عام ويُفَضَّل أن يكون خلال النهار.
8. ذَكِّره بعدم الاستجابة إذا ما أرسل أحدهم رسائل سلبية أو طلب شيئا يبعث على عدم الارتياح وبضرورة إبلاغ شخص بالغ آخر موثوق به عن هذه الرسائل السلبية وضرورة حفظها.
9. شَجِّعه على إنشاء حساب منفصل للتواصل مع الشبكات الاجتماعية اذا ما أرادوا الترويج لأنفسهم أو لاهتمام ما والتواصل مع أمثالهم من الاشخاص الذين لا يعرفونهم حاليا وينبغي التأكد من خلو الموقع من معلوماتهم الشخصية.

المحتوى غير اللائق

قد يكون الأطفال عرضة لرؤية مواد غير ملائمة أو حتى مُضِرَّة لهم عبر الإنترنت، إذ يمكن لهذه المادة أن تكون ذات محتوى جنسي صريح أو بذئ أو عنيف وقد يكون المحتوى أيضا عنصري ويدعو الى كراهية مجموعات معينة أو يكون على شكل مادة تشجع على سلوكيات غير آمنة كتلك التي تسبب اضطرابات غذائية خطيرة (كاتباع وصفات وحِميات غذائية ما). وتختلف المواد التي تعتبر غير لائقة تبعا للمعايير والقِيَم الأسرية والثقافية.

- **كيفية وصول الأطفال إلى المحتويات غير اللائقة؟**

قد لا يتعمد الأطفال والشباب البحث عن محتوى غير لائق وقد يتعرضوا لمثل هذا المحتوى عن غير قصد من خلال أنشطة قد تكون بخلاف ذلك غير ضارة، مثل:

1. نتائج غير متوقعة من عمليات البحث على الانترنت
2. النقر على وصلات غير معروفة ضمن المواقع أو ضمن رسائل البريد الإلكتروني
3. كتابة عنوان ويب بشكل غير صحيح أو النقر على أحد الإعلانات المنبثقة(pop-ups)
4. النقر على محتوى لعبة على الانترنت أو على أحد عروض الجوائز.

يتعمَّد الأطفال والشباب في بعض الحالات الوصول الى مواد غير ملائمة، لا سيما أثناء الانتقال الى مرحلة المراهقة وقد يكون ذلك من باب الفضول أو لمشاركتها مع الزملاء لتحقيق ما يعرف بـ "قيمة الصدمة" للمحتوى.(shock value)

- **ما هي المحتويات المحظورة عبر الإنترنت؟**

يمكن لبعض المحتوى الذي يعتبر غير لائق أن يكون محظوراً أو غير قانوني أيضا في دولة الإمارات العربية المتحدة.

وعلى الرغم من وجود برامج تصفية على مستوى وطني تقوم بعمل جيد في تصفية المحتويات المحظورة إلا أنَّه يمكن لبعض هذا المحتوى أن ينفذ من خلال برامج التصفية لذا ينبغي إطلاعك على قوانين دولة الإمارات العربية المتحدة لفهم أنواع المحتويات والسلوكيات غير القانونية في دولة الإمارات العربية المتحدة.

بالنسبة للأطفال من المهم للآباء والأمهات محاولة الحد من تعرض الطفل لمحتويات غير لائقة. وهناك طريقة جيدة للقيام بذلك من خلال استخدام مرشحات/مصفيات الإنترنت.

تُمَكِّن مُرَشِّحات الحاسوب الشخصي والعلامات والمناطق الآمنة الوالدين من الحد من مخاطر تَعَرُّض الأطفال للمواقع غير المناسبة أو غير القانونية وتُمَكِّن أيضاً من وضع حدود زمنية للاتصال بالإنترنت. عند البت في ماهية الأدوات الأنسب لأسرتك، قد يكون من المفيد النظر في مستوى التوجيه اللازم منك وموازنته مع أعمار أطفالك ومدى المحتوى الذي قد يحتاجون إلى الوصول إليه.

مُرَشِّحات الحاسوب الشخصي هي برامج على الكمبيوتر الخاص بك تقدم مجموعة واسعة من الوظائف المختلفة لمنع، أو حجب أو مراقبة المحتويات غير اللائقة ويمكن أيضا تخصيص اعدادات العديد من الفلاتر لتتناسب مع أنشطة الإنترنت لكل مستخدم.

ومن السمات الشائعة لمرشحات الحاسوب الشخصي ما يلي:

1. "حجب الفئة category blocking" والتي تُمَكِّن المستخدم من الاختيار من بين مجموعة من فئات المحتوى (على سبيل المثال العنف، والمواد الإباحية) وتقرر عندها أي منها سيتم حجبه أو فرض قيود زمنية عليه تُمَكِّن المُستَخدم من قَصر الوصول إلى الإنترنت على أوقات معينة من اليوم، بما في ذلك مقدار الوقت الذي يمكن للطفل تمضيته على شبكة الانترنت. ويمكن لهذا أن يضمن اقتصار امكانية استخدام الأطفال لشبكة الانترنت أثناء تواجد الآباء للإشراف عليهم ويمكن أن يحد من استخدام الشبكة في أوقات متأخرة من الليل وهي أوقات مغرية لبعض المراهقين.
2. الدخول الذي يُمَكِّن أولياء الأمور من تتبع وتسجيل تاريخ بالمواقع التي تم زيارتها من خلال خدمة الحجب المُستخدمه مع طفلهما والتي تتيح للمستخدمين منع أو تصفية الحصول على خدمات معينة، مثل خدمة النظير للنظير peer-to-peer، وخدمات الشبكات الاجتماعية أو الألعاب عبر الإنترنت.

لا تعتبر مرشحات الإنترنت بديلا عن توجيه وإشراف الوالدين إذ لا يمكن لأداة تصفيةٍ حجبَ كافة المواد غير المناسبة، ولأنَّ شبكة الإنترنت واسعة ودائمة التغيُّر، لا بد من القيام بتحديث قوائم المواقع المحجوبة باستمرار لضمان عمل المُصَفي بفعالية. ومع ذلك ستبقى هناك بعض المواقع غير المرغوب فيها التي تستطيع النفاذ من خلال هذا المُصَفي.

تُرفق أدوات وضع العلامات" labeling tools بطاقات تعريفية tags " بالمواقع ويمكن لمعظم المتصفحات قراءة هذه البطاقات التعريفية لتمنع الوصول إلى هذه المواقع أو لتقدم المشورة عندما لا تكون المواقع مناسبة للأطفال إذا تم برمجتها لتفعل ذلك وتصبح البطاقات التعريفية بذلك أداة مُكَمِّلة لأدوات التصفية.

تُوضَع العلامات على المواقع لتحديد مدى ملاءمتها للأطفال أو لتحديد نوع المواد التي تحتويها، على سبيل المثال: نشاط جنسي متوسط.

تُمَكِّن هذه الأدوات، جنبا إلى جنب مع متصفح الويب المستخدمين من تعيين مستويات الوصول للمواقع التي تحمل علامات، ومنع الوصول إلى أي شيء فوق تلك المستويات، كما وتتيح بعض المتصفحات للمستخدمين تقييد الوصول إلى مواقع لا تحمل علامات.

في حين أن وضع العلامات يعتبر أداة مفيدة، إلا أنَّ معظم المواقع لا تزال بدون علامات.

المناطق الآمنة هي شبكات آمنة تتيح الوصول إلى مجموعة من المواقع المصممة خصيصا للأطفال بقليل من خطر التعرض لمحتوى غير لائق، العديد من المناطق الآمنة مجانية لكن بعضها يتطلب اشتراك وتسجيل دخول وكلمة مرور كونها محمية من خطر غيرها من المناطق على شبكة الانترنت.

تساعد النصائح العامة التالية الوالدين على إدارة مخاطر المحتويات الغير لائقة بالنسبة لصغار وكبار الأطفال وبالنسبة للمراهقين.

الأطفال الصغار

قد يتعرض صغار الأطفال لمحتوى غير لائق أو غير قانوني عبر الإنترنت عن طريق الصدفة أو بتشجيع من آخرين كالأشقاء الأكبر سنا.

ويمكن للنصائح التالية أن تساعدك على توجيه الأطفال الصغار فيما يتعلق بالأنشطة التي يقومون بها عبر الإنترنت.

3. يجب أن يكون استخدام الأطفال للإنترنت في هذا العمر مُراقباً عن كثب وللمساعدة في هذا ينبغي محاولة إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.
4. كن على علم بكيفة استخدام أطفالك للإنترنت، واستكشفها معهم. قم بتعيين قائمة بالمواقع المفضلة التي تكون مرتاحاً لزيارة أطفالك لها وعلِّمهم كيفية الوصول إلى هذه القائمة.
5. علم طفلك أنه ليس كل شيء على الكمبيوتر آمن للنقر عليه وقد يكون من المفيد أن نضع قاعدة بضرورة لجوء الأطفال الصغار الى استشارة الأشخاص البالغين قبل قيامهم بالنقر وفتح أشياء جديدة أو غير معروفة.
6. علم طفلك بأن هناك وسائل يستطيعون بواسطتها التعامل مع المواد الذي تبعث فيهم القلق أو الخوف، إذ ينبغي عدم الاستجابة عند استلام ما هو غير لائق، ومن الضروري إبلاغ شخص بالغ وموثوق على الفور إذا شعر الأطفال بعدم الارتياح.
7. علم طفلك كيفية إغلاق صفحة الويب أو إيقاف الشاشة واستدعاء شخص بالغ وموثوق إذا احسوا بالقلق اتجاه ما يرونه.
8. إذا تعرض طفلك لمحتوى غير لائق وبدى عليه الحزن لذلك ، تحدث إليه حيال ذلك وقم بطلب المشورة الفنية إذا تطلب الأمر.
9. فكر في استخدام الفلاتر، والعلامات والمناطق الآمنة للمساعدة في إدارة حدود وصول طفلك الى الانترنت.

الأطفال الأكبر سنا

قد يتعرض الأطفال الأكبر سناً لمحتوى غير لائق أو غير قانوني عبر الإنترنت عن طريق الصدفة أو عن طريق البحث عنه بأنفسهم بتشجيع من زملائهم.ويمكن للنصائح التالية أن تساعد الأطفال الأكبر سناً في التعامل مع المحتويات التي يواجهونها عبر الإنترنت.

10. يجب أن يكون استخدام الأطفال للإنترنت في هذا العمر مُراقباً عن كثب وللمساعدة في هذا ينبغي محاولة إبقاء جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل.

<=="" li="" style="margin: 0px; padding: 0px;">

11. علم طفلك أن هناك طرقا للتعامل مع المواد المزعجة، إذا لا ينبغي لهم الرد عند استلام مادة غير لائقة بل ينبغي عليهم إبلاغ شخص بالغ وموثوق إذا ما شعروا بعدم الراحة أو القلق.
12. طَمئِن طفلك بأنك لن تحرمه من استخدام الإنترنت إذا أفصح عن شعوره بعدم الراحة أو الأمان عند تصفح الإنترنت إذ أن هذا الحرمان يُعَد مصدر قلق حقيقي وكبير للأطفال قد يمنعهم من الحديث إليك بصراحة.
13. علم طفلك كيف يغلق صفحات الويب التي لا تعجبه أو كيف يغلق الشاشة وينادي شخص بالغ وموثوق.
14. إذا تعرض طفلك لمحتوى غير لائق وبدى عليه الحزن لذلك ، تحدث إليه حيال ذلك وقم بطلب المشورة الفنية إذا تطلب الأمر.
15. فكر في استخدام الفلاتر والعلامات والمناطق الآمنة للمساعدة في إدارة مستوى وصول طفلك الى الانترنت.

قد يتعرض المراهقون لمحتوى غير لائق أو غير قانوني عبر الإنترنت عن طريق الصدفة أو عن طريق البحث عنه بأنفسهم ويمكن للنصائح التالية أن تساعدهم على التعامل مع المحتويات التي يواجهونها عبر الإنترنت

16. يجب الأخذ بعين الاعتبار أن بعض المواقع تشجع السلوكيات غير القانونية كأعمال العنف أو السلوكيات الضارة مثل حميات الطعام الضارة. فكر في نقاط ضعف المراهق أمام الحصول على المعلومات وتحقق مما يقومون بمشاهدته عبر الإنترنت.
17. حاول أن يكون جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل خاصة إذا كان ابنك المراهق ضعيفاً، كأن يكون يعاني من مشاكل عقلية أو سلوكية.
18. علم إبنك أن هناك طرقا للتعامل مع المواد المزعجة، إذا لا ينبغي لهم الرد عند استلام مادة غير لائقة بل ينبغي عليهم إبلاغ شخص بالغ وموثوق إذا ما شعروا بعدم الراحة أو القلق على أنفسهم أو على أصدقائهم.
19. طَمئِن المراهق بأنك لن تحرمه من استخدام الإنترنت إذا أفصح عن شعوره بعدم الراحة أو الأمان عند تصفح الإنترنت إذ أن هذا الحرمان يُعَد مصدر قلق حقيقي وكبير للأطفال قد يمنعهم من الحديث إليك بصراحة.
20. شَجِّع المراهق على الانتباه الى الأصدقاء وإذا كان يعرف عن صديق يقوم بالوصول إلى محتوى يبدو أنه يؤثر عليه سلبا فعليه التعبير عن ذلك أمام صديقه وعليه إذا لزم الأمر إبلاغ شخص بالغ وموثوق عن ذلك دون الافصاح عن هويته.
21. إذا تعرض المراهق لمحتوى غير لائق وبدى عليه الحزن، تحدث إليه حيال ذلك وقم بطلب المشورة الفنية إذا تطلب الأمر
22. يمكن للمدرسة التي يدرس فيها ابنك أن أن تقوم بتقديم المساعدة أو التوجيه.
23. فكر في استخدام الفلاتر والعلامات والمناطق الآمنة للمساعدة في إدارة مستوى وصول طفلك الى الانترنت.

الإفراط في استخدام الإنترنت

يبدو لكثير من الآباء كما لو كان أطفالهم وأبناؤهم من الشباب متواجدون على الانترنت بصفة دائمة فهم على الغالب يقومون بعدة مهام في نفس الوقت، على سبيل المثال تحميل الملفات والاستماع إلى الموسيقى أثناء الدراسة والدردشة مع الأصدقاء أو إرسال الرسائل من هواتفهم المحمولة.
يمكن لعدد الساعات التي يقضيها الأطفال والشباب على الانترنت أن تتفاوت تفاوتا كبيرا، إذ لا يوجد توجيه عام يحدد الكمية الصحيحة من الوقت الذي يمكن للأطفال قضاؤه على الانترنت، ولكن إذا ما تبين بأن سلوكهم على الإنترنت قد بدأ بالتأثير سلبا على سلوكهم أو عافيتهم أو سلوك وعافية الأسرة يتحتم عندها مناقشة سقف توقعاتهموضع حدود زمنية لاستخدام الإنترنت

متى يكون الاستخدام مفرطاً

يمكن للتغييرات الملحوظة على سلوك الأطفال والشباب أثناء استخدام الإنترنت وخارجه أن تكون مؤشرات داله على الإفراط في استخدام الإنترنت. وتشمل هذه السلوكيات ما يتعارض مع صحتهم العامة وعافيتهم كالهوس بمواقع أو ألعاب معينة، وظهور القلق أو الشد العصبي عند الابتعاد عن الكمبيوتر، وقضاء أوقات متزايدة على الانترنت، والتعب المفرط، وانخفاض الأداء الأكاديمي، وعند الانعزال أو الابتعاد عن الأصدقاء والأنشطة خارج شبكة الإنترنت.
قد يكون بعض هذه المؤشرات سلوكيات تطوُّرية تتناسب مع سن الشباب وخصوصاً من هم في سن المراهقة، وقد تكون بدلاً من ذلك عبارة عن مؤشرات لقضايا أخرى مهمة كبلطجة الإنترنت والمصاعب المتعلقة بالصداقات وقضايا الصحة العقلية.
إذا كان لديك مخاوف بشأن سلوك طفلك على الانترنت أو خارجها وخصوصاً التغيرات التي تطرأ على المزاج أو السلوك، ناقش مخاوفك معه والجأ إذا لزم الأمر الى ذوي الاختصاص لمساندة طفلك.
تساعد النصائح التالية الوالدين على التعامل مع قضية الإفراط في استخدام الإنترنت من قبل الأطفال الصغار والكبار ومن قبل المراهقين.

الأطفال الصغار

من غير المحتمل أن يكون لدى الأطفال الصغار مشاكل تتعلق بقضاء الكثير من الوقت على شبكة الانترنت بسبب محدودية وصولهم اليها وبسبب محدودية قدراتهم. إذا كان الأطفال يستخدمون أجهزة الكمبيوتر ويقومون بالتفاعل عبر الإنترنت فمن المهم أن يبدء الآباء والأمهات بتثقيفهم حول مستويات الاستخدام المناسب.

1. فكر في إنشاء قواعد تحدد الوقت الذي يمكن للأطفال فيه لعب الألعاب عبر الإنترنت أو استخدام شبكة الانترنت والمدة التي يمكن تمضيتها في ذلك، ويمكن الاتفاق مع الطفل على تحقيق توازن بين مجموعة من الأنشطة يمارسها عبر الإنترنت وبين أنشطة أخرى خارج الشبكة كاللعب في الخارج أو الرسم.
2. يمكن لوضع القواعد الخاصة بالأطفال منذ الصغر أن تساعدهم على إدارة أنشطتهم عبر الإنترنت أثناء تقدمهم في السن وزيادة نشاطهم على الانترنت.
3. حاول أن تضع جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل لتعرف مقدار الوقت الذي يقضيه طفلك على الانترنت.
4. إذا كان لديك مخاوف بشأن سلوك طفلك على الانترنت أو خارجها ناقش مخاوفك معه والجأ إذا لزم الأمر الى ذوي الاختصاص لمساندة طفلك.
5. إذا كان الطفل في سن المدرسة، فيمكن لمدرسته أن توفر التوجيه والدعم.

الأطفال الأكبر سنا

يقضي العديد من الأطفال كبار السن وقتهم على شبكة الانترنت بالتعارف والدراسة والترفيه ولا توجد قاعدة توجيهية بخصوص مقدار الوقت الذي يمكن للأطفال قضاءه على الانترنت، ولكن إذا أصبح سلوكهم على الإنترنت يؤثر سلبا على سلوكهم أو عافيتهم أو سلوك وعافية الأسرة يتحتم عندها مناقشة سقف توقعاتهم ووضع حدود زمنية لاستخدام الإنترنت.

1. تنبه للمؤشرات الدالة على قضاء الطفل لوقت طويل على الإنترنت مثل تدني الاهتمام بالأنشطة الأخرى والتحدث باستمرار عن لعبة أو نشاط على الانترنت وانخفاض التحصيل الدراسي والسخط عند الابتعاد عن اللعب على الانترنت وقد يساورك الشك حول قيام بعضهم بالسهر بعد وقت النوم المحدد لممارسة ألعاب الكمبيوتر.

<=="" li="" style="margin: 0px; padding: 0px;">

2. قد ترغب في التحقق من خلال مدرسة طفلك من إمكانية مواجهته لمشاكل تتعلق بالحدود الزمنية لفروضه المدرسية أو جودة أداءها ومن ظهور التعب عليه.
3. النظر في إنشاء قواعد حول الوقت الذي يمكن فيه للأطفال اللعب أو استخدام الإنترنت والمدة التي يمكن لهم أن يقضوها كل يوم ويمكن النظر في الوصول الى اتفاق مع الطفل حول تحقيق توازن بين مجموعة الأنشطة التي يمارسها عبر الإنترنت والأنشطة الأخرى مثل اللعب خارج المنزل وعمل الواجبات الدراسية المنزلية والقيام بالأعمال المنزلية. ومن المفيد تجريب هذه القواعد الجديدة لمدة أسبوعين للتأكد من أنَّها توفر توازنا مناسباً لطفلك وعائلتك.

4. يمكن لوضع القواعد الخاصة بالأطفال منذ الصغر أن تساعدهم على إدارة أنشطتهم عبر الإنترنت أثناء تقدمهم في السن وزيادة نشاطهم على الانترنت.
5. حاول أن تضع جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل لتعرف مقدار الوقت الذي يقضيه طفلك على الانترنت.
6. إذا كان لديك مخاوف بشأن سلوك طفلك على الانترنت ناقش مخاوفك معه والجأ إذا لزم الأمر الى ذوي الاختصاص لمساندة طفلك.
7. يمكن للمدرسة التي ينتمي لها ابنك أن توفر التوجيه والدعم.

المراهقون

يقضي العديد من المراهقين وقتاً معتبراً على شبكة الانترنت بالتعارف والدراسة والترفيه وتشكل الأنشطة التي يمارسونها على شبكة الإنترنت بالنسبة لهم جزءا من هويتهم الاجتماعية، ولكن يبقى من المهم أن يرعي المراهقون أنفسهم لتحقيق التوازن بين التفاعل عبر الانترنت وعبر الجوانب الأخرى من حياتهم.

لا توجد قاعدة توجيهية بخصوص مقدار الوقت الذي يمكن للمراهقين قضاؤه على الانترنت، ولكن إذا أصبح سلوكهم على الإنترنت يؤثر سلبا على سلوكهم أو عافيتهم أو سلوك وعافية الأسرة يتحتم عندها مناقشة سقف توقعاتهم ووضع حدود زمنية لاستخدام الإنترنت.

1. تنبه للمؤشرات الدالة على قضاء المراهق لوقت طويل على الإنترنت مثل تدني الاهتمام بالأنشطة الأخرى والتحدث باستمرار عن لعبة أو نشاط على الانترنت وانخفاض التحصيل الدراسي والسخط عند ابتعادهم عن اللعب على الانترنت وقد يساورك الشك حول قيام بعضهم بالسهر بعد وقت النوم المحدد لممارسة ألعاب الكمبيوتر والدردشة مع الآخرين.
2. قد يبدو المراهق متعباً تماما خلال النهار وقد يعمد الى تتخطى وجبات الطعام ليتجنب ترك جهاز الكمبيوتر.
3. قد ترغب في التحقق من خلال مدرسة ابنك المراهق من إمكانية مواجهته لمشاكل تتعلق بالحدود الزمنية لفروضه المدرسية أو جودة أداءها.
4. إذا برزت المشاكل فانظر في وضع قواعد تنظم الوقت الذي يمكن فيه للمراهقين اللعب أو استخدام شبكة الانترنت والمدة اليومية المسموحة لذلك. ويمكن النظر في التوصل الى اتفاق معه حول تحقيق توازن بين مجموعة الأنشطة التي يمارسها عبر الإنترنت والأنشطة الأخرى ويجدر بك تحديد العواقب المترتبة على إخلاله بالاتفاق فإذا أخفق في القيام بما هو مطلوب منه على سبيل المثال، يترتب على ذلك فرض تحديدات على ممارسته الألعاب عبر الانترنت.
5. حاول أن تضع جهاز الكمبيوتر في مكان مشترك أو مرئي في المنزل لتعرف مقدار الوقت الذي يقضيه ابنك على الانترنت.
6. إذا كان لديك مخاوف بشأن سلوك المراهق على الانترنت ناقش مخاوفك معه والجأ إذا لزم الأمر الى ذوي الاختصاص لمساندته.
7. يمكن للمدرسة التي ينتمي لها ابنك أن توفر التوجيه والدعم.

الهواتف المحمولة

تعتبر الهواتف المحمولة وسيلة رائعة للمحافظة على تواصل الأطفال مع ذويهم ومع وأصدقائهم إذ تتيح الهواتف المحمولة للمستخدمين إجراء المكالمات والتقاط الصور ولعب الألعاب، وإرسال الرسائل النصية (SMS) ورسائل الوسائط المتعددة (MMS)الى جانب الوصول إلى الإنترنت.

على الرغم من توفير الهواتف النقالة الاتصال المباشر ومتعة الاستخدام، لكن حقيقة أن كونها متاحة 24 ساعة في اليوم وعدم وجودك على نحو دائم للإشراف يعني وجود مخاطر محتملة بالنسبة للأطفال والشباب، ومن هذه المخاطر ما يلي:

1. التكاليف المفرطة الناجمة عن المكالمات والرسائل والخدمات المميزة وعمليات التحميل،
2. حصول الأطفال على مدخل الى شبكة الانترنت دون رقابة وضوابط من الوالدين،
3. حصول الأطفال على امكانات نظام تحديد الموقع العالمي GPS والبلوتوث التي قد تمكن الآخرين من تحديد مواقعهم،
4. استلام الأطفال لمحتويات غير مرغوبة بما في ذلك المحتويات المسيئة أو محتويات تنطوي على البلطجة عبر الانترنت،
5. قدرة الأطفال على مشاركة الصور الشخصية بما في ذلك صورهم العارية أو ما يعرف بتبادل الصور والرسائل الجنسية عبر المحمول."sexting"

• تكاليف الهاتف المحمول

هناك العديد من خدمات الهاتف المحمول المختلفة المتاحة للاستخدام لقاء رسوم وتعرفات متفاوتة، ولا يحتاج المستخدم في بعض الحالات، كما في الخدمات المدفوعة مسبقا الى توقيع عقد للخدمة المستمرة بينما يتطلب غيرها من الخدمات توقيع عقدٍ قد يسري لسنوات عديدة، تتفاوت تكلفة المكالمات والرسائل النصية وعمليات التنزيل بين مزودي خدمة الهاتف المحمول. فقبل اختيار الهاتف والخدمة يجدر التدقيق في الشروط والأحكام، لتعرف فيما إذا كان الهاتف مضمناً في العقد وما هي عواقب فقدان طفلك للهاتف إضافة الى طول مدة العقد وكلفة مختلف أنواع الخدمات بما في ذلك الرسائل القصيرة والمكالمات الهاتفية والاتصال بشبكة الإنترنت.

تستمر عقود تزويد الخدمة لفترة محددة، تقوم خلالها شركة الهاتف المحمول بتزويد العميل بخدمات الاتصال بالشبكة وأحيانا خدمة استخدام الهاتف وعدد معين من المكالمات والرسائل القصيرة (الرسائل النصيّة) واستخدام البيانات شهرياً وإذا ما تم تجاوز عدد الرسائل النصيّة أو المكالمات أو حد التنزيل المسموح في نهاية كل شهر فمن الممكن أن تترتب على ذلك رسوم باهضة جدا.

توفر خدمات الهاتف المحمول المدفوعة مسبقا المزيد من السيطرة على المبلغ الذي يتم إنفاقه وبدلا من الالتزام بعقد مستمر، يتم شراء الرصيد من مزود الخدمة لاستخدام الهاتفويتم تطبيق قائمة أسعار تنكبق على الرسائل القصيرة والمكالمات واستخدام

البيانات، وبمجرد نفاذ الرصيد لا بد من إعادة تعبئته قبل أن تتمكن من التمتع بخدمات الهاتف باستثناء خدمة الاتصال بالطوارئ (999) التي تبقى فعالة.

بعض شركات الهاتف النقال تقدم أيضا عروض على أساس شهري دون وجود عقد بشروط ثابتة مما يوفر للعملاء قدر أكبر من المرونة مع هواتفهم الخاصة.

عند جعل الهاتف متاحاً لطفلك، ينبغي النظر في ما إذا كنت بحاجة الى تحديد استخدامه للهاتف النقال أو فيما إذا كان مسؤولاً الى حدٍ كافٍ لفهم كيفية إدارة هاتفه الخاص وتذكر بأن هذه قد تكون المسؤولية المالية الكبيرة الأولى للعديد من الأطفال وقد يحتاجون الى التوجيه أوالى وجود قواعد لمساعدتهم على فهم وإدارة التكاليف.

خدمات المحمول المميزة

يطلق على خدمات المحمول المميزة غالبا عبارة (الرسائل النصية المميزة) أو (رسائل الوسائط المتعددة)، وتسمى بالمميزة لأنه يتوجب على العملاء دفع تعرفة إضافية مقابل الحصول على هذه الخدمة وهذا يعني أنها تكلف أكثر مما تكلف الرسائل العادية وتختلف تعرفتها وغالبا ما تظهر بأحرف صغيرة في أسفل الإعلان الذي يروج لهذه الخدمة وهذه خدمات رائجة جدا مع الأطفال لأنها توفر الوصول إلى النغمات والخلفيات المستخدمة في الهاتف الجوال والألعاب ومقاطع الفيديو والمقطوعات الموسيقية.

ويتم الوصول عموما إلى خدمات الهواتف المحمولة المميزة من خلال رسالة نصية قصيرة أو عن طريق الاشتراك عبر الإنترنت.

عند الاشتراك بالخدمة المتميزة قد تكون هناك تكلفة لمرة واحدة لخدمة واحدة، أو قد يكون هناك اشتراك جاري، وكلما زادت عدد الرسائل غير المجانية التي يتلقاها الطفل في الأيام أو الأسابيع اللاحقة كلما ترتب عليه تكاليف أخرى، وقد يشترك بعض الأطفال بالخدمة عن غير قصد أو فهم للتكاليف المترتبة عليها ويدرك العواقب عندما ينفذ رصيده الخاص أو عندما تصل الفاتورة.

لمساعدة طفلك في عملية إدارة استخدامه للخدمات المميزة، ينبغي تشجيعه على النظر في بنود وشروط وتكاليف الخدمة قبل الاشتراك أو الطلب من مزود الخدمة إظهار التفاصيل أولاً. يتوجب الاشتراك في خدمات الرسائل المميزة إرسال رسالة نصية إلى جوال المستخدم بعد طلبه الأولي للاشتراك لتأكيد الطلب، شجِّع طفلك على حفظ هذه الرسالة أو تسجيل تفاصيلها لديه ليصبح لديه وسيلة سهلة تساعده على إلغاء الاشتراك عندما يرغب بذلك.

عند الوصول إلى الخدمات التي تتطلب من الأطفال تحميل محتوى من الإنترنت، مثل الألعاب أو مواد الفيديو، قد تتقاضى شركة الهاتف المحمول رسوم اضافية على البيانات التي يتم تحميلها الى جانب الرسوم التي تتقاضاها أصلاً على الرسالة. تحقق من عقد الهاتف ومن بنود وشروط الرسوم المترتبة على تنزيل البيانات.

إذا كنت غير متأكد من قدرة طفلك على إدارة التكاليف، تحدث إلى مزود خدمة الهاتف لحجب امكانية وصوله إلى أرقام الخدمة الممتازة والإنترنت حيث يتوجب على مزودي خدمة الهاتف المحمول حجب خدمات الرسائل المميزة عند الطلب.

سلامة الهاتف المحمول

توفر العديد من الهواتف النقالة خصائص تمكن من استخدام الإنترنت والخدمات التي تعتمد على الموقع، وعلى الرغم من أن هذه الوظائف مفيدة إلا أنها تجلب مخاطر محتملة.

يمكن للهواتف المحمولة توفير خدمة الوصول إلى الإنترنت 24 ساعة في اليوم، وربما دون وجود خدمة التصفية والإشراف التي يمكن تقديمها من خلال حسابات الانترنت المنزلية مما يعني أنَّ الأطفال والمراهقين سيكونوا قادرين على الوصول إلى المحتويات غير اللائقة. وللتعامل مع هذه المخاطر يتحتم على الآباء وضع قواعد تحدد الأوقات الذي يمكن فيها الوصول إلى الإنترنت وأنواع المحتوى التي يمكن دخولها وإذا كنت تشعر بالقلق إزاء دخول طفلك إلى الإنترنت اتصل بشركة الهاتف المحمول للحصول على المساعدة في حجب وظائف الإنترنت عن هاتفه.

تُمكِّن خدمات تحديد المواقع مستخدمي الشبكات الاجتماعية من تحديد مواقعهم الفعلية للآخرين عبر هواتفهم النقالة.وهي خدمة تلاقي شعبية متزايدة في خدمات مثل "فورسكواير" و "فيسبوك"، وباستخدام هذه الوظيفة، يمكن للأطفال والمراهقين استخدام الهواتف النقالة لتحديد الموقع الفعلي للأصدقاء وغيرهم من على مواقع الشبكات الاجتماعية.ويمكن لبعض الأفراد تسجيل الدخول من موقع ما ليعرف الآخرون مكان وجودهم وتقوم بعض خدمات الشبكات الاجتماعية بتشغيل خدمة الموقع افتراضيا.

للتعامل مع هذه الخدمات، شجِّع طفلك على مراجعة الإعدادات الخاصة به على الشبكات الاجتماعية لمنع خاصية تحديد الموقع أو لتحديد الأشخاص القادرين على رؤية معلومات الموقع الخاص به وقد ترغب أيضا في الاتصال بشركة الهاتف المحمول للحصول على المساعدة بخصوص حجب الإنترنت وتقنية بلوتوث ونظام تحديد المواقع عن هاتف طفلك المحمول للحد من قدرته على إخطار الآخرين عن أماكن وجوده وأخباره.

تستخدم الهواتف المحمولة في بعض الأحيان من قبل الأطفال والشباب للبلطجة أو "التَنَمُّر" على بعضهم البعض عبر الانترنت. وللتعامل مع هذه المخاطر ينبغي التحدث مع الأطفال عن "البلطجة الإلكترونية" لتشجيعهم على الإبلاغ عن هذه البلطجة والاتفاق معهم على استراتيجيات لمعالجة البلطجة الإلكترونية قبل وقوعها إذ يجب حفظ رسائل البلطجة الإلكترونية ويمكن الإبلاغ عنها إلى شركات الهاتف النقال، أو في الحالات الخطيرة، إلى الشرطة. يرجى زيارة قسم البلطجة الإلكترونية للمشورة وللحصول على معلومات أكثر تفصيلا.

يشير مصطلح(Sexting) إلى عملية إرسال الصور والرسائل ومقاطع الفيديو الاستفزازية أو الجنسية باستخدام الهاتف المحمول بشكل عام، ويمكن أن تشمل العملية أيضا نشر هذا النوع من المواد على شبكة الانترنت. مع أنَّ مشاركة الصور أو الرسائل النصية الموحية قد يبدو وكأنه مزحة بريئة أو دعابة مضحكة للشباب، إلا أنِّه يمكن أن يكون له عواقب اجتماعية وقانونية خطيرة. للمساعدة في حماية صورة الشباب سواء على الانترنت إو خارجها ينبغي عليهم التنبه الى كيفية التعامل مع ما يخصهم ويخص غيرهم من رسائل وصور.

يقدم هذا القسم النصائح المفصلة التالية للآباء والأمهات من أجل مساعدة الأطفال الصغار والكبار والمراهقين على إدارة تكاليف الهاتف المحمول وقضايا السلامة المتعلقة به.

الأطفال الصغار

في حين أنَّ قلة من الأطفال الصغار يمكنهم الحصول على هواتف محمولة خاصة بهم، قد يتمكن البعض منهم من الوصول الى هاتف والديه أو أشقاءه من وقت لآخر. يمكن للنصائح التالية أن تساعد في توجيه الأطفال الصغار في عملية الاستخدام الآمن للهاتف المحمول:

1. تَعَرَّف على كافة ميزات الهاتف المحمول قبل السماح لطفلك الصغير باستخدامه، ومن المفيد أن يتم وضع قواعد تنظِّم استخدام الأطفال الصغار للمحمول ومن أمثلة ذلك: "يمكنك فقط استخدام الهاتف المحمول للاتصال مع والديك إذا تأخرت الحافلة أو إذا كنت تشعر بالخوف أو القلق."
2. تعرف على كيفية الوصول إلى وإدارة المحتويات "المخصصة للبالغين/المحتويات الجنسية " وغيرها من الخدمات كخدمات الرسائل النصية القصيرة المميزة أو خدمة الدخول إلى الإنترنت وعادة ما تكون هذه المعلومات متاحة على الموقع الالكتروني لناقل الخدمة.
3. ساعد طفلك على فهم أنَّ الهاتف كالمحفظة وأنَّ كل رسالة نصية أو مكالمة هاتفية أو عملية تحميل تكلف مالاً.
4. ذكر طفلك بأنَّه لا ينبغي له بأن يسمح لأحدٍ باستعارة هاتفه المحمول.
5. تحدث مع طفلك عن تجاربه مع هاتفه النقال واجعله يعرف بأنَّه من الممكن له أن يحدثك إن حصل وتعرَّض لشيء سبب له الخوف أو القلق بما في ذلك أية رسائل بذيئة من آخرين.
6. علم طفلك بأن هناك طرقا يستطيع من خلالها التعامل مع المواد التي تقلقه أو تخيفه إذ ينبغي عدم الرد على المواد غير اللائقة التي قد يستلمها بل ينبغي عليه إنهاء المكالمة فوراً وإبلاغ شخص بالغ وموثوق إذا شعر بعدم الارتياح.

الأطفال الأكبر سناً

يمكن أن يمتلك الأطفال الأكبر سناً هواتفهم الخاصة ويمكن أن يكون لهم امكانية الوصول إلى هواتف والديهم وهواتف أصدقائهم ويمكن للنصائح التالية أن تساعد في إرشاد الأطفال الى الاستخدام الآمن للأجهزة المحمولة:

1. كن معنياً في كيفية استخدام ابنك للتقنيات الجديدة واطلب منه أن يريك كيفية تشغيلها واستخداماتها المختلفة وحذِّره من نشر رقم هاتفه أو رقم هاتف أي كان على شبكة الإنترنت وشجعه على إبلاغك عن أية مشاكل قد تواجهه على هاتفه المحمول.
2. ساعد طفلك على أن يدرك بأن كل رسالة نصية ومكالمة هاتفية أو عملية تحميل تكلفة المال، وقد يكون من المفيد وضع قواعد حول الأوقات التي يُسمح فيها للطفل باستخدام الهاتف وينبغي وضع سقف للمبلغ الشهري المسموح له به.
3. إذا كنت تشعر بالقلق إزاء قدرة ابنك المراهق على إدارة فاتورة هاتفه، تَعَرَّف على كيفية ادارة الوصول إلى المحتوى المخصص للبالغين وغيرها كخدمات الرسائل المميزة وخدمة الدخول إلى الإنترنت وعادة ما تكون هذه المعلومات متاحة على الموقع الالكتروني لناقل الخدمة
4. يمكنك النظر في استخدام خدمة البطاقة المدفوعة مسبقاً لطفلك والتي سوف تمكنك من الحد من التكاليف بشكل أكثر سهولة حيث يمكن إجراء مقارنة بسيطة للتكاليف المختلفة وحدود التحميل المترتبة على الخدمة المرتبطة بعقد والخدمة المدفوعة مسبقا لتحدد الخدمة الأفضل بالنسبة لك ولطفلك.
5. ذكر طفلك بأن لا يسمح لأي كان باستعارة هاتفه المحمول وحذره ممن يطلبون استعارة الهواتف بشكل علني.
6. علم طفلك بأن هناك طرقا يستطيع من خلالها التعامل مع المواد التي تقلقه أو تخيفه إذ ينبغي عدم الرد على المواد غير اللائقة التي قد يستلمها بل ينبغي عليه إنهاء المكالمة فوراً وإبلاغ شخص بالغ وموثوق إذا شعر بعدم الارتياح.
7. إذا اصبحت فاتورة ابنك باهظة، اتصل بمجرد حدوث ذلك مع مزود الخدمة الخاص بهاتفه المحمول.

المراهقون

يعتبر العديد من المراهقين من مستخدمي الهواتف المحمولة المتحمسين، وقد تتوفر لديهم هواتف محمولة شخصية أو قد تتوفر لهم امكانية استخدام هواتف اصدقائهم. يمكن أن تساعد النصائح التالية في توجيه المراهق نحو الاستخدام الآمن والمسؤول للأجهزة المحمولة:

1. كن معنياً في كيفية استخدام ابنك للتقنيات الجديدة واطلب منه أن يريك كيفية تشغيلها واستخداماتها المختلفة وحذِّره من نشر رقم هاتفه أو رقم هاتف أي كان على شبكة الإنترنت وشجعه على إبلاغك عن أية مشاكل قد تواجهه على هاتفه المحمول.
2. إذا كنت تشعر بالقلق إزاء قدرة ابنك المراهق على إدارة فاتورة هاتفه، تَعَرَّف على كيفية ادارة عملية الوصول إلى المحتوى المخصص للبالغين وغيرها كخدمات الرسائل المميزة وخدمة الدخول إلى الإنترنت وعادة ما تكون هذه المعلومات متاحة على الموقع الالكتروني لناقل الخدمة
3. انظر مع ابنك المراهق في شروط واحكام خطط اشتراك المحمول المختلفة وتأكد من أنَّه على علم بالتكاليف المحتملة لذلك، ولا سيما تكاليف التحميل من الانترنت وبمقارنة تكاليف وحدود التحميل التي تقدمها خدمة العقد والخدمة المدفوعة مسبقا يمكن تحديد الخدمة الأفضل بالنسبة لك ولطفلك.
4. ساعد المراهقين على فهم التكاليف المحتملة لخدمات الاشتراك وشجِّعهم على التحقق من والشروط والأحكام قبل الاشتراك في الخدمة.
5. ذكر ابنك بأن لا يسمح لأي كان باستعارة هاتفه المحمول ونبهه بأن يبقى على حذر ممن يطلبون استعارة الهواتف بشكل علني – حتى وإن كان ذلك لحالة طارئة حيث يمكن لهم القيام بطلب رقم الطوارئ (999) بأنفسهم لمن هو في حاجة إليه.
6. علِّم ابنك على عدم الرد على المواد غير اللائقة التي قد يستلمها بما فيها الرسائل النصية ذات المحتوى الجنسي وعلِّمهُ بأنَّ عليه إنهاء المكالمة فوراً والقيام بإبلاغ شخص بالغ وموثوق إذا ساوره القلق اتجه ذلك.
7. شجِّع المراهق على الإبلاغ عن أية رسائل شريرة قد يتلقاها لشخص بالغ وموثوق وأن يحفظ الرسالة اذا اقتضى الأمر المتابعة مع مزود الخدمة أو الشرطة.
8. ينبغي على المراهق عدم الرد على الرسائل القادمة من مصادر مجهولة إذ قد تكون هذه الرسائل بقصد الاحتيال.
9. إذا اصبحت فاتورة ابنك باهظة، فاتصل بمجرد حدوث ذلك مع مزود الخدمة الخاص بهاتفه المحمول.

الشبكات الإجتماعية والأصدقاء على الإنترنت

موقع الشبكات الاجتماعية هو موقع على شبكة الإنترنت يوفر مجتمع من الأشخاص لهم مصالح مشتركة ومتماثلة يتيح لهم فرصة التواصل وتبادل الآراء والمعارف. ويمكن إعتباره أيضا خدمة تركز على بناء الشبكات أو العلاقات الإجتماعية بين الناس وعادة ما يكون التسجيل مجانا فى تلك المواقع. أمثلة على بعض مواقع الشبكات الاجتماعية مثل فيس بوك، تيوتر، وغيرها الكثير.

التعرف على الأساسيات

1. قم بتحديد قائمة الأصدقاء – وتفادى الصداقات العشوائية.
2. قم بحماية خصوصيتك – ولا تعط كلمة المرور الخاصة بك لأى شخص وقم بوضع تعريفك الموجز بطريقة خاصة.
3. التفاصيل الشخصية الخاصة بك قيمة- لا تعطيها لأى شخص دون أسباب وجيهة.
4. قم بحماية بياناتك – وقم بإزالة الصور العبثية والألقاب.
5. كن حذراً فيمن تثق بهم – قد يتقمص الشخص شخصا آخر دون أن تدرى.
6. فكر قبل أن تنشر

AKAIS-AZRA

الألعاب على الإنترنت

أصبحت الألعاب الالكترونية في كل مكان وزمان خاصة بعد ما شهد العالم تطوراً ملحوظاً في مجال الانترنت والتطور الهائل في التكنولوجيا التي جعلت التصوير الجرافيكي أكثر واقعية في إطار ما يسمى بالألعاب الإلكترونية. فقد يشكل الانترنت والألعاب الالكترونية وإدمانها خطراً على الصحة وعلى حياة الكثيرين ممن يمارسونها يومياً ولساعات كثيرة أطفالاً أكانوا أم كباراً.. لذلك وجب علينا معرفة أخطار استخدام الانترنت والألعاب الالكترونية بشكل مفرط وآثارها الجانبية من أجل تحقيق وعي للتخفيف منها.

منذ العام 2002، كان هناك نحو 4 حالات وفاة لأشخاص بعدما أمضوا أكثر من 86 ساعة في مقاهي الانترنت يلعبون من دون أكل أو نوم. كما بدأت محطة (أم تي في) أغسطس الماضي تصوير فيلم وثائقي عن إدمان ألعاب الكمبيوتر. وبحسب مخرج هذا الفيلم، فالأولاد فيه لا يدركون أن اللعبة أصبحت جزءاً رئيسياً من حياتهم ولا يسعهم التوقف أو تصور حياتهم غير ذلك. حتى الـ (فيسبوك) ففيه يجد الصغار والكبار على السواء تسلية بالساعات في الدردشة الالكترونية (تشات) والألعاب (فارمفيل ومافيا وور والشوبينغ، الخ) فضلاً عن قضائهم ليالي بكاملها في تحميل صورهم والتعليق عليها متناسين واجباتهم المدرسية والعملية وأوقات الطعام وضرورة التواصل الاجتماعي الحقيقي لا الخيالي.

AKAIS-AZRA

وتشير الأبحاث العلمية إلى أن حركة العينين تكون سريعة جداً أثناء ممارسة الألعاب الالكترونية ما يزيد من فرص إجهادها، كما إن مجالات الأشعة الكهرومغناطيسية والمنبعثة من الشاشات تؤدي إلى حدوث احمرار العين وجفافها وكذلك الزغللة، وكلها أعراض تعطي الإحساس بالصداع والشعور بالإجهاد البدني وأحياناً بالقلق والاكتئاب. وقد أثبتت دراسة طبية نشرت مؤخراً في ألمانيا إن الأطفال الذين يقضون ساعات طويلة أمام الألعاب الالكترونية يصابون بقصر النظر أكثر من غيرهم. وحذر فريق طبي ياباني من أن الجلوس لساعات طويلة في اليوم أمام شاشات الألعاب الالكترونية قد يكون له علاقة بمرض خطير يصيب العين (الجلوكوما أو الماء الأزرق) وهذا قد يؤدي إلى العمى التام.

كما توصلت نتائج الأبحاث الطبية إلى ظهور مجموعة جديدة من الإصابات الخاصة بالجهاز العظمي والعضلي على مدى الخمس عشرة سنة الماضية مع كثرة انتشار الألعاب الالكترونية، وذلك نتيجة للحركة السريعة والمتكررة، كما توصلت إلى أن الجلوس لساعات طويلة أمام هذه الألعاب يسبب آلاماً مبرحة في أسفل الظهر، وتتعاظم مشاكل الجهاز العظمي والعضلي عند الأطفال بشكل كبير لأنهم يمرون بفترات نمو تحتاج إلى تمارين رياضية وفترات راحة.

AKAIS-AZRA