دليل إرشادي للوالدين

حماية الأبناء على الإنترنت !

بدعم من:

حركة سونزان مبارك
الدولية للمرأة من أجل السلام

LIBERTYGLOBAL

ins@fe

المحتويات

أ. كيف تستخدم هذا الدليل

إن كنت تزرع لعام واحد، فلتزرع أرزاً.
وإن كنت تزرع لعشرة أعوام، فلتزرع شجرة.
أما إن كنت تزرع لعمر برمته، فلتربي ولدك.
مثل صيني

عزيزي ولي الأمر/القائم على رعاية الطفل،

إليكم دليل الأمان الإلكتروني للأسر التي تضم أطفالاً ما بين ٦ سنوات و١٢ سنة. وهو عبارة عن مادة تعليمية تم إعدادها انطلاقاً من المعتقد الراسخ أن التكنولوجيا الحديثة يجب ألا تفصل ما بين الأجيال، وإنما توحدهم. وقد تم إعداده اعتماداً على خبرة Insafe، الشبكة الأوروبية لمراكز الاتصال القومية التي تعمل على رفع درجة الوعي بشأن كل ما يتعلق بالأمان على شبكة الإنترنت. وقد لاقى تطوير وإنتاج هذا الدليل للأمان الإلكتروني دعماً من قبل Liberty Global، كما لاقى ترجمة الدليل دعما من حركة سوزان مبارك الدولية للمرأة من أجل السلام[١] .

تماماً كما أن اللعب في الفناء أو عبور الطريق قد تحفه المخاطر إن لم تكن حذراً، فإن استخدام الإنترنت والتكنولوجيا المحمولة ينطوي أيضاً على المخاطر لمن لا يتوخى الحذر. ولكن لحسن الحظ، هناك أدوات متاحة لتزويد مستخدمي الإنترنت بمعلومات حول منافع ومخاطر تصفح شبكة الإنترنت.

١. توجد مراكز Insafe بعدد من الدول الأوروبية، وفي حالة الدول الأخرى يتم الإتصال بالهيئات أو المؤسسات ذات الصلة.

استخدم دليلك الجديد كي تساعد أبناءك على تعلم كيفية استخدام الإنترنت بأمان وفاعلية. يقدم لك الدليل ما يزيد على خمسين توجيها وتدريباً لتعليم أبنائك الأمان الإلكتروني بأسلوب ممتع شيق وخالٍ من التهديدات. فهو يشمل:

كتيبين عن الأمان الإلكتروني، قسم للمرح والتسلية العائلية ودليل إرشادي للوالدين؛

القواعد الذهبية؛

الشهادة العائلية؛

مجموعة من الملصقات؛

١٢ بطاقة لمواقف عديدة يقوم الأبناء بفصلها.

و يعتمد كل من كتيب العائلة وكتيب الوالدين على الرموز اللونية للإشارة إلى أربع موضوعات رئيسية عن الأمان الإلكتروني: الأمان، التواصل، التنمر على الإنترنت والترفيه والتحميل. يُعتبر كتيب الوالدين بمثابة مرجع لقسم المرح والتسلية العائلية: فهو يتضمن معلومات عامة، وملحوظات حول الأنشطة، وحلول مقترحة للتدريبات وبطاقات المواقف.

أما كُتيب العائلة، فيُفترض أن يستخدمه الوالدان والأبناء سوياً. يتم تناول الموضوعات الرئيسية الأربع من خلال قصة الصغيرين أليكس ولوسي، ووالديهما وخبيرة الحاسب العبقرية سيرينا. يتضمن كل فصل أنشطة تعليمية، بما في ذلك تدريبات على الإنترنت، ومسابقات، وقواعد ذهبية وروابط مفيدة.

اقرأ القصة بصوت مسموع مع أبنائك واعملوا معاً على حل الأنشطة المقترحة. وفي نهاية كل فصل، يمكنك استخدام بطاقات المواقف المناظرة لبدء النقاش مع أبنائك لتعزيز فهم المحتوى.

حين يتمم أبناؤك رحلتهم بنجاح مع هذا الدليل، كافئهم بالموافقة على مجموعة من القواعد الذهبية وتوقيع الجميع على شهادة العائلة. وفي النهاية، يستطيع الأبناء تزيين الكتيب بملصقات أيقونات المشاعر. نحن نقدر رأيك. لذا لا تتردد في الاتصال بمركز Insafe في منطقتك لطرح الأسئلة أو الإدلاء بالتعليقات. نأمل أن تمضوا أنتم وأبناؤكم وقتاً سعيداً أثناء تصفحكم للإنترنت!

نتمنى لكم تصفحاً آمناً

١. الأمان يمنحك السلامة

حاسب في المنزل

إن وجود حاسب في المنزل يمكن أن يكون وسيلة تعليمية وترفيهية رائعة للأسرة كلها. إلا أن وضع الحاسب في غرفة المعيشة بالمنزل ووضع قواعد محددة تتعلق بشروط الاستخدام والوقت الذي يمكن قضاؤه أمام الشاشة يساعد أفراد أسرتك الصغار على أن يظلوا في مأمن.

ولكن تذكر أن أبناءك يمكنهم الدخول على **الإنترنت** من منازل أصدقائهم، ومقاهي الإنترنت، الخ. لذا فمن المهم أن تقوموا معاً بوضع قواعد للسلوك يمكن اتباعها في أي مكان وزمان.

تأمين حاسبكم

يمكن تحقيق الأمان من خلال الفهم الأساسي للمخاطر المحتملة ومعرفة الحلول السهلة. تشمل هذه الحلول الأدوات التكنولوجية البسيطة وكذلك فطنة المستخدم. وشأنها شأن أي شيء آخر، فإن الفطنة تتطور مع العمر والممارسة.

إن الأشياء التي يُرجح أن تقوم أنت وأبناؤك بها على حاسبكم المنزلي كاستخدام **بطاقات الذاكرة** أو **الأسطوانات المدمجة**، و**فتح المرفقات** و**تحميل الملفات**، قد تنطوي جميعها على المخاطر. تتعلق هذه المخاطر بالدرجة الأولى ببرامج الحاسب الضارة، أي البرمجيات الخبيثة، التي تم تصميمها لإلحاق الضرر بحاسبك، وسرقة المعلومات الشخصية، أو ملاحقتك بالدعاية غير المرغوب فيها.

يتعرف الأبناء على أنواع البرمجيات الضارة: **الفيروسات**، **الدودات**، **أحصنة طرادة**، و**برمجيات التجسس** ويتعلمون كيفية التعرف على أعراض الحاسب المصاب. كما يتعلمون كيفية تجنب الإصابة من خلال الحرص دوماً على الدخول إلى الإنترنت من خلال حاسب تحميه برمجيات حديثة مضادة للفيروسات ومضادة للتجسس. كذلك يُنصحون بتوخي الحذر عند فتح مرفقات البريد الإلكتروني الذي يصلهم من مرسل مجهول، وعند تحميل البرامج من على الإنترنت، وكذلك عند استخدام بطاقات الذاكرة المعتمدة على USB أو الأسطوانات المدمجة.

مقاومة الرسائل العشوائية

نحو ٨٠٪ من رسائل البريد الإلكتروني المتداولة على شبكة الإنترنت هي **رسائل عشوائية** (رسائل غير مرغوب فيها) يمكنها بسهولة التأثير على أبنائك. فنشر **عنوان البريد الإلكتروني** دون قصد على **الشبكة** عند استخدام **مجموعة إخبارية**، أو **موقع للدردشة**، أو **منتدى عام**، أو **موقع التعارف الاجتماعي** أو **نموذج استمارة** على الإنترنت يمكن أن تنتج عنه رسائل عشوائية. وهناك برمجيات معينة تستطيع جمع عناوين البريد الإلكتروني من على شبكة الإنترنت لتكوين قوائم بريدية تُستغل بعدها في توزيع الرسائل العشوائية بأعداد هائلة. أما الشركات التي تضطلع بمثل هذه الأنشطة تتواجد غالباً في مواقع لا توجد بها تشريعات تمنع الرسائل العشوائية!

في المعتاد تتعلق الرسائل العشوائية بالمواد الإباحية، المستحضرات الطبية، الصفقات المالية المشبوهة، الخ. علاوة على ذلك، قد تكون الرسائل العشوائية أيضاً مصدراً للبرامج الخبيثة. وفي أغلب الحالات، تُوزع الرسائل العشوائية لأغراض الاحتيال. إليك بعض النصائح لمساعدتك على حماية أسرتك:

- استخدم "**عوامل تصفية الرسائل العشوائية**". في المعتاد يقدم موفر خدمة البريد الإلكتروني خيارات مقاومة الرسائل العشوائية التي يمكنها أن تنشط داخل برنامج البريد الإلكتروني الخاص بك. اتصل بموفر خدمة البريد الإلكتروني للحصول على معلومات مفصلة. واحرص على تفقد **مجلد الرسائل العشوائية** أو **الرسائل غير الهامة** على نحو كمنظم للتأكد من عدم دخول رسائل بريئة إليه بطريق الخطأ. فالتكنولوجيا ليست معصومة من الخطأ.
- علم أبناءك إلا يقدموا على فتح رسائل بالبريد الإلكتروني من أشخاص مجهولين. فالرسائل العشوائية تكاد دائماً تحتوي على عروض ومرفقات جذابة. أريهم كيف يقومون بحذف مرسل هذه الرسائل أو فقط اطلب منهم حذف الرسائل المشتبه فيها.

تصفح شبكة الإنترنت

حتى الأطفال صغار السن يمكنهم الاستفادة من تصفح شبكة الإنترنت للترفيه وزيارة **المواقع** التعليمية. إلا أن الإنترنت تحتوي على كل أنواع المحتوى الذي قد لا يتناسب دائماً مع أعمارهم.

محركات البحث تعد وسيلة رائعة للعثور على المحتوى على شبكة الإنترنت. ولكن، نظراً لأن البحث يعتمد على اختيار الكلمات الدالة، فمن السهل العثور على محتوى غير مطلوب. فكلمة قد تبدو بريئة جدا قد تقودك إلى موقع غير بريء يتضمن الكلمة الدالة التي بحثت عنها. إليك بعض النصائح لمساعدة أبنائك على التصفح بشكل أكثر أمناً على الإنترنت.

- قم بإنشاء حساب مستخدم لطفلك باستخدام **نظام تشغيل** (مثل Windows, Linux, Mac OS) والذي يمكنك أن تقوم بتنشيط **الرقابة الأبوية** عليه؛
- تفقد خصائص الرقابة الأبوية على **متصفح الإنترنت** ومحرك البحث لديك. وتأكد من أنك على علم بجميع الخيارات التى تقدمها **إعدادات الأسرة** بهذه الأدوات؛
- اقترح **محركات بحث** ملائمة لصغار مستخدمي الإنترنت. و من أمثلة هذه المحركات http://www.askforkids.com , http://kids.yahoo.com[٢]؛
- احفظ العناوين التي يكثر أبناؤك من استخدامها في مجلدات **المواقع المفضلة** (أحد خيارات المتصفح). بهذه الطريقة يمكنك أن تسمح لهم باستخدام أماكنهم المفضلة على الشبكة مراراً وتكراراً دون الحاجة إلى المرور عبر محرك البحث.

إلى جانب تنشيط خصائص الرقابة الأبوية على المتصفح ومحرك البحث لديك، يمكنك استخدام **عامل تصفية** إضافي، وهو برنامج يهدف إلى حماية الصغار من المحتوى غير الملائم. استشر منفذ بيع البرامج في منطقتك، أو ابحث على الإنترنت عن **برنامج** تجريبي. ولكن تذكر أن لا شيء يمكن أن يحل محل الإرشاد الذي يقدمه الوالدان ومقدمو الرعاية. فالأدوات التكنولوجية ليست معصومة من الخطأ ومن الممكن أحياناً أن تعطيك إحساسا زائفا بالأمان، ما لم تتحلى بالفطنة مع استخدامها.

يمكن أن تكون برمجيات التصفية شديدة التقييد بحيث تمنع حتى المواقع البريئة. فعلى سبيل المثال، قد تمنع الأبناء من إجراء بحث في التاريخ عن الحرب العالمية الثانية لأن البحث يقود إلى مواقع تصف العنف. فضلاً عن ذلك، فإن أي عامل من عوامل التصفية تقوم بتشغيله قد يغلقه الصغار الأذكياء الذين في الغالب يكونون خبراء في إخفاء آثارهم. ستعرف أن ذلك يحدث فقط لو تعلمت كيف تستخدم الحاسب والبرنامج بنفسك.

قم بزيارة موقع SIP-Bench (راجع الروابط المفيدة)، وهي دراسة تمت برعاية المفوضية الأوروبية، جرى من خلالها اختبار ٣٠ أداة من أدوات الرقابة الأبوية ومكافحة الرسائل العشوائية لقياس فاعليتها في حماية الأبناء الذين تتراوح أعمارهم ما بين ٦ سنوات و١٦ سنة من المحتوى الضار في مختلف تطبيقات الإنترنت: **التصفح**، البريد الإلكتروني، **نقل الملفات**، الدردشة و**الرسائل الفورية**.

بالإضافة إلى تجنب المحتوى الضار، يجب أن تحرص على ألا يصدق أبناؤك كل ما يرونه أو يقرأونه على الإنترنت. في كتيب المرح والتسلية العائلية، نقترح أن يقوموا بزيارة ٣ مواقع على الأقل لمقارنة المحتوى عند البحث عن معلومات على الإنترنت. كما يُنصحون بذكر مصدر معلوماتهم بشكل منتظم حالما يستعينون بهذه المعلومات في الواجبات المنزلية.

نصائح ذهبية لأولياء أمور الأبناء متصفحي الإنترنت

- تأكد من أن حاسبك يحميه جدار حماية، إلى جانب البرامج المضادة للفيروسات والمضادة للرسائل العشوائية. داوم على تحديث هذه البرامج وانتبه إلى أية تنبيهات قد تصدر عنها. اسأل مقدم خدمة الإنترنت لديك إن كانت لديهم أدوات يمكنك استخدامها لمقاومة الفيروسات والرسائل العشوائية؛
- استخدم عامل تصفية للرسائل العشوائية في برنامج البريد الإلكتروني لديك واحتفظ بعنوان

٢. ينصح اختيار المواقع المختلفة طبقا للمنطقة والثقافة، على سبيل المثال يمكن الرجوع إلى المواقع التالية فى المنطقة العربية:
www.makhmakh.iti.gov.eg
www.arabkids.com
www.ritsec.org.eg/html/little_horus.html

بريدك الإلكتروني سرياً بقدر المستطاع، عن طريق الامتناع عن نشره على الإنترنت. تجنب فتح الرسائل من المرسلين المجهولين وقم بسمح المرفقات قبل فتحها؛

- ارفع خصائص الرقابة الأبوية إلى الدرجة القصوى على: نظام التشغيل، متصفح الإنترنت، محرك البحث وبرنامج البريد الإلكتروني. قم بإنشاء حسابات مستخدم لكل واحد من أبنائك. وتأكد من أن إعدادات الخصوصية عند أعلى درجاتها (تفقد قائمة "الخيارات" في متصفحك)؛
- فكر في الاستعانة ببرنامج تصفية إضافي؛
- سارع بالاتصال بمقدم خدمة الإنترنت أو خبير الحاسب بمجرد أن تظهر علامات غريبة على حاسبك، إذ ربما يكون مصاباً. سيتمكن مقدم خدمة الإنترنت من تقديم المشورة للوالدين؛
- تقدم ببلاغ إلى الخط الساخن القومي للإنترنت (راجع الروابط المفيدة) إن صادفك محتوى غير مرغوب فيه على الإنترنت؛[٣]
- اجلس إلى جوار أبنائك متى استطعت بينما يقومون بتصفح الإنترنت. فهذه طريقة ممتازة للتشجيع على النقاش وزيادة الثقة. اجعل من التعلم الجماعي تحدياً مثيراً؛
- تذكر أن هذه القواعد الأمنية تنطبق عليك وعلى أبنائك. شجعهم على أن يطلعوك على كل ما يظنونه غريباً.

روابط مفيدة

هناك عدد من المواقع المفيدة المتاحة لاستخدام الأطفال. الأطفال ما بين عمر الخامسة والسابعة يمكنهم زيارة عالم هيكتور عبر www.thinkuknow.co.uk/5-7. أما الأطفال ما بين عمر الثامنة والحادية عشرة، فيمكنهم استخدام موقع مقهى الإنترنت الذي يصطحب الأطفال في جولات تفاعلية تهدف إلى منحهم فرص للتعرف على المخاطر التي يواجهونها على الإنترنت.
http://www.thinkuknow.co.uk/8_10/cybercafe

للاستمتاع بالتصفح الآمن، فالسر يكمن في المعرفة: اعرف المخاطر، اعرف كيف تحمي نفسك واعرف المزيد. يمكن الحصول على التفاصيل من موقع Childnet Know it All for Parents :
http://www.childnet.com/kia/parents/cd

إن صادفت محتوى تعتقد أنه قد يكون غير قانوني أثناء تصفحك للإنترنت، يمكنك التقدم ببلاغ لخدمة الخط الساخن في المملكة المتحدة:
http://www.iwf.org

للاطلاع على دراسة SIP-Bench حول الرقابة الأبوية وأدوات مقاومة الرسائل العشوائية:
http://www.sip-bench.org/index.html

٣. يختلف الخط الساخن طبقا للمنطقة، على سبيل المثال ففى مصر إذا تعرض طفلك لجريمة من جرائم الإنترنت، يمكن الرجوع إلى الإدارة العامة للتوثيق و المعلومات لمكافحة جرائم الحاسب المعلوماتية ٠٠٢٠٢٧٩٢٨٤٨٤، أو بخط نجدة الطفل بالمجلس القومي للطفولة و الأمومة بمصر وهو خط مجاني لكل الجمهورية ١٦٠٠٠، أو لجنة حماية حقوق المستهلك بالجهاز القومي للإتصالات ١٥٥.

٢. التواصل

قطع الأحجية (البازل)

أتذكر كم كان من المهم بالنسبة لك أن تظل على اتصال بأصدقائك حين كنت صغيراً؟ توفر الإنترنت أماكن جديدة لمقابلة الأصدقاء وسبلاً جديدة للتعبير عن الذات والتعارف من خلال البريد الإلكتروني، نقل الملفات، المدونات، والتعارف الاجتماعي (مثل مواقع MySpace، Facebook، Hi5، Habbohotel) الخ. يستخدم المراهقون اليوم التكنولوجيا لتجربة الأشياء الجديدة والتعارف في مكان يشعرون فيه بالخصوصية والبعد عن مراقبة الوالدين.

يهدف فصل التواصل إلى تعريف الوالدين والأبناء بمفهوم **البيانات الشخصية**، و**الخصوصية**، والتفاعل الإيجابي على الإنترنت وإدارة المخاطر مثل الاحتكاك بالغرباء. إن الخصوصية على الإنترنت لهي شديدة الارتباط بمفهومي **الحسابات** و**ملفات التعريف**. الحساب هو ما يمكّن المرء من الدخول على خدمة الإنترنت.

بعيداً عن الإنترنت، فإن تذكرة الحافلة أو بطاقة الجمانيزيوم أو بطاقة العضوية تضم معلومات شخصية عنك تماما مثل حسابك الشخصي والخدمات على الإنترنت. لا يمكنك فتح أي منها ما لم تقدم بعض المعلومات الشخصية التي تستخدم في إنشاء "ملف تعريف المستخدم" الخاص بك. المهم هو أنك تستطيع اختيار أي نوع من المعلومات تريده أن يكون متاحاً عن نفسك، ومن تود أن يطلع على هذه المعلومات.

إن حماية خصوصيتك يتعلق بالتحكم فما تريد أن يطلع الناس عليه فيما يتعلق بك، بدلاً من الكذب بشأن هويتك. يتحمس الشباب حيال التحدث إلى أصدقائهم عبر الإنترنت وإنشاء صورة لهم على الإنترنت. غير أنهم لا يدركون دوماً الأثر الذي قد يترتب على جعل معلوماتهم الشخصية متاحة علناً.

إنشاء ملف تعريف

أولى خطوات حماية معلوماتك الشخصية هي إنشاء ملف تعريف أكثر أمناً من خلال التفكير ملياً في البيانات التي سوف يحتوي عليها وإعدادات الخصوصية التي ستطبقها.

قم بإنشاء عدة حسابات للبريد الإلكتروني لمختلف السياقات على الإنترنت. على سبيل المثال، عند استخدام خدمة على الشبكة كالدردشة، أو الرسائل الفورية، أو المدونات، الخ، شجع ابنك على استخدام عنوان للبريد الإلكتروني و**اسم شاشة** محايدين. بهذه الطريقة فإن ابنك الذي يهوى الدردشة لن يستخدم عنواناً للبريد الإلكتروني يكشف عن اسمه/اسمها كاملاً.

احتفظ دوماً **بكلمات المرور** للحسابات سرية. وتأكد أن أبناءك يتفهمون أنه يتعين عليهم عدم مشاركة

أصدقائهم في حساباتهم الشخصية حيث قد يسيئون استغلال ثقتهم. من ناحية أخرى، قد ترغب في معرفة كلمات مرور أبنائك كي تتمكن من مراقبة حساباتهم – تحدث إليهم في هذا الشأن.

تذكر أن تقوم بتخصيص **إعدادات الخصوصية** في ملف تعريفك/حسابك بأن تجعله خاصاً وليس عاماً. هذا الخيار يمنحك فرصة التحكم في الأشخاص الذين يمكنهم رؤية حسابك والأشخاص الذين يمكنك التفاعل معهم. ملف التعريف الخاص يعني قائمة الأسماء. علم أبناءك أن يقبلوا الاتصال على الإنترنت فقط بالأشخاص الذين يعرفونهم بالفعل و ليس فقط من الإنترنت.

إن كان أبناءك يستخدمون غرف الدردشة تأكد من أن:

- هناك وسطاء حاضرين. عدم وجود وسطاء يعني دردشة غير آمنة؛
- هناك أدوات لتجاهل أو حظر بعض المشاركين في الدردشة غير المرغوب فيهم؛
- هناك خاصية المساعدة و**الإبلاغ** على الموقع بحيث يمكن اللجوء إليها في حالة وجود مشكلة؛
- قواعد الخدمة مبينة بوضوح.

الصور وكاميرات الويب

يجب أن يفهم الأبناء أن صورهم هي جزء أساسي من خصوصيتهم، وأن الصور الرقمية واسعة الإمكانيات. فمن السهل تداولها و**التلاعب بها**، ومن الصعب جداً محوها بمجرد إرسالها عبر الحاسب أو الجوال – فقد تظل الصور على شبكة الإنترنت إلى الأبد! كاميرات الويب يجب استعمالها بحذر، كما ينبغي ألا يستخدم الأبناء كاميرات الويب دون رقابة. **فأدوات وأدلة الدردشة باستخدام الكاميرا** قد تنطوي على الكثير من المخاطر. فأنت وأبناؤك يجب ألا تطلعوا على صوركم الشخصية إلا من تعرفونهم وتثقون بهم -- استأذن دائماً قبل نشر صورة شخص آخر. ولا تدع أبناءك يستخدمون الحاسب وكاميرا الويب بمفردهم في الغرفة.

التخاطب مع الغرباء

إن الأشخاص الذين تلتقي بهم على الإنترنت ليسوا دائما كما يدعون كما يدعون. علم أبناءك أن يحموا خصوصيتهم على الإنترنت بالضبط كما يفعلون بعيداً عن الإنترنت. أنت تضع قواعد بشأن كيفية تعاملهم مع الغرباء في الواقع، فلم لا يتبعون نفس القواعد على الإنترنت؟

قد يبني أبناؤك أواصر قوية للصداقة مع أقران على الإنترنت، ويميلون إلى أن يضعوا ثقتهم بسهولة فيمن يظهرون الاهتمام بهم والتفاهم معهم حتى وإن كانوا لا يعرفونهم بالفعل. وبالتالي، قد يجتذبهم إغراء مقابلة هؤلاء الأصدقاء بعيداً عن الإنترنت دون علمك. في أغلب الأحوال لا يدرك الأبناء مخاطر مثل هذه اللقاءات وقد يستخفون بها. وبهذا يصبحون ضحية سهلة **الاستمالة** على الإنترنت. تشير الدراسات أن الكثير من الأطفال يخرجون للقاء "أصدقائهم" على الإنترنت دون مرافق ودون إخبار والديهم. تحدث إلى أبنائك عن ذلك كي تتأكد من عدم حدوث هذا. فالسر يكمن في التواصل.

آداب الإنترنت

آداب الإنترنت يُقصد بها حسن السلوك على الإنترنت ومعاملة الآخرين على الشبكة تماماً كما تحب أن يعاملوك. فالأطفال قد لا يدركون أنهم قد يسيئون إلى شخص ما على الإنترنت دون قصد. للأسف، أحياناً يستخدم البعض الإنترنت و/أو الهواتف الجوالة لمضايقة أو التحرش بالآخرين. وهذا ما يطلق عليه التنمر على الإنترنت والذي يؤثر على واحد من كل أربعة أطفال (للمزيد من المعلومات راجع الفصل ذي الصلة).

لغة الدردشة[٤]

عند الدردشة على الإنترنت، يستخدم الصغار لغة فريدة، مليئة **بأيقونات المشاعر** و**الاختصارات!** ألق نظرة على الجداول أدناه للتعرف عليها 😂

قائمة **لاختصارات الدردشة**، للمزيد من المعلومات راجع الروابط المفيدة:

GR8	great	عظيم
Brb	Be right back	سأعود بعد قليل
TYT	Take your time	خد وقتك
Tx / Thnx	Thanks / Thank you	شكرا
ISA	Inshaalaa	إنشاء الله
G2g / Gtg	Got to go	يجب أن أمضى
Eshta		قشطة –
K	ok	موافق
C U	See you	سوف أراك
C	See?	شفت – رأيت
ILY	I love you	إنى أحبك
Donno	I don't know	لست أعلم
WB	Welcome back	مرحبا بك عائدا

٤. تختلف الإختصارات من ثقافة إلى أخرى وتستخدم بعض الدول المختصرات الإنجليزية، كما تستخدم بعض الثقافات مزيج من المختصرات بلغات أخرى – من لغات الدردشة المتعارف عليها :
http://www.shobiklobik.com/variety/qamoos.asp?cat=12
http://www.al-mjd.com/e7tesarat.htm

H r u?	How are you?	كيف حالك ؟
Gd	Good	جيد
F9	Fine	كويس
7		ح
7		خ
2		ق (ء)
7a2i2y		حقيقى
<3		قلب
4	for	من أجل

يمكنك صنع أيقونات المشاعر عن طريق المزج بين علامات الترقيم والحروف، انظر الأمثلة أدناه:

وجه مبتسم (بأنف أو بدون)	:) أو : -) نقطتان، (شرطة)، قوس
وجه حزين (بأنف أو بدون)	:(أو :-(نقطتان، (شرطة)، قوس
وجه غامز (بأنف أو بدون)	;) أو;-) نقطتان، (شرطة)، قوس
وجه مندهش (بأنف أو بدون)	o : أو :-o نقطتان، (شرطة)، حرف oصغير
ابتسامة عريضة (بأنف أو بدون)	D : أو :-D نقطتان، (شرطة)، حرف Dكبير
وجه يخرج لسانه (بأنف أو بدون)	p : أو :-p نقطتان، (شرطة)، حرف pصغير

القواعد الذهبية

- كرس وقتاً لتكتشف كيف يقضي أبناؤك وقتهم على الإنترنت ودعهم يبينون لك كيف يتواصلون مع أصدقائهم؛
- علمهم أن يحموا خصوصيتهم على الإنترنت عن طريق:
  - إنشاء ملفات تعريف آمنة مع تمكين إعدادات الخصوصية.
  - حماية كلمات مرورهم.
  - عدم التحدث إلى أو الرد على إلا من يعرفونهم فعليا من عالم خارج الإنترنت.
  - المداومة على طلب موافقة الوالدين قبل رفع صورهم أو صور الأسرة أو المنزل أو المدرسة، الخ.
  - عدم إطلاع أي شخص على المعلومات الشخصية كأرقام الهاتف، والعنوان، والمدرسة، والفريق الرياضي، الخ ما عدا الأشخاص الذين تعرفهم معرفة جيدة في الواقع.
  - ضع الحاسب المنزلي في غرفة المعيشة كي تتمكن من مراقبة أنشطتهم على الإنترنت؛
- تأكدوا من أنكم على معرفة بما يلي :
  - كيفية رفض الأشخاص أو حظر الأشخاص من الانضمام إلى قائمة الأسماء .
  - خاصيتي الأمن والإبلاغ المتاحتين على المواقع التي تستخدمونها .
- قم ببناء جسور الثقة بأن تطمئن أبناءك أن بوسعهم التحدث إليك عن أخطائهم كي تبحثوا معاً عن الحلول! فالأخطاء ليست سوى جزءاً من التعلم.

روابط مفيدة

قامت Childnet International بإنشاء ChatDanger وKidsmart وهما موقعان يعملان على تقديم المشورة الأمنية للأطفال والشباب. يتضمن الموقعان معلومات نافعة تقدم بطريقة ممتعة وشيقة أثناء إيصال الرسائل الهامة:
http://www.chatdanger.com
http://www.kidsmart.org.uk

Think U Know هو موقع للآباء فقط:
http://www.thinkuknow.co.uk/parents

افهم شفرة الدردشة عن طريق زيارة wikiHow:
http://www.wikihow.com/Understand-Chat-Acronyms

راجع تقرير Eurobarometer لعام ٢٠٠٧ واقرأ عن إنترنت أكثر أمناً للأطفال:
http://ec.europa.eu/information_society/activities/sip/eurobarometer

٣. التنمر على الإنترنت (التحرش)

واقعة تنمر على الإنترنت

للتواصل عبر الإنترنت والهواتف الجوالة مميزات رائعة. ولكن مع الأسف قد يكون الوضع أحياناً عكس ذلك -- فقد يتلقى أو يرسل أبناؤك رسائل ذات محتوى يجرح مشاعرهم أو مشاعر الآخرين. لذا من المهم أن تعلم أبناءك السلوك المقبول اجتماعياً – فحتى أبناؤنا فلذات أكبادنا ليسوا ملائكة.

التنمر على الإنترنت يعني استخدام أجهزة وخدمات المعلومات والتواصل الجديدة بغرض التنمر أو التحرش أو إخافة فرد أو مجموعة. ومن الممكن استخدام البريد الإلكتروني، والدردشة، والرسائل الفورية، والهواتف الجوالة وغيرها من الأدوات الرقمية. ففي بيئات اللعب الإفتراضي (الرقمي)، قد يقوم المتنمرون بمهاجمة الصورة التجسيدية (الأفاتار) لابنك، عن طريق مثلاً إطلاق النار عليها، أو سرقة الممتلكات الإفتراضية لها أو إجبار الصورة التجسيدية على التصرف بطرق غير مقبولة.

بشكل عام، يبلغ الأبناء عن المشكلات التي تتعلق بإفشاء المعلومات الخاصة في أماكن عامة، كنشر صورة خاصة أو معلومات شخصية في منتدى أو موقع عام. وتماماً مثل التنمر في المدارس أو أفنية اللعب، فإن مثل هذا السلوك غير مقبول، ويجب على الآباء والمعلمين والأبناء الانتباه والاستعداد للاستجابة. ولكن على العكس من التنمر في صورته التقليدية، فإن التنمر على الإنترنت من الممكن أن يؤثر على الطفل حتى وإن لم يعد موجوداً مع المتنمر. فعلى سبيل المثال، قد يقوم المتنمرون بإرسال رسائل تهديد لحسابات البريد الإلكتروني المنزلية والهواتف الجوالة في أي وقت من الليل أو النهار.

يستطيع الآباء العمل على تعزيز بيئة لا يكون التنمر مقبولاً فيها – علم أبناء أن كون المرء مجهولاً على الإنترنت لا يعني أنه يمكنه التصرف بشكل غير مسؤول. فعليهم أن يكونوا على علم بحقوقهم ومسؤولياتهم، وكيفية احترام حقوق الآخرين.

احرص دوماً على إقامة حوار مفتوح مع أبنائك، كي تتمكنوا من التحدث عن أي موقف مقلق. فسبل التكنولوجيا الجديدة، كالإنترنت والهواتف الجوالة يمكنها أن توفر فرصاً رائعة للحوار واقتراح موضوعات تدعو إلى التأمل والتفكير!

القواعد الذهبية

- امنع وقوع التجارب السلبية عن طريق التأكد من أن أبناءك يعرفون كيف يحمون خصوصياتهم وكيف يحترمون خصوصية الآخرين؛
- علم أبناءك ألا يستجيبوا لرسائل التحرش؛

- ساعد أبناءك على فهم أنواع الرسائل والسلوك التي قد تسيء إلى الآخرين، وكيفية تجنب ذلك؛
- تأكد من أنهم يعرفون كيف يقومون بحظر أحد المرسلين من قائمة أسمائهم؛
- احتفظ بالرسائل المسيئة، فقد تحتاجها كدليل هام؛
- تعرف على الإستراتيجيات المتبعة في مدرسة أبنائك لمقاومة التنمر. تعاون مع أولياء الأمور الآخرين والمدرسين لمنع التنمر والتنمر على الإنترنت؛
- ابق على اتصال ببيئة أبنائك، تعرف على أصدقائهم، وأهالي أصدقائهم، ومدرسيهم وزملائهم في قاعة الدرس؛
- شجع أبناءك على أن يخبروك بأي حدث مزعج وقع على الإنترنت أو بعيداً عنها. وطمئنهم أنهم حتى لو أتوا تصرفاً طائشاً، فأنت موجود لمساعدتهم وأنكم معاً ستجدون حلولاً!
- تأكد من أن أبناءك يفهمون أنه لا لوم عليهم لو تحرش بهم أحد.

روابط مفيدة

موقع Digizen (أي المواطن الرقمي) يضم خضماً من المعلومات حول كيفية التحكم في معلوماتك الشخصية وكيفية التحلي بالذكاء والفطنة على الإنترنت. هناك قسم خاص عن التنمر على الإنترنت يقدم المعلومات والنصح حول التعرف على والتعامل مع التنمر على الإنترنت. كما يوجد فيلم مؤثر يمكن استخدامه مع الأطفال والشباب:
http://www.digizen.org

على موقع stop bullying ستجدون أفلاماً بالرسوم المتحركة عن التنمر وأنشطة مقترحة في قاعات الدرس عن كيفية التعامل مع التنمر وإيقافه:
http://www.stopbullying.org

احصل على نصائح عن كيفية إيقاف التنمر بالرسائل النصية عبر:
www.stoptextbully.com

موقع التحالف ضد التنمر يحتوي على ثروة من المعلومات عن التنمر على الإنترنت للأطفال والبالغين:
http://www.anti-bullyingalliance.org.uk/Page.asp

Childline هي خدمة متاحة على مدار ٢٤ ساعة للصغار حتى سن ١٨ سنة. يقدم موقع Childline الدعم للصغار من خلال خدمة الاستماع من Childline عبر الهاتف وكذلك عبر موقع Childline على الإنترنت:
http://www.childline.org.uk

٥. الرقم المجاني لـ Childline على الإنترنت: ٠٨٠٠ ١١١١

٤. الترفيه والتحميل

ليس كل ما يلمع ذهباً على الإنترنت

تعد الإنترنت فضاءاً إفتراضيا لممارسة العديد من الأنشطة، بما فيها الأنشطة التجارية. فإن كنت لا تسمح لأبنائك بشراء كل ما يرون إعلاناً عنه على التلفاز، أو كل ما يبهرهم في المتاجر، يجب عليك إذن أن تعلمهم ألا يرغبوا أو يصدقوا كل ما يُعلن عنه على الإنترنت، كالموسيقى والألعاب، و**رنات الجوال**، وغيرها من الكماليات وشراء الخدمات على الإنترنت.

إن قضاء بعض الوقت مع أبنائك يمنحك الفرصة كي تشرح لهم أن المنتجات كرنات الجوال، و**خلفيات الشاشة**، و**الأغاني الـ mp3**، و**الصور التجسيدية** الخ قلما تكون مجانية. أينما وجدت مثل هذه الإعلانات، إلفت نظرهم إلى الكتابة الموجودة بالخط الصغير كي توضح لهم ألا يعتبروا كل ما يرونه على الإنترنت شيئاً لا يقبل الشك.

للاشتراك في أية خدمة (سواء مجانية أم لا)، سيكون عليك **ملء نموذج على الإنترنت** بالمعلومات الشخصية ذات الصلة. قم باستكمال هذه النماذج فقط إن كنت تعرف كيف ستُستغل بياناتك الشخصية، وأقنع أبناءك ألا يقوم بملء هذه النماذج إلا حين تكونون معاً.

النوافذ المنبثقة تُستخدم غالباً لأغراض بيع المنتجات على الإنترنت. وهي لا تكون دائماً سيئة – ولكن هذا يتوقف على مصدرها وهل هو موقع موثوق به أم لا. بشكل عام، إن كنت تثق بالموقع، فيمكنك أن تثق بالنافذة المنبثقة. ولكن بعض النوافذ المنبثقة تستخدم لتسويق منتجات غير جديرة بالثقة أو تقود إلى استبيانات على الإنترنت لجمع البيانات الشخصية. علم أبنائك أن يقوموا بغلق النوافذ المنبثقة غير الموثوق بها بالنقر على علامة x باللون الأحمر في الركن الأيمن الأعلى.

اللعب على الإنترنت

تختلف الألعاب على الإنترنت عن الألعاب الرقمية الأقدم لأنها تستلزم الاتصال الحي بالشبكة. يستطيع الأبناء الاستمتاع بالألعاب على سي دي/دي في دي على **مواقع الإنترنت**، على كونسول الألعاب أو على الهواتف الجوالة أو غيرها من الأجهزة المحمولة.

الألعاب على الإنترنت تتراوح من الألعاب البسيطة السهلة مثل باك مان وتيتريس إلى ألعاب الواقع الإفتراضي التي يشترك فيها العديد من اللاعبين معاً على الإنترنت، إذ يقومون بتقديم المحتوى والقصص. الكثير من هذه **الألعاب متعددة اللاعبين** تدعم المجموعات الإفتراضية للاعبين. وهذا من شأنه أن يعرض الأبناء إلى المخاطر التي تنطوي عليها مقابلة الغرباء على الإنترنت (راجع فصل التواصل).

تقوم الألعاب بدور هام في تطور الأطفال نظراً لأن المهارات الاجتماعية والتفكير الإستراتيجي تنمو في بيئة تقيدها قواعد اللعب. إلا أن الكثير من الألعاب الرقمية جذابة وتفاعلية وتستخدم للأغراض التعليمية.

ولكن ليست كل الألعاب الرقمية جيدة. عليك أن تقرر أي الأنواع تتناسب مع أبنائك – ومن خلال وضع القواعد، يمكنك أن تضمن أن الوقت الذي يمضيه أبناؤك في اللعب على الإنترنت لن يضر بالأنشطة الأخرى.

هناك نظام أوروبي للتصنيف بحسب العمر، PEGI online، يتم من خلاله تصنيف الألعاب بحسب العمر والمحتوى. هذا النظام تدعمه العديد من الشركات المصنعة، بما في ذلك، Xbox، PlayStation، وNintendo، فضلاً عن الناشرين ومطوري الألعاب التفاعلية في أنحاء أوروبا. ابحث عن هذه المواصفات على ظهر علبة اللعبة التي تبتاعها لطفلك، ولكن تذكر أن ليس كل الأطفال في عمر ١٢ ربيعاً متشابهين.

القواعد الذهبية

- شجع أبناءك على استخدام مواقع تقدم محتوى ووضح لهم أن الأمور على الإنترنت ليست دائما كما تبدو؛
- وضح مخاطر تحميل مواد من على الإنترنت دون حذر؛
- تأكد من أن حاسبك يتمتع بالحماية واحرص دوماً على استخدام نسخة محدثة من البرنامج المضادة للفيروسات؛
- علم أبناءك أن يقوموا بحفظ الملفات التي انتهوا من تحميلها على القرص الصلب وأن يقوموا بمسحها بحثاً عن الفيروسات قبل فتحها؛
- اقرأ دائماً إقرار الخصوصية واتفاقيات المستخدم قبل تثبيت أي شيء. تأكد (على الإنترنت) من أن البرنامج الذي ترغب في تحميله يمكن الوثوق به؛
- أغلق النوافذ المنبثقة التي لا يمكن الوثوق بها بالنقر على علامة x باللون الأحمر في الركن الأيمن الأعلى. إياك والنقر داخل هذه النوافذ المنبثقة.

الأطفال والألعاب:

- ضع قواعد تتعلق بالمدة التي يستطيع طفلك أن يقضيها في اللعب؛
- احرص على أن يلعبوا في غرفة المعيشة حيث يمكنك أن تراقبهم؛
- راقب عادات أبنائك في اللعب – إن كنت تراقبهم في فناء اللعب، فلم لا تفعل نفس الشيء حين يلعبون على الإنترنت؟
- ناقش محتوى اللعبة، أي الخصائص تضاهي الواقع وأيها لا تضاهيه، وما الذي يعجبهم فيها؟
- قبل أن تبتاع لعبة لابنك، تأكد من أن المحتوى يناسب العمر (بحسب نظام PEGI الأوروبي للتصنيف أو أي نظام قومي للتصنيف).

حين يلعب أبنائك على الإنترنت مع آخرين:

- اختر مواقع تفرض قيوداً صارمة وبها وسطاء حاضرون؛
- حذرهم من إفشاء التفاصيل الشخصية للاعبين الآخرين؛
- حذرهم من مقابلة اللاعبين الآخرين على أرض الواقع دون صحبتك؛
- شجع أبناءك على الإبلاغ عن حالات التنمر، والتهديد، واللغة غير اللائقة، وعرض محتوى بغيض، والدعوات للمقابلة خارج إطار اللعبة؛
- اسحب ابنك من اللعبة أو غير هويته على الإنترنت إن كان هناك شيء في داخل اللعبة أو الطريقة التي تسير بها يجعلك تشعر بعدم الاطمئنان.

روابط مفيدة

اعرف المزيد عن الألعاب على الإنترنت ونظام PEGI للتصنيف بحسب العمر:
http://www.pegioline.eu

يقدم CEOP معلومات مفيدة حول البقاء في أمان عند استخدام الدردشة والرسائل الفورية ومواقع التعارف الاجتماعي. استكشف الجلسات التفاعلية مع أبنائك:
http://www.thinkuknow.co.uk

افهم لغة الرسائل النصية من خلال موقع transl٨it:
http://www.transl8it.com

اصبح خبيراً في لغة الإنترنت بزيارة:
http://www.netlingo.com

جـ. الحلول المقترحة للأنشطة

١. الأمان يمنحك السلامة

أنشطة مفصلة

صل بين الصور والكلمات: صندوق الحاسب، مسند الفأرة، الشاشة، مكبرات الصوت، كاميرا الويب، الطابعة، عصا الـ USB (أو بطاقة الذاكرة)، الفأرة، أسطوانة مدمجة (سي دي).

تدريب تمهيدي لتعرف أبناءك بأجزاء الحاسب المختلفة وغيرها من المكونات. يمكنك أن تزيد إليها حسبما يتراءى لك.

اطلب من والديك أن يرسلا إليك رسالة بالبريد الإلكتروني بها مرفق، أو أرسل رسالة إلى نفسك. تدرب على ما يلي: انقر بالزر الأيمن من الفأرة على المرفق واحفظه على سطح الكتب في حاسبك. اذهب إلى سطح المكتب، انقر بالزر الأيمن بالفأرة ثم انقر على امسح. حين تعلم أن الوثيقة آمنة، يمكنك فتحها. تذكر: انقر بالزر الأيمن واحفظ – امسح – افتح.

أرسل رسالة إلى عنوان البريد الإلكتروني لابنك أو لعنوانك أنت وأرفق بها ملفاً. دع ابنك يتبع التعليمات المبينة في التدريب لحفظ الوثيقة عن طريق النقر عليها بالزر الأيمن دون فتحها. بعد حفظ الملف على سطح المكتب أو في مجلد مثل 'مستنداتي'، وضح لابنك كيف يقوم بالنقر على الملف بالزر الأيمن مرة أخرى لمسحه قبل فتحه للتشجيع على اتباع العادات الآمنة.

اتبع نصيحة سيرينا وتعلم كيف تصف عنوان بريدك الإلكتروني وقتما تحتاج بالفعل إلى نشره على الإنترنت. وهذا لتجنب التقاط عنوانك أتوماتيكياً واستغلاله من قبل مرسلي البريد المزعج. على سبيل المثال: cybercat = cybercat.smith@mymail.com دوت smith علامة 'أت' دوت كوم.

للتدريب، صف عناوين البريد الإلكتروني الخاصة لأفراد أسرتك: عنوانك، عنوان أسرتك، عنوان والدك، عنوان والدتك.

لتفادي التقاط عنوان بريدك الإلكتروني العام بواسطة برنامج ما لأغراض التوزيع، قم بوصفه بدلاً من كتابته بالطريقة المعتادة. دع ابنك يتدرب على هذا الأسلوب المقترح أعلاه. ولكن تذكر أنه يجب على أبنائك الامتناع عن نشر عناوين بريدهم على الإنترنت، وإن فعلوا، ينبغي أن يستخدموا عنواناً لا يكشف عن أسمائهم (راجع فصل التواصل).

لمساعدة لوسي على الفهم قبل أن تواصل سيرينا، ألق نظرة على الأنشطة الموجودة بالصندوق وارسم دائرة حول الأشياء التي يمكنك فعلها فقط إن كنت متصلاً بشبكة الإنترنت.

أبناؤك صغار السن قد لا يفهمون بوضوح أي الأنشطة تحتاج إلى الاتصال بالإنترنت وأيها لا يحتاج إلى ذلك. فكتابة نص لا يحتاج إلى حاسب متصل بالإنترنت، ولكن الدردشة تحتاج إلى ذلك. يمكنك الاستماع إلى الموسيقى بواسطة أسطوانة سي دي أو ملف موسيقى محفوظ على حاسبك، ولكنك تستطيع أيضاً الاستماع إلى الموسيقى مباشرةً على الإنترنت. على أبنائك أن يضعوا علامة على تلك الأنشطة فقط التي تستلزم الاتصال بالإنترنت.

قم مع والديك بكتابة العنوان التالي في متصفحك http://kids.yahoo.com. ابحث عن معلومات عن Tyrannosaurus Rex، وحاول أن تعرف متى كان هذا الديناصور يعيش على الأرض. كذلك حاول العثور على صورة واضحة له. لا تنس التأكد بالرجوع إلى ثلاثة مواقع مختلفة.

علم أبناءك مهارات البحث السليمة بأن تذكرهم ألا يثقوا بكل ما يرونه على الإنترنت. ذكرهم أن يبحثوا ويقارنوا المعلومات على ثلاثة مواقع على الأقل، مع ذكر المصدر دائماً عند كتابة الواجب المدرسي.

قم مع والديك بكتابة العنوان التالي في متصفحك http://kids,yahoo.com. ثم ابحث في موضوع ما، على سبيل المثال، Tyrannosaurus Rex، واحفظ المواقع الثلاثة التي تجدها شيقة بالنقر على قائمة المواقع المفضلة أعلى صفحة المتصفح وإضافتها إلى قائمة مواقعك المفضلة. كذلك يمكنك إنشاء مجلدك الخاص.

إن حفظ وتنظيم المواقع الشيقة في مجلد المواقع المفضلة (من خلال شريط أدوات الخيارات بالمتصفح) تُعد طريقة ممتازة لتقليص الوقت الذي يحتاجه أبناؤك الصغار للعثور على المعلومات على الإنترنت.

هل توصلت إلى الإجابات الصحيحة؟

١: (محمياً) ٢: (فيروس)، (غير معلوم)، (تحميل)، (مصابة)، (غير محم) ٣: (بطريقة غريبة) ٤: (لا تعرفهم) (مرفقات)، (عناوين موضوعات)، (بريداً مزعجاً) ٥: (واحداً)، (البريد المزعج) ٦: (أول)، (ثلاثة)، (قارن)، (أي شخص)، (نشر) ٧: (البرمجيات المضادة للفيروسات)، (والمضادة لبرمجيات التجسس) ٨: (تحدث)، (والديك) ٩: (أخبر)

الحلول المقترحة لبطاقات المواقف

الموقف ١. لا تقم أبداً بتصفح الإنترنت إن لم يكن حاسبك محمياً بواسطة نسخة حديثة من برنامج مضاد للفيروسات وبرنامج مضاد لبرمجيات التجسس. فهذا أشبه بأن يكون لك حدود دون حارس لها، من الممكن أن يصاب حاسبك ببرمجيات ضارة، كالفيروسات، أحصنة طروادة، الدودات وبرمجيات التجسس.

الموقف ٢. انتبه دوماً لرسائل البريد الإلكتروني التي تصلك من أشخاص لا تعرفهم والي تحتوي على مرفقات أو تلك الرسائل التي 'تغرقك بالوعود الوردية' – فهي في أغلب الظن من قبيل البريد المزعج! قد يتسبب البريد المزعج في إصابة حاسبك بالبرمجيات الضارة، كالفيروسات، أحصنة طروادة، الدودات وبرمجيات التجسس. لا تفتح هذه الرسائل. بدلاً من ذلك، قم بمنع المرسل عن طريق النقر بالزر الأيمن على البريد واختيار 'منع المرسل' أو فقط قم بحذفها.

الموقف ٣. عند البحث عن معلومات على الإنترنت، لا تثق فوراً في أول صفحة مفيدة تقابلها. راجع على الأقل ثلاثة مواقع مختلفة وقارن المعلومات التي تجدها عليها. تذكر: أي شخص لديه القدرة على الاتصال بالإنترنت يمكنه إنشاء أو نشر المعلومات على الشبكة. عند كتابة التقرير أو الواجب المنزلي، عليك دائماً أن تذكر مصدر المعلومات والصور التي استخدمتها... فهذا ما يفعله العلماء الحقيقيون.

٢. التواصل

أنشطة مفصلة

ضع علامة لتوضح درجة خصوصية الآتي بالنسبة لك: رقم هاتفك، لون شعرك، اسمك، البلد الذي تعيش فيه، المدرسة التي تدرس بها، عنوانك، اسم حيوانك الأليف، عنوان بريدك الإلكتروني، صورك، عمرك.

هل لدى أبنائك نفس مفهوم الخصوصية الذي لديك؟ الألوان الثلاثة تعني معلومات شديدة الخصوصية (أحمر)، معلومات خاصة تماماً (برتقالي)، ومعلومات ليست بهذه الخصوصية (أخضر).

ساعد لوسي على إنشاء كلمة المرور (كلمة السر) قوية باتباع نصائح سيرينا.

كلمات السر القوية تتألف من مجموعة عشوائية من الحروف (أرقام، حروف أبجدية وعلامات ترقيم) ويجب أن تظل سرية.

اتبع مثال لوسي وأنشئ ملف تعريف آمن. ثم اضرب مثلاً لملف تعريف آخر غير آمن.

دع أبناءك يقومون بإنشاء ملف تعريف آمن، ثم ملف آخر أقل أمناً يفشي معلومات خاصة. ذكر أبناءك أن إنشاء ملف تعريف آمن لن يحميهم إن لم يستمروا في حماية خصوصيتهم عند التواصل على الإنترنت.

استعرض هذه الصورة واكتب ما تستطيع استنتاجه عن هذا الشخص.

أي معلومات شخصية يمكن استنتاجها من الصورة؟ لا يدرك الأطفال في المعتاد قوة الصور.

'اتبع فكرة لوسي وفكر في ثلاث نصائح يحصل عليها "أليكس ذو الرداء الأحمر" من سيرينا لحماية نفسه من "ذئاب الإنترنت".

تأكد ما إذا كان أبناؤك قد أدركوا أن الاحتكاك الغرباء على الإنترنت قد ينطوي على المخاطر.

كيف تفضل أن يعاملك الناس على الإنترنت؟ (١..... ٢..... ٣.....)

تأكد أن أبناءك يفهمون أن عليهم معاملة الغير تماماً كما يودون أن يُعاملوا....

فك ألغاز الشفرة: اكتشف معاني بعض أشهر الاختصارات المستخدمة في الدردشة بربطها بمعانيها.

حسّن فهمك للاختصارات بالرجوع إلى فصل التواصل – آداب الإنترنت، ولغة الدردشة.

استخدم ثنائيات المفاتيح للرمز إلى أيقونات المشاعر التالية: وجه باسم – وجه حزين – وجه غامز – وجه مندهش – ابتسامة عريضة – وجه يخرج لسانه.

للمزيد من المعلومات راجع فصل التواصل – آداب الإنترنت، ولغة الدردشة.

هل توصلت إلى الإجابة الصحيحة؟

١: (ملف تعريفك) ٢: (خصوصيتك)، (مسؤولاً) ٣: (الغرباء)، (أخبر) ٤: (آداب الإنترنت)، (تُعامل) ٥: (أيقونة المشاعر) ٦: (كلمة المرور)، (ترقيم) ٧: (سرية) ٨: (أرفض) ٩: (تعرفهم)

الحلول المقترحة لبطاقات المواقف

الموقف ٤. حين تستخدم الإنترنت، فإن ملف تعريفك أو المعلومات التي تفصح بها عن نفسك يمكن أن تصل إلى العشرات، بل المئات، بل الآلاف، بل الملايين من الأشخاص. لذا من المهم أن تختار بعناية المعلومات التي تريد الإفصاح بها عن نفسك. لا تعط المعلومات الشخصية إلا لمن تعرفهم وتثق بهم جيداً خارج الإنترنت.

الموقف ٥. الأرجح أن "مايك" قد أطلع صديقه على كلمة المرور لبريده الإلكتروني، والذي قرر بدوره بعدها الانتقام منه عن طريق إرسال رسائل بغيضة باسمه. احتفظ دوماً بكلمات المرور لنفسك إلا إذا كنت لا تمانع أن يقرأ الآخرون بريدك الإلكتروني أو أن ينتحلوا شخصيتك ويقولون على لسانك ما يستحيل أن تتلفظ به قط!

الموقف ٦. مقابلة أحد الغرباء ليست فكرة صائبة. لكن إن كنت تظن أنه يمكنك حقاً أن تثق بأحد الأصدقاء من على الإنترنت ممن يريد مقابلتك، أخبر والديك بالأمر، وتأكد من أن يصحبك أحدهم. ولا يمكن أن يعترض على ذلك صديق حقيقي نواياه طيبة. فهذه تعتبر مشكلة فقط لمن لديهم ما يخفونه.

٣. التنمر على الإنترنت (التحرش)

أنشطة مفصلة

ارسم صورة للدعوة التي تلقاها أليكس من مدرسيه. أظهر رمز مقاومة التنمر والشعار الذي ترفعه المدرسة في أسبوع مقاومة التنمر.

دع أبناءك يظهرون قدراتهم الإبداعية ويرسمون في الإطار الخاوي.

اتبع مثال أليكس وقدم خمسة أسباب تجعلك ترفع البطاقة الحمراء لشخص ما.

ناقش مع أبنائك أي نوع من السلوك يجدونه غير مقبول.

هل توصلت إلى الإجابة الصحيح؟

١: (وفقاً للقواعد)، (يفسدون) ٢: (التحدث) ٣: (وجيه) ٤: (التنمر على الإنترنت) ٥: (أمنع) ٦: (أعرفهم) ٧: (أرد)

الحلول المقترحة لبطاقات المواقف

الموقف ٧: هذه بالقطع ليست طريقة مقبولة لاستخدام جوالك. لا تقم بتداول الرسائل والصور وغيرها من المواد الخبيثة. دائماً عامل الآخرين كما تحب أن يعاملوك. وفي مثل هذا الموقف، تحدث دوماً إلى والديك أو أي شخص آخر بالغ تثق به.

الموقف ٨: يجب على أليكس أن يخبر صديقه أن سوء سلوك المتنمر ليس خطأه. وعليه ألا يرد على رسائل المتنمر، ولكن يحتفظ بها كدليل ويريها لوالديه أو مدرسيه. كذلك يتعين على أليكس أن يناقش الأمر مع والديه إذ يمكنهم دعمه في مساعدة صديقه.

الموقف ٩: تتعلق آداب الإنترنت بمعاملة الآخرين على الشبكة كما تحب أنت أن يعاملوك. ونحن واثقون أنك قد تعلمت بالقدر الكافي الآن لمساعدة لوسي في هذه المهمة.

٤. الترفيه والتحميل

أنشطة مفصلة

افتح محرك البحث المفضل لك. واكتب "رنات جوال مجانية" أو "ألعاب مجانية"، واطلع على النتائج التي ستحصل عليها. تفقد بضعة مواقع. هل عثرت على أية فخاخ؟

تدرب عن طريق إجراء بحث بالكلمات الدالة المعطاة وتفقد المواقع التي ستجدها بحثاً عن خدع تسويقية. انظر كيف أن المعلومات المدونة بحروف صغيرة قد حذفت من الشعارات الإعلانية.

ما هي لعبتك المفضلة على الحاسب؟ تأكد هل يعرفها والداك ويستطيعان وصفها. إن كانا ليست لديهما فكرة، اشرحها أولاً ثم دعهما يكتبان وصفاً صغيراً عنها. هل أصابا؟ كم درجة من ١٠ درجات تعطيهما على هذا الوصف؟ .../١٠. يقوم الوالدان بتقديم موجز عن لعبة الابن المفضلة، ويقوم الطفل برسم صورة لها.

هل تعرف فعلاً أي نوع من الألعاب يلعبها أبناؤك على الإنترنت، وهل تعرف أي الألعاب هي المفضلة لديهم؟ دعهم يختبروا فهمك لهذا الأمر!

هل توصلت إلى الإجابة الصحيحة؟

١: (مجانية) ٢: (نماذج استمارات) ٣: (فخاخ) ٤: (علامة x) ٥: (تتجاهلها) ٦: (خصوصيتك)
٧: (استشارة) ٨: (تحميل)

الحلول المقترحة لبطاقات المواقف

الموقف ١٠. الاستبيانات على الإنترنت يمكن أن تكون وسيلة ناجحة جداً لتقديم رأي المستخدم. ولكن إن تم جمع معلومات عن المستخدم، فلابد من توضيح السبب. انصح أبناءك ألا يقوموا بملء نماذج استمارات على الإنترنت ما لم يفهموا السياق. وحتى إن فهموا السياق، فعليهم توخي منتهى الحذر عند الإفصاح عن معلومات شخصية (راجع فصل التواصل).

الموقف ١١. هناك خدمات مجانية على الإنترنت، إلا أن رنات الجوال، وخلفيات الشاشة، وأغاني الـMP3، والصور التجسيدية وما شابهها قلما تكون مجانية. ولو تأمل أليكس ذلك الموقع، الأرجح أنه سيجد الكتابة الموجودة بالخط الدقيق تشير إلى الكلفة الحقيقية للخدمة. رنات الجوال، والمسابقات، والألعاب، الخ، كلها وسائل ممتازة لجذب الناس للاشتراك في ما يُدعى بالخدمات "المجانية" التي، في واقع الأمر، ستكلفهم المال.

الموقف ١٢. يجب على أليكس أن يتذكر أن يحتفظ بهويته سرية كلما أراد اللعب على الإنترنت مع أشخاص لا يعرفهم في الحياة الواقعية. فعليه أن يمتنع عن الإفصاح عن معلومات تتعلق بمكان سكنه، والمدرسة التي يدرس بها، واسم عائلته، الخ. كذلك يتعين عليه أن يخبر والديه عن الألعاب التي يلعبها، وأن يمتنع عن تحميل أية لعبة من على الإنترنت قبل استئذانهما، إذ أن ذلك قد يلحق الضرر بحاسب المنزل.

د. مسرد المصطلحات

***Account* حساب:** يسمح لك الحساب بالخضوع للتوثيق والحصول على الإذن لاستخدام خدمات الإنترنت من خلال اسم المستخدم وكلمة المرور. كما يمكن إنشاء حسابات مستخدمين منفصلة ترتبط بنظام التشغيل لكل فرد من أفراد الأسرة يستخدم الحاسب.

***Acronym* الاختصار:** هي تسمية مختصرة تتألف من الحروف الأولى من كل كلمة في عبارة أو تعبير. كثيراً ما تُستخدم الاختصارات من قبل من يمارسون الدردشة لإيصال المعنى بشكل أسرع، مثل برب، تيت، باك (راجع فصل التواصل).

***Alert* الإنذار:** هو صندوق صغير يظهر على الشاشة لإعطاء معلومات أو التحذير من عملية قد تكون تخريبية، كبريد جديد أو حالة تلاعب ببرنامج حمايتك من الفيروسات.

***Anti-Virus* البرنامج المضاد للفيروسات:** هو برنامج للحاسب يحاول تحديد، وعزل، ومنع، وإزالة فيروسات الحاسب وغيرها من البرمجيات الخبيثة. يقوم البرنامج المضاد للفيروسات مبدئياً بمسح الملفات بحثاً عن الفيروسات غير المعروفة ثم يقوم بتعريف السلوك المشتبه فيه الصادر من برامج الحاسب والذي يشير إلى وجود إصابة.

***Anti-spyware* البرنامج المضاد للتجسس:** هو برنامج يقاوم برمجيات التجسس. يقوم البرنامج بمسح جميع البيانات الواردة بحثاً عن برمجيات التجسس ثم يقوم بمنع التهديدات التي عُثر عليها وتقديم قائمة يمكن الحذف منها.

***Attachment* المرفقات:** وهو ملف يتم إرساله مع رسالة البريد الإلكتروني. فالدودات والفيروسات غالباً تُوزع كمرفقات بالبريد الإلكتروني. يجب التشكيك و الحرص فى التعامل مع رسائل البريد الإلكتروني من المرسلين المجهولين.

***Avatar* الصورة التجسيدية:** هو ملف تعريف المستخدم الذي يمثله اسم المستخدم إلى جانب صورة، أيقونة أو شخصية ثلاثية الأبعاد في ألعاب الحاسب وعالم الإنترنت.

***Blog* المدونة:** هي لفظة مختصرة لعبارة مدونة الشبكة. هو موقع يقوم فيه فرد أو مجموعة بإضافة محتوى، غالباً يومياً، يتألف من النصوص، والصور، وملفات الصوت والفيديو، والروابط.

***Browser* المتصفح:** هو برنامج يُستخدم لاستعراض مواقع الإنترنت. بعض أشهر المتصفحات على برنامج التشغيل Windows هي Netscape Navigator، Internet Explorer وFirefox، أما Safari فهو أشهر المتصفحات على أجهزة Mac. تشتمل أحدث الإصدارات من هذه المتصفحات على خصائص الرقابة الأبوية.

***Browsing* التصفح:** هي عملية استخدام المتصفح من أجل استعراض موقع أو مجرد التجول عبر شبكة الإنترنت.

***Bullying* التنمر:** هو التحرش من خلال تكرار الأذى، والتعليقات الجنسية، والاعتداء الجسدي والكلام المهين من قبل واحد أو أكثر من المتنمرين.

***CD-Rom* سي دي روم:** هي اختصار لعبارة ذاكرة القراءة فقط على أسطوانة مدمجة. أي أسطوانة مدمجة غير قابلة للتسجيل عليها بيانات لا يستطيع قراءتها إلا الحاسب. يشيع استخدام الأسطوانات المدمجة لتوزيع برمجيات الحاسب.

***Chat* الدردشة:** هو الاتصال المتزامن على الإنترنت عن طريق الرسائل المكتوبة باستخدام تطبيقات الدردشة والرسائل الفورية (مثل MSN).

***Chat room* غرف الدردشة:** هي مكان افتراضي عام للاتصال اللحظي. يستطيع أشخاص من مختلف أنحاء العالم الالتقاء في غرف الدردشة والتحاور من خلال الرسائل التي يكتبونها بواسطة لوحة المفاتيح. إن كان أبناؤك يستخدمون غرف الدردشة، تأكد من أنها تتناسب مع أعمارهم وأن بها مراقبون ووسطاء.

***Child pornography* المواد الإباحية المتعلقة بالأطفال:** المواد الإباحية المتعلقة بالأطفال لها تعريفات قانونية مختلفة في مختلف الدول، الحد الأدنى منها هو ما يُعرّف المواد الإباحية المتعلقة بالأطفال بأنها صورة لطفل ضالع أو يبدو ضالعاً في نشاط جنسي واضح.

***Computer file* ملف:** هو أرشيف/مجموعة من المعلومات ذات الصلة (وثائق، برامج، الخ) مخزنة على الحاسب تحت مسمى خاص بها. يمكن اعتبار ملفات الحاسب النظير الحديث للوثائق الورقية التي كانت تُحفظ في ملفات المكاتب والمكتبات.

***Computer program* برنامج الحاسب:** وغالباً ما يُشار إليه بلفظة برمجية. تتألف البرمجية من سلسلة مهيكلة من الأوامر قام بوضعها مبرمجو الحاسب، بحيث تمكن مستخدمي الحاسب من إنجاز المهام. حين تبتاع أحد برمجيات الحاسب، ففي الغالب تحصل عليها على أسطوانة مدمجة (راجع التعريف)، وهي وسيلة مادية لتخزين البرامج.

***Contact list* قائمة الأسماء:** هي مجموعة من أسماء الأشخاص الذين تتصل بهم في برامج الرسائل الفورية والبريد الإلكتروني، والألعاب على الإنترنت، والجوال، الخ. من الممكن إضافة الأسماء، أو رفضها أو حذفها.

Cookies كوكيز: هو ملف يضيفه موقع الإنترنت إلى متصفحك. وفي كل مرة تدخل على هذا الموقع مرة أخرى، تعود ملفات الكوكيز إلى الخادم المخزن عليه الموقع. تحمل ملفات الكوكيز معلومات عن تفضيلاتك على الموقع، كما تُستخدم في مواقع التسوق عبر الإنترنت. قد يتسبب رفض ملفات الكوكيز في جعل بعض المواقع غير قابلة للاستخدام.

Copyright حقوق النشر والتأليف: هي مجموعة من الحقوق الحصرية تنظم استخدام فكرة أو عمل أو معلومات. حقوق النشر والتأليف يُشار إليها برمز "©".

Cracker مخترق: هو من يقوم بالدخول إلى أنظمة الحاسبات بشكل غير قانوني.

Crack, to اخترق: هو القيام بنسخ البرمجيات التجارية على نحو غير قانوني من خلال خرق خاصية حماية حقوق النشر والتأليف.

Cyberbulling التنمر على الإنترنت: يشير إلى التنمر عبر الوسائط الإلكترونية، غالباً من خلال الرسائل الفورية والبريد الإلكتروني. وقد ينطوي على تكرار الأذى، والتعليقات الجنسية، والاعتداء الجسدي والكلام المهين. قد يقوم المتنمرون على الإنترنت بنشر بيانات الاتصال الشخصية للضحايا وكذلك انتحال شخصياتهم ونشر مواد بأسمائهم لأغراض تشويه سمعتهم أو الاستهزاء بهم.

Digital Game الألعاب الرقمية: هي الألعاب التي يقوم بتصميمها ولعبها مطورو الألعاب على الحاسب. تُعرف الألعاب على الإنترنت بأنها ألعاب رقمية تحتاج إلى الاتصال الحي بالشبكة كي يُمكن لعبها. يمكن للألعاب على الإنترنت أن تدعم التفاعل بين عدة لاعبين.

Directory الدليل: هو وحدة تنظيمية يستخدمها حاسبك لتنظيم المجلدات والملفات في هيكل هرمي، مثل 'مستنداتي'، 'صوري'، الخ.

Download التحميل: يشير إلى عملية نسخ ملف من خدمة على الإنترنت إلى الحاسب.

Email البريد الإلكتروني: هو وسيط للاتصال الكتابي الإلكتروني يسمح لك بإرسال رسائل مرفق بها أي نوع من ملفات الحاسب – سواء ملفات نصية أو صوتية أو صور وغيرها.

Email address عنوان البريد الإلكتروني: هو عنوان افتراضي تصل إليه رسائل البريد الإلكتروني. يتألف عنوان البريد الإلكتروني من جزأين تفصلهما علامة @.

Emoticon أيقونات المشاعر: هي صورة أو أيقونة تُستخدم لنقل الأحاسيس والمشاعر مثل الوجه الباسم. يمكن الرمز إليها باستخدام الأحرف التقليدية وعلامات الترقيم على لوحة المفاتيح أو باستخدام الأحرف الجاهزة التي توفرها غرف الدردشة، وغرفة الألعاب، وخدمات الرسائل الفورية، الهواتف الجوالة، الخ.

Family settings إعدادات الأسرة: والتي تعرف أيضاً بالرقابة الأبوية. هي إعدادات تُستخدم لتخصيص المتصفح أو غيره من أدوات الإنترنت بغرض جعلها أكثر ملاءمة للأطفال من خلال استخدام خصائص كتصفية المحتوى، القيود الزمنية، القيود داخل الألعاب، الخ.

Favourites المواقع المفضلة: هو أحد مجلدات المتصفح التي يمكن تخصيصها ويمكنك أن تخزن به الروابط/الإشارات المرجعية المميزة. يمكن ترتيب الإشارات المرجعية في مجلدات فرعية و/أو ربطها بكلمات توضيحية لضمان سهولة البحث.

File sharing مشاركة الملفات: هو عملية تبادل الملفات بين الحاسبات على الإنترنت. يشمل المصطلح تقديم الملفات للمستخدمين الآخرين (الرفع) ونسخ الملفات المتاحة من الإنترنت إلى الحاسب (التحميل). في المعتاد، تتم المشاركة في الملفات بواسطة شبكات P2P (النظير للنظير).

File transfer نقل الملفات: هي عملية نقل الملفات عبر شبكة حاسبات. من وجهة نظر المستخدم، فإن عملية نقل الملفات في الغالب يُشار إليها إما بالرفع أو التحميل.

Filter عامل تصفية: هو تطبيق يعمل على تنظيم سبل الوصول إلى المعلومات أو خدمات محددة على الإنترنت، والتحذير من مواقع مشتبه فيها، واقتفاء جولات المستخدم في تصفحه للشبكة، ومنع المواقع التي تنطوي على مخاطر، وربما أيضاً إغلاق الحاسب تماماً. أنظمة التصفية يمكن تثبيتها على الحاسبات المستقلة، الخوادم، الهواتف الجوالة التي تدخل على الإنترنت، الخ.

Firewall جدار الحماية: هو جهاز (يتم إدماجه مع الموجه "الراوتر") أو برنامج (يتم تثبيته على حاسبك) ويتم ضبطه بحيث يمنع المستخدمين غير المصرح لهم (المتسللين أو المخترقين) من الدخول إلى الحاسب أو شبكة الحاسبات المتصلة بالإنترنت.

Flaming الرسالة النارية: هي التفاعل العدائي والمهين بين مستخدمي الإنترنت. وهو في الغالب يدور على ساحات النقاش، الدردشة عبر الإنترنت أو حتى من خلال البريد الإلكتروني.

Folder المجلد: هو كيان داخل نظام الملفات يحتوي على مجموعة من الملفات و/أو الأدلة الأخرى. يمكن أن تضم المجلدات عدة مستندات وهي تُستخدم لتنظيم المعلومات.

Form(online form) نموذج استمارة (على الإنترنت): هي وثيقة منسقة تحتوي على خانات فارغة يمكن ملؤها بالبيانات. نموذج الاستمارة الإلكترونية يمكن ملؤها بواسطة النص الحر أو عن طريق الاختيار من قائمة سابقة الإعداد (القوائم المنسدلة). بعد تقديم النموذج، تُرسل البيانات مباشرةً إلى تطبيق معالجة البيانات، الذي يقوم بدوره بإدخالها إلى قاعدة البيانات.

Forum المنتدى: هي مجموعة نقاش على الإنترنت حيث يستطيع المشاركون ذو الاهتمامات المشتركة تبادل الرسائل بحرية حول مختلف الموضوعات.

Freeware and shareware البرمجيات المجانية والبرمجيات المشتركة: بصفة عامة، تتمتع البرمجيات بحماية حقوق النشر والتأليف ومن ثم فلا يمكن تحميلها. يُقصد بالبرمجيات المجانية أن صاحب حقوق النشر والتأليف يوافق على استخدام البرمجيات من قبل أي شخص دون مقابل. أما البرمجيات المشتركة فتعني أن صاحب حقوق النشر والتأليف يوافق على استخدام البرمجيات من قبل أي شخص لفترة تجريبية. بعد انتهاء تلك الفترة، يتعين على المستخدم دفع رسوم للاستمرار في استخدام الخدمة.

Grooming الاستمالة: هي استخدام غرف الدردشة من قبل بعض المهاويس بجنس الأطفال بغرض استمالة الأطفال بالتظاهر بأنهم نظرائهم. يبدأ هؤلاء المهاويس الحوار مع الضحايا المحتملين لاستخلاص معلومات بشأن أماكنهم واهتماماتهم وهواياتهم وخبراتهم الجنسية. ويستعمل هؤلاء المعتدون مختلف السبل لجذب الأطفال من خلال حوارات ذات طبيعة جنسية.

Hacker المتسلل: هو مصطلح شائع الاستخدام يشير إلى شخص يضطلع بأنشطة اختراق الحاسب (راجع 'مخترق'). كما يمكن استخدامها في مجالات الحاسبات لوصف شخص من هواة الحاسب.

Hardware مكون الحاسب: الجزء الملموس من الحاسب، لتمييزه عن برمجيات الحاسب التي تعمل داخل مكوناته. هذه الأجزاء قد تكون داخلية: كاللوحات الأم، محركات الأقراص الصلبة، ذاكرة الوصول العشوائي – والتي غالباً ما يُشار إليها بالمكونات، أو خارجية: الشاشات، لوحات المفاتيح، الطابعات، الخ – والتي تسمى أيضاً بالوحدات الطرفية للحاسب.

Harmful content المحتوى الضار: الصور، والنصوص، والوثائق، الخ ذات المحتوى القادر على إلحاق الضرر، فمثلاً الصور التي تظهر العنف تعد غير مناسبة وخبيثة للأطفال والقصر.

Helpline خط المساعدة: هي خدمة بالبريد الإلكتروني وأحياناً بالهاتف توفرها منظمات دعم الطفل وأعضاء شبكة Insafe في مختلف الدول. يمكن للأطفال إثارة مخاوفهم بشأن المحتوى غير القانوني والضار وكذلك التجارب غير المريحة والمخيفة التي تتعلق باستخدامهم لسبل التكنولوجيا عبر الإنترنت.

Homepage الصفحة الرئيسية: هي تلك الصفحة على الإنترنت التي تظهر تلقائياً عند بدء المتصفح. كما يُستخدم المصطلح أيضاً للإشارة إلى الصفحة الأمامية أو الصفحة الرئيسية من موقع الإنترنت (راجع التعريف).

Hotline الخط الساخن: هو خط هاتف للمساعدة أو الخدمة عبر الإنترنت حيث يمكن للناس التقدم بالشكاوى بشأن إدعاء أن المحتوى و/أو استخدام الإنترنت غير قانوني. لابد أن تكون للخطوط الساخنة إجراءات فعالة وواضحة في التعامل مع الشكاوى وأن تحظى بدعم الحكومة والصناعة وإنفاذ القانون ومستخدمي الإنترنت في البلدان التي تعمل فيها هذه الخطوط.

Identity theft سرقة الهوية: هي سرقة البيانات الشخصية (كالاسم، وتاريخ الميلاد، ورقم بطاقة الائتمان)، واستخدامها بطريقة غير مشروعة.

Illegal content المحتوى غير المشروع: هو ذلك المحتوى على الإنترنت الذي يُعد غير مشروع وفقاً للتشريع القومي. أكثر الأنواع شيوعاً لمثل هذا النوع من المحتوى هو صور الاستغلال الجنسي للأطفال، الأنشطة غير القانونية في غرف الدردشة (مثل الاستمالة)، ومواقع الكراهية وبغض الأجانب.

Instant Messaging (IM) الرسائل الفورية: هي صورة من صور الاتصال الإلكتروني الفوري واللحظي بين مستخدمَين أو أكثر. تسمح لك الرسائل الفورية بالتواصل مع قائمة مختارة من الأشخاص. حين يكون الأشخاص المدرجون في قائمتك متصلين بالإنترنت، ستتسلم إخطاراً على الفور.

Internet الإنترنت: هي شبكة عالمية عامة مفتوحة للجميع تتألف من شبكات من الحاسبات المتصلة تتم من خلالها عمليات نقل وتبادل البيانات. وهي تضم شبكات أصغر تتباين في طبيعتها من منزلية إلى أكاديمية وتجارية وحكومية، كما تحمل العديد من الخدمات المختلفة ، كالمعلومات والبريد الإلكتروني والدردشة على الإنترنت ونقل البيانات، الخ.

Internet connection وسيلة الاتصال بالإنترنت: يشير إلى الوسيط الذي يمكن من خلاله للمستخدمين الاتصال بالإنترنت. تتضمن السبل الشائعة للدخول على الإنترنت الاتصال الهاتفي، خطوط T، شبكات Wi-Fi اللاسلكية، الأقمار الصناعية والهواتف النقالة.

Junk/Spam folder مجلد الرسائل غير المرغوب فيها/العشوائية: في صندوق البريد الإلكتروني، هو ذلك المكان التي تُخزن فيها الرسائل التي تعتبر عشوائية أو غير مرغوب فيها.

Junk mail البريد غير المرغوب فيه: هي رسائل البريد الإلكتروني التي لا يرغب فيها المستخدم والتي تكاد تكون مطابقة والتي تُرسل إلى أصحاب عناوين البريد الإلكتروني. ونظراً لأن الإنترنت شبكة عامة، فليس هناك ما يمكن فعله لمنع البريد غير المرغوب فيه، تماماً كما يستحيل منع الرسائل العشوائية.

Link الرابطة: هي إشارة مرجعية إلى وثيقة ما متاحة على الإنترنت (كصفحة من موقع، وثيقة نصية، صورة، الخ). حين تقوم بالنقر على الرابطة، ستأخذك إلى صفحة جديدة أو إلى موقع مختلف تماماً. الروابط النصية تكون في المعتاد زرقاء اللون ويظهر تحت خط أفقي، غير أنها قد تكون بأي لون آخر وغير محددة بخط أسفلها. كما أن الصور تؤدي وظيفة روابط تقود إلى صفحات أخرى على الإنترنت.

Malware البرمجيات الخبيثة: وهي البرمجيات التي صُممت كي تخترق أو تلحق الضرر بأنظمة الحاسب دون الموافقة الواعية من قبل المستخدم. وهي تشمل الفيروسات، الدودات، أحصنة طروادة، برمجيات التجسس، البرمجيات الإعلانية المضللة وغيرها من البرمجيات الخبيثة غير المرغوب فيها.

Manipulate التلاعب: هي عملية التغيير في صورة أو ملف أو صورة فوتوغرافية أو رسم إيضاحي بطريقة واضحة أو غير واضحة. توجد حالياً العديد من الأدوات التي يمكن استخدامها للتأثير على محتوى أو شكل البيانات مما يؤدي إلى نتيجة تختلف عن الواقع.

Massively Multiplayer Games الألعاب الهائلة متعددة الأطراف: وهي الألعاب التي تقدم عالماً ثرياً ثلاثي الأبعاد يعج بآلاف اللاعبين الذين ينتحلون أسماء شخصيات وهمية ويتنافسون في اللعب. وتنتشر في هذا النوع ألعاب تمثيل الدور حيث يتعاون اللاعبون على البدء في أو متابعة قصة.

Memory/USB stick بطاقة ذاكرة/USB: هي وسيلة تخزين بيانات تعتمد على واصلة الـ USB. بطاقات الذاكرة تكون في المعتاد صغيرة، خفيفة الوزن، يمكن نقلها وإعادة التخزين عليها.

Mobile الجوال: هو جهاز إلكتروني للاتصال عن بعد، يعرف أيضاً بالمحمول، والخلوي، والنقال. يتمتع الجوال بنفس الإمكانيات الأساسية للهاتف الثابت. وحالياً تتضمن أغلب الجوالات كاميرا، كما أن الكثير منها يوفر إمكانية الدخول على الإنترنت (من خلال خدمة مدفوعة).

Mp3 : هي صيغة ترميز خاصة بالملفات المسموعة. يصل حجم الملف بصيغة Mp3 إلى نحو عشر حجم الملف الصوتي الأصلي، غير أن الصوت يكون بجودة الأسطوانات المدمجة. وبسبب حجمه الصغير ونقاء جودته، صارت ملفات الـMp3 طريقة شائعة لتخزين ملفات الموسيقى على أجهزة الحاسبات والأجهزة المحمولة.

Net الشبكة: هي اختصار لشبكة الإنترنت.

Netiquette آداب الإنترنت: هي الآداب الداخلية التي تملي قواعد التأدب في الاتصالات عبر الإنترنت.

Newsgroup المجموعة الإخبارية: راجع تعريف المنتدى.

Nickname الكنية: مرادف لاسم الشاشة وكود التعريف. فهو يمثل مستخدم إحدى خدمات الإنترنت ويحدده المستخدم بنفسه. كما يمثل المستخدمين الذين يظهرون في قوائم الأسماء، وغرف الدردشة، الخ. الكُنى، إن اختيرت بعناية، فمن الممكن أن تعمل على إخفاء هويتك على الإنترنت.

Operating System نظام التشغيل: هو برنامج يقوم بتشغيل الوظائف الأساسية للحاسب، ويمكّن البرامج الأخرى من العمل. من أشهر الأمثلة Linux، Windows وMac OS.

Parental control الرقابة الأبوية: راجع تعريف إعدادات الأسرة.

Password كلمة المرور: هي سلسلة سرية من الأحرف تمكّن صاحبها من الدخول إلى الملفات، والحاسب، وبرنامج ما على سبيل الإجراء الأمني ضد المستخدمين غير المصرح لهم (راجع فصل التواصل).

Personal data البيانات الشخصية: هي أية معلومات يمكن ربطها بالشخص. إن كانت هناك حاجة إلى جمع، ومعالجة وتخزين البيانات الشخصية، فلابد من ذكر الأغراض بوضوح.

Pop-up window النافذة المنبثقة: هي نافذة تظهر فجأة عند زيارة موقع ما أو الضغط على زر له وظيفة خاصة. في المعتاد، تتضمن النوافذ المنبثقة قائمة بالأوامر وتبقى على الشاشة حتى تختار أحد هذه الأوامر أو تغلقها بالنقر على علامة x في الركن الأعلى الأيمن.

Port المنفذ: هي وصلة بينية على الحاسب تُستخدم لإيصاله بجهاز آخر. المنافذ إما داخلية أو خارجية. المنافذ الداخلية تتصل بمحرك الأقراص أو شبكة ما، أما المنافذ الخارجية فتتصل بالأجهزة الطرفية كالطابعة أو لوحة المفاتيح.

Privacy الخصوصية: هي قدرة الفرد أو المجموعة على التحكم في تدفق المعلومات الخاصة بهم ومن ثم فهم يكشفون عن هويتهم باختيارهم. تتعلق الخصوصية أحياناً إخفاء الهوية، وهي الرغبة في أن يظل المرء مستتراً في العلن.

Privacy settings إعدادات الخصوصية: هي مجموعة من تفاصيل الخصوصية المتعلقة بحساب المستخدم والتي يمكنك أن تغيرها كي تزيد من خصوصيتك ضد انكشاف المعلومات الشخصية، وملفات الكوكيز، الخ.

Private خاص: هي كل ما يتعلق بالفرد أو المجموعة ولا يتم الإفصاح عنه علناً. حين يكون شيء ما خاصاً بالنسبة للشخص، فهذا في الغالب يعني أن لديه ما يعتبره مميزاً في ذاته أو حساساً بشكل شخصي.

Processor المعالج: أو وحدة المعالجة المركزية هي تلك الجزء من الحاسب الذي يعالج البيانات، ويصدر إشارات التحكم، ويخزن النتائج. هذه الوحدة إلى جانب، ذاكرة الحاسب، يمثلان مركز الحاسب.

Profile ملف التعريف: هي المعلومات الشخصية للمستخدم في مواقع التعارف الاجتماعي، وأنظمة الرسائل الفورية، وتطبيقات الدردشة على الإنترنت، والألعاب على الإنترنت، الخ. قد تكون ملفات التعريف إما عامة أو خاصة، ويقوم المستخدمون أنفسهم بتخصيصها في الأماكن الافتراضية.

P2P network شبكة النظير للنظير: تسمح شبكة النظير للنظير لمن يتصل بها بتبادل الملفات عن طريق رفعها وتحميلها (راجع التعريفات). وهي مجرد إحدى سبل المشاركة في الملفات عبر الإنترنت. إلا أن بعض خدمات مشاركة الملفات غير قانونية.

Recycle bin سلة المحذوفات: هي دليل بالحاسب تُخزن به مؤقتاً الملفات المحذوفة قبل أن يقوم المستخدم بحذفها نهائياً. يتعين عليك المداومة على التخلص من البيانات القديمة التي لا تحتاجها من سلة المحذوفات لتحرير مساحة على القرص الصلب، وهو حيز التخزين الداخلي بحاسبك.

Report الإبلاغ: هي خاصية تسمح لمستخدمي الفضاءات الافتراضية العامة بالإبلاغ عن مشكلة (سواء مشكلة فنية، أو سلوك غير مقبول من قبل أحد المستخدمين، أو محتوى غير قانوني، الخ) إلى الوسيط أو مسؤول الموقع.

Ringtone رنة الجوال: هي الصوت الذي يصدره الهاتف الجوال عند استقبال مكالمة. هناك مجموعة متنوعة وهائلة من الرنات والموسيقى القابلة للتخصيص والمتاحة لأصحاب الهواتف الجوالة لتحميلها، وفي الغالب شرائها، واستخدامها.

Safety settings (profile) إعدادات (ملف تعريف) الأمان: هي مجموعة من خيارات الأمان القابلة للتخصيص والمتصلة بملف تعريف على الإنترنت (راجع التعريف). في المعتاد تتعلق هذه الخيارات بفتح الصور والملفات، والتعرف على موفري المعلومات الذين يمكن الوثوق بهم ومستويات السماح بالمحتوى المخصص للبالغين.

Scan مسح: هي عملية تحويل المادة المطبوعة إلى ملفات رقمية باستخدام الماسحة الضوئية. يسمح لك هذا التحويل باستعراضها على حاسبك وتوزيعها على الإنترنت.

Screen name اسم الشاشة: راجع تعريف الكنية.

Search engine محرك البحث: هي أداة تُستخدم للبحث عن معلومات من على مواقع الإنترنت. أشهر محركات البحث هما Google وMSN Search. تحتوي محركات البحث على تفضيلات متقدمة للمستخدمين قد تشمل إعدادات هامة للأمان.

Second Life : هو مجتمع ثلاثي الأبعاد شهير على الإنترنت تقدمه شركة أميركية تُدعى Linden Labs. يمكن للمستخدمين التفاعل افتراضياً عبر الصورة التجسيدية (راجع التعريف)، وإنشاء منازل، وبيئات مختلفة، والانخراط في التجارة وكسب عملة افتراضية، الخ. قم بزيارة www.secondlife.com.

Sign-up الانضمام: تعني الاشتراك في خدمة على الإنترنت: كالرسائل الإخبارية، ومنتديات النقاش، والبريد الإلكتروني، ومنابر الدردشة، الخ. في المعتاد، يجب أن يُتاح للمستخدمين خيار تسجيل الخروج وقتما يشاءون.

SIP-Bench : هي دراسة تدعمها المفوضية الأوروبية قامت بفحص ٣٠ أداة من أدوات التحكم ومقاومة الرسائل المزعجة بغرض قياس درجة فاعليتها في حماية الأطفال من المحتوى الضار على الإنترنت.

Social networking التعارف الاجتماعي: هو مجموعة من الأعضاء على الإنترنت تجمعهم اهتمامات وأنشطة مشتركة، يتفاعلون ويتعارفون على الإنترنت باستخدام برمجيات وخدمات ملائمة (راجع مواقع التعارف الاجتماعي).

***Social networking sites* مواقع التعارف الاجتماعي:** هي المنابر الافتراضية التي تستضيف مجموعات الأعضاء الذين تجمعهم اهتمامات وأنشطة مشتركة. يتعين على الأعضاء إنشاء ملفات تعريف ويمكنهم التشارك في الأدوات لرفع النصوص، والصور وغيرها من الملفات، ونشر الرسائل على لوحات النقاش والمشاركة في المنتديات. تحظر العديد من مواقع التعارف الاجتماعي دخول الأطفال دون عمر ١٣ عاماً وتقدم إعدادات للملفات التعريف الآمنة.

***Software* البرمجيات:** راجع تعريف برنامج الحاسب.

***Spam* الرسائل المزعجة:** هي البريد الإلكتروني غير المرغوب فيه، وغالباً ما يكون ذا طبيعة تجارية، ويتم إرساله بأعداد ضخمة. إرسال الرسائل المزعجة إلى الناس هو بالقطع إحدى أسوأ صور الاختراقات الشهيرة على الإنترنت.

***Spam filter* عامل تصفية الرسائل المزعجة:** هو تطبيق يمنع تخزين الرسائل المزعجة في صندوق الوارد ببريدك الإلكتروني.

***Spyware* برمجيات التجسس:** هي برمجيات خبيثة تُرفق سراً إلى الملفات التي يتم تحميلها من على الإنترنت، وتقوم بتثبيت ذاتها على الحاسب لمراقبة الأنشطة. ثم تقوم بإرسال المعلومات إلى طرف ثالث، الذي يكون في الغالب شركات تهتم بتحديد ملفات التعريف الشخصية بغرض إرسال إعلانات وغيرها من المعلومات، أو إلى المخترقين ممن يرغبون في الوصول إلى بياناتك الخاصة.

***Subscribe* الاشتراك:** هي عملية التسجيل الطوعي في خدمة أو تحديث إخباري حيث يتم إرسال المعلومات مباشرةً إلى صندوقك للبريد الإلكتروني الوارد.

***Toolbar* شريط الأدوات:** هي مجموعة من الأيقونات أو الأزرار التي تشكل جزءاً من واجهة برنامجاً للحاسب. تتمثل فائدة شريطة الأدوات في كونه واجهة سهلة الاستعمال ومتاحة دائماً لإتمام الوظائف الأساسية.

***Trial software* برمجيات تجريبية:** هي البرمجيات التي يمكنك تجربتها قبل شرائها. تحتوي النسخ التجريبية من البرمجيات في أغلب الأحيان على جميع الخواص الوظيفية للنسخة المعتادة، إلا أنه لا يمكن استخدامها إلا لمدة محدودة.

***Trojan horses* أحصنة طروادة:** هو كود خبيث، أي برنامج خبيث يمكنه أن يدخل إلى حاسبك متخفياً وراء مظهر بريء كالألعاب أو ربما برامج تتعقب الفيروسات. لا تقوم أحصنة طروادة بالتكاثر ذاتياً، إلا أنها في المعتاد تكون مصممة بحيث تدخل إلى البيانات الحساسة أو تدمر البيانات، كما يمكنها مسح قرصك الصلب أو سرقة معلومات سرية.

***URL (Uniform Resourse Locator)* (عنوان موحد للمصدر):** هو عنوان موقع أو ملف بعينه على الإنترنت. وهو لا يتضمن أحرف خاصة أو مسافات ويستخدم الشرطة المائلة للأمام للإشارة إلى مختلف الأدلة. يشير الجزء الأول من العنوان إلى البروتوكول المستخدم، أما الجزء الثاني فيحدد عنوان الIP (بروتوكول الإنترنت) أو اسم النطاق الذي يوجد به المورد.

***User profile* ملف تعريف المستخدم:** هي مجموعة من البيانات التي تصف مستخدم بعينه للبرمجيات، أو موقع ما أو غيرها من الأدوات الفنية. وهو في المعتاد يشمل معلومات كاسم المستخدم وكلمة المرور وغيرها من التفاصيل (كتاريخ الميلاد، والاهتمامات).

***Virtual possession* الممتلكات الافتراضية:** هي مجموعة من الأغراض تخصص لكل واحد من اللاعبين في لعبة ما. ويكون لكل لاعب الحق في الامتلاك الافتراضي لأغراضه عبر جهاز طرفي للحاسب تظهر عليه مجموعة الأغراض.

***Virus* فيروس:** هو نوع من الأكواد الخبيثة، أو البرمجيات الخبيثة، صُمم كي ينتشر بتدخل من قبل المستخدم. في المعتاد ينتشر الفيروس من خلال مرفقات البريد الإلكتروني وكذلك من خلال أدوات الذاكرة الخارجية المصابة (كبطاقات USB، أو الأسطوانة المدمجة – ذاكرة القراءة فقط)

***Voice over Internet Protocol (VoIP)* نقل الصوت عبر بروتوكول الإنترنت:** هي تكنولوجيا تسمح للمستخدمين بالتحدث عبر الإنترنت، بعد تحميل البرمجيات اللازمة. يمكن أن تكون المكالمات مجانية بالنسبة للمتحدثين الذين يستخدمون نفس برنامج التحدث بنظام VoIP (مثل Skype، Voicebuster). كما توفر مثل هذه البرمجيات أيضاً في المعتاد إمكانياتي الدردشة ومشاركة الملفات.

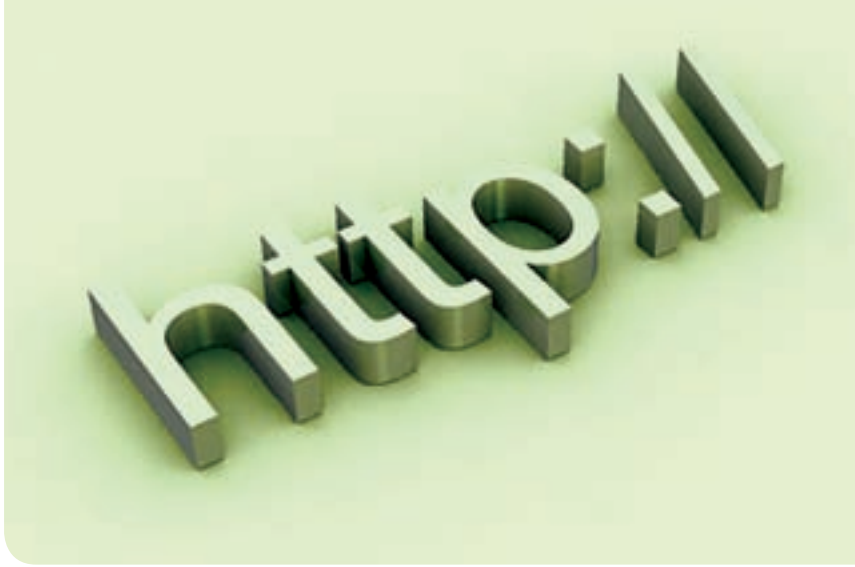
***Wallpaper* خلفيات الشاشة:** هو نقش أو رسم أو صورة تشكل خلفية شاشة حاسبك.

***Web* الشبكة العنكبوتية:** هي مجموعة من الوثائق على الإنترنت ذات تنسيق HTML (لغة تحديد النص المترابط) تشمل روابط تقود إلى وثائق أخرى كالصور والملفات الصوتية أو ملفات الفيديو. الشبكة العنكبوتية هي جزأ من شبكة الإنترنت الأعم.

***Website* موقع الإنترنت:** هو موقع من المواقع التي توجد على شبكة الإنترنت. يحتوي كل موقع على صفحة رئيسية، وهي الوثيقة الأولى التي تراها حين تدخل إلى الموقع. في المعتاد يضم كل موقع روابط إلى ملفات ومواقع إضافية. مواقع الإنترنت يملكها ويديرها الأفراد والشركات والمنظمات.

***Webcam* كاميرا الويب:** هي كاميرا يمكنها أن تبث ما تلتقطه عبر الإنترنت، في الرسائل الفورية وتطبيقات المؤتمرات المرئية عبر الحاسب الشخصي، ومنابر الدردشة، الخ. تشمل الكاميرات التي يمكنها الدخول على الإنترنت كاميرا رقمية تقوم برفع الصور إلى خادم الويب، إما بشكل متواصل أو على فترات منتظمة.

***Worm* الدودة:** هي نوع من الفيروسات يتكاثر ذاتياً ويمكنه الانتشار بدون تدخل من المستخدم عبر مختلف الحاسبات وإلحاق الضرر بالشبكة، أو شغل جزء كبير من عرض النطاق الترددي، أو إغلاق الحاسب، الخ.



هـ. عناوين مفيدة

Thinkuknow

هذا الموقع الذي تستضيفه CEOP، هو تلك العقدة المتعلقة بالوعي والأمان على الإنترنت في الشبكة البريطانية. يقدم موقع Thinkuknow المعلومات والنصح، فضلاً عن الأدوات للوالدين والمدرسين لدعم الأمان والاستخدام المسؤول للإنترنت:

http://www.thinkuknow.co.uk

BECTA

الوكالة البريطانية للاتصالات والتكنولوجيا التعليمية هي وكالة بريطانية حكومية أُنشئت لتقديم النصح والدعم والمعلومات المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات في مجال التعليم:

http://www.becta.org.uk

The Hotline

للتقدم ببلاغ بشأن محتوى صادفته على الإنترنت وتشك في كونه غير قانوني، اتصل بالخط الساخن:

http://www.iwf.org.uk

Childnet

يقدم موقع Childnet نطاقاً من الموارد للوالدين والأبناء والمدرسين. Childnet هي منظمة غير هادفة للربح تتعاون مع الغير "للعمل على جعل الإنترنت مكاناً آمناً للأطفال":

http://www.childnet.com

Childline Online

Childline هي خدمة تستمر ٢٤ ساعة للأطفال والشباب حتى عمر ١٨ سنة. وهو مفتوح ٣٦٥ يوماً في العام (حتى في الأعياد!) لتقديم الدعم للشباب من خلال خدمة Childline للإنصات (٠٨٠٠ ١١١١) عبر الهاتف ومن خلال موقع Childline Online. يمكنك الاتصال بخدمة Childline للدردشة أو التحدث عن أية مشكلات تعاني منها بما فيها تلك المتعلقة بالإنترنت:

http://www.childline.org.uk

Get Safe Online

Get Safe Online هو موقع يُعنى بالوعي القومي والمعلومات (تحت رعاية الحكومة البريطانية) ويركز على مسائل أمان تكنولوجيا المعلومات، تحديداً؛ التصيُّد، وبرمجيات التجسس، وسرقة الهويات:

http://www.getsafeonline.org

Insafe

تهدف الشبكة الأوروبية لرفع الوعي حول الأمان الإلكتروني إلى تمكين المستخدمين من الاستفادة من الجوانب الإيجابية لاستخدام الإنترنت مع تفادي المخاطر المحتملة:

http://www.saferinternet.org

بدعم من:

العنوان: دليل إرشادي للوالدين • أعدته شبكة Insafe بدعم من Liberty Global/UPC وthe South West Grid for Learning عام 2008.
Prefix: 9789078209 • Id 51950 • ISBN-NUMBER: 9789078209577 • EAN: 9789078209577