

Heads Up:

توقف. فكر.
اتصل

ARABIC

انقر

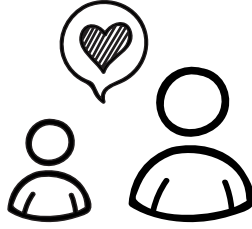
www



.com



#



لمساعدة أطفالك على البقاء آمنين عند استخدامهم للإنترنت، اشترك في حملة *Heads Up*: توقف. فكر. اتصل. وهذه هي بعض الأفكار التي تساعدك على بدء النقاش معهم. اختر قسم من الكتيّب واقرأه معهم لمعرفة كيفية مشاركة المعلومات بوعي والتعامل وحرص عبر الإنترنت والتصدي للابتزاز السيبراني، وحماية معلوماتهم (معلوماتك) الشخصية أثناء استخدامهم للإنترنت. هذه الأدوات ستساعدك في تدريب أطفالك على كيفية اتخاذ اختيارات جيدة واستخدام التكنولوجيا مع التحلي بالوعي والمسؤولية. وذلك من خلال التحدث مع أطفالك، فإنك تجعلهم يعرفون أن لديهم شخصاً كبيراً موثقاً به يقدم لهم المساعدة عندما يرتكبون أخطاءً.

To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

التواجد عبر الإنترنت هو جزء من حياتك. حيث يمكنك مشاهدة المحتوى وإنشائه، ونشر الصور ومقاطع الفيديو، ولعب الألعاب، ومشاركة موقعك وتفاعلاتك مع أصدقائك وعائلتك. ولكن هناك مخاطر عندما تقوم بالنشر واللعب والتواصل عبر الإنترنت. حيث يختلف بعض الأشخاص أو المواقف الذين تتفاعل معهم على النحو الذي يتظاهرون به أو تبدو عليه.

وبغض النظر عن سرعتك في الكتابة على لوحة المفاتيح أو الهاتف أو الجهاز اللوحي التابلت، فإن أفضل الأدوات المتوفرة لديك لتجنب المخاطر عبر الإنترنت هي استغلال عقلك ووقتك. فيمكنك التوقف والتفكير في المواقف للمساعدة في حماية نفسك وأصدقائك وعائلتك وحساباتك وأجهزتك. وإلا ربما ينتهي بك الأمر إلى المشاركة المفرطة أو التسبب في إحراج نفسك أو الآخرين أو إتلاف جهاز الكمبيوتر الخاص بك أو التحدث مع أشخاص ليست هوياتهم كما يقولون.

شارك بعناية ✓

من الرائع أن تكون لطيفًا ✓

تصدى للابتزاز السيبراني ✓

التواصل الآمن ✓



شارك بعناية

فكر قبل المشاركة

ما تفعله عبر الإنترنت له انعكاس أثره على عالمنا الحقيقي. تؤثر الصور ومقاطع الفيديو والرسائل التي تشاركها عليك وعلى خصوصيتك وعلى سمعتك أنت وهؤلاء الأشخاص حولك، في الوقت الحالي وفي المستقبل. توقف وفكر قبل أن تنشر شيئاً.

من المستحيل أن تتحكم بشكل كامل في الأشخاص الذين يمكنهم رؤية ملفك الشخصي أو صورك أو مقاطع الفيديو الخاصة بك أو النصوص الخاصة بك - حتى إذا استخدمت إعدادات الخصوصية أو التطبيقات التي تحذف محتواك

يمكن أن يكون ما
تنشره "جمهوراً"
أكبر مما تظن.

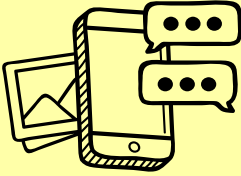
الذي تنشره بعد مشاهدته أو في غضون 24 ساعة. حيث يمكن لأي شخص يرى منشورك ويأخذ لقطة شاشة له أو يسجله. فاسأل نفسك: "هل أريد أن يقف شخص ما في منتصف وقت الغداء وهو يشارك تلك الصورة أو مقطع الفيديو مع كافة الموجودين في الكافيتريا؟"

قد يؤثر ما تشاركه على الآخرين. ربما يكون محرراً وغير عادل، وربما غير آمن إرسال أو نشر صوراً أو مقاطع فيديو دون الحصول على إذن من الأشخاص الموجودين فيها. لذا احصل على موافقة الأشخاص الموجودين فيها أولاً قبل نشرها، واسألهم: "هل أنتم موافقون لو نشرت تلك الصورة أو مقطع الفيديو على وسائل التواصل الاجتماعي؟" وإذا كان ردهم بالرفض، فلا تنشر تلك الصورة أو مقطع الفيديو.

بمجرد أن تنشر شيئًا ما عبر الإنترنت، فلا يمكنك التراجع عن هذه الخطوة

حتى إذا حذفت شيئًا ما قمت بنشره، أو انتهت صلاحية المنشور، يمكن حفظ ومشاركة وبت تلك الصورة أو ذلك التعليق الذي لا تريد لأحد رؤية أي منهما بعد ذلك الوقت في مكان آخر عبر الإنترنت بشكل دائم.

المراسلة الجنسية: لا تفعل ذلك

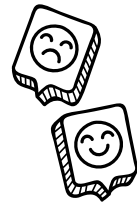


ربما تكون قد سمعت قصصًا في
المدرسة أو في الأخبار عن أشخاص
يقومون "بالمراسلة الجنسية" - أي
إرسال صورًا عاريةً من هواتفهم. فلا

تستجب لذلك. فكّر للحظة. حيث يعرض إنشاء أو إعادة
توجيه أو حتى حفظ صور أو مقاطع فيديو أو رسائل
جنسية صريحة صداقاتك وسمعتك للخطر. والأسوأ من ذلك
أنك قد تنتهك بفعلك هذا القانون.

ملاحظة حول وسائل التواصل الاجتماعي

وفقًا لتوجيهات إدارة الجراحة العامة بالولايات المتحدة،
يمكن أن تسبب وسائل التواصل الاجتماعي أضرارًا جسدية
بحسب مقدار الوقت الذي تقضيه على منصات التواصل
الاجتماعي، ونوع المحتوى الذي تراه على هذه المنصات،
ومدى تأثيرها سلبًا على أمور مثل نومك وممارستك
للتمارين الرياضية، وهي تلك الأنشطة التي تُعتبر ضروريةً لصحتك.





من الرائع أن تكون لطيفاً

دمائة الأخلاق مهمة

عندما لا يمكنك رؤية تعبيرات الوجه أو لغة الجسد أو الإشارات المرئية الأخرى لشخص ما عبر الإنترنت، ربما تشعر بعدم التردد في أن تنشر أو تخبره بأمور لا يمكنك نشرها أو تفصح عنها بشكل شخصي. ولكن يمكن أن يكون لدى إرسال الرسائل النصية والنشر والمراسلة المباشرة ولعب ألعاب الفيديو نفس تأثير التحدث المباشر لشخص ما وجهًا لوجه. فانتبه إلى كيفية التواصل مع شخص ما وفكر قبل أن تتحدث إليه أو تنشر له منشورًا.

تمهّل، فمن السهل أن يحدث لك سوء الفهم عند التواصل عبر الإنترنت. فقبل أن ترسل رسالةً ما، اسأل نفسك: "كيف سيكون تأثير هذه الرسالة على شعور الآخرين؟"

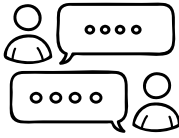
راعي واحترم وجهات نظر ومشاعر الآخرين عبر الإنترنت -

تمامًا كما لو كنت ستتواصل معهم بشكل مباشر. وتذكر:

يوجد أشخاص حقيقيون وراء الصور الرمزية وأسماء الملفات

الشخصية.

خفف من حدة كلماتك. لا تستخدم في كتابتك جميع الحروف الهجائية الكبيرة أو الجمل الطويلة التي تحتوي على علامات التعجب أو الخطوط العريضة ذات الحجم الكبير. لأن تأثيرها يضاوي نفس تأثير الصراخ.



لا تضع كل شيء في الدردشة الجماعية. قبل أن ترسل رسالة جماعية أو تضغط على خيار الرد على الكل، توقف وفكر: من الذي يحتاج إلى رؤية هذه الرسالة؟

لا تنتحل شخصية شخص آخر.

من الخطأ ومن المحتمل أن يكون ضارًا إنشاء ملفات شخصية أو تعليقات أو منشورات تبدو بأنها تخص شخص آخر مثل شخص ما في فصلك أو مدرسك.

اجهر برأيك

إذا رأيت صديقًا ينشر شيئًا طائشًا أو غير آمن عبر الإنترنت، اخبره بذلك. حيث يمكنك إبعاد صديقك عن المشاكل وعن إحراج نفسه. وإذا رأيت شيئًا غير لائق عبر الإنترنت، ابلغ عنه واخبر شخصًا بالغًا تثق فيه بذلك. حيث أن معظم التطبيقات والمنصات لديها طريقة للإبلاغ عما إذا كان سلوك شخص ما يمثل تهديدًا أو غير لائق.





تصدي للابتزاز السيبراني

يستحق كل شخص الشعور بالأمان في تفاعلاته اليومية مع الأشخاص الآخرين، سواء كانوا متواجدين عبر الإنترنت أو وجهًا لوجه.

إذا نشر شخص ما تعليقات مسيئة أو ميمات مؤذية أو صورًا محرجة، أو أرسل دردشات أو رسائل خاصة عنك، فهذا يُعتبر تنمرًا وليس أمرًا مقبولًا. تحدث مع شخص بالغ تثق به لمساعدتك في هذا الموقف وفي اتخاذ قرارًا بشأن الكيفية التي سترد بها.

إذا قام شخص ما بمضايقتك عبر الإنترنت، فإليك ما يجب عليك القيام به:

تجاهل هذا الشخص أو قم بحظره لمنع التواصل معك أكثر نهائياً.



احفظ السجلات واطلب المساعدة من شخص بالغ تثق به.



ابلاغ عن تلك المضايقة. لدى العديد من التطبيقات والمنصات أدوات للإبلاغ عن قيام شخص ما بسلوك غير لائق أو بسلوك تهديد.



غالبًا ما يجعل الابتزاز أو التنمر الشخص الذي يتعرض للمضايقة يشعر بالاستياء - ويجعل المتنمر يبدو شخصًا سيئًا.

يمكن أن يؤدي التنمر والابتزاز أيضًا إلى وقوعك في مشاكل في مدرستك أو مع الشرطة.

إذا كنت شاهدًا على حالة تنمر أو ابتزاز، فابحث عن طرق لتصبح شخصًا مناصرًا - أي شخص يتدخل أو يقاطع أو يجهر برأيه لإيقاف التنمر. فعادةً ما يتوقف السلوك الوضيع بسرعة كبيرة عندما يناصر شخص ما شخصًا يتعرّض للابتزاز.



التواصل الآمن

احمي خصوصيتك

عندما تفعل أي شيء عبر الإنترنت، فإنك تترك أثرًا له. اتخذ هذه الخطوات للتأكد من أن الأثر الذي تركته لفعلك هذا لا يقود إلى معلومات ربما لم تكن تنوي مشاركتها.

استخدام إعدادات الخصوصية. تعرّف على كيفية تشغيل إعدادات الخصوصية للأجهزة والتطبيقات وحسابات التواصل الاجتماعي - ثم استخدمها. وهذا يساعدك على تحديد الأشخاص الذين يمكنهم رؤية موقعك وما تنشره، وعلى تحديد الأشخاص الذين يمكنهم التواصل معك.

تحقق من إعدادات موقعك. تتيح لك بعض التطبيقات رؤية موقع أصدقائك. كما تشارك موقعك معهم. فكّر متى يكون من المنطقي مشاركة موقعك معهم. وعندما لا يكون ذلك منطقيًا، قم بإيقاف تشغيل مشاركة الموقع. وقد تحتوي الميزات الموجودة على أجهزتك مثل الكاميرا

على معلومات عن الموقع الذي كنت متواجداً فيه عندما التقطت صورة ما. فإذا كنت لا ترغب في مشاركة الموقع الذي كنت فيه في كل صورة ذاتية، قم بإيقاف تشغيل مشاركة موقعك أثناء التقاط الصورة بكاميرا هاتفك. واسأل نفسك دائماً: "هل يحتاج هذا التطبيق إلى معرفة موقعي؟"



اقتصر على أصدقائك الواقعيين ليكونوا أنفسهم أصدقاءك عبر الإنترنت. قد يكون التواصل مع الأصدقاء من خلال الرسائل أو وسائل التواصل الاجتماعي أو ألعاب الفيديو أمراً ممتعاً - ولكن لا تكون هوية بعض الأشخاص كما يقولون عبر الإنترنت. وإذا لم تكن حذراً، فرمما تشارك معلومات شخصية مع شخص غريب.

احمي معلوماتك

بمجرد أن تعطي معلوماتك الشخصية - مثل رقم الضمان الاجتماعي الخاص بك أو كلمات المرور الخاصة بك أو معلومات حسابك البنكي - إلى شخص ما، فإنه لا توجد طريقة للتراجع عن هذه الخطوة.

وإليك كيفية حماية معلوماتك عبر الإنترنت:

لا ترد على الرسائل التي تطلب منك إعطاء معلومات شخصية. حتى إذا كانت الرسائل تبدو وكأنها مُرسلة من أحد أصدقائك أو أفراد أسرته أو من إحدى الشركات التي تعرفها - أو كان مفادها أن شيء سيئ سيحدث لك إذا لم ترد عليها. فهناك احتمالات بأنها رسالة مُزيّفة ومُرسله

لسرقة معلوماتك. ابحث عن شخص بالغ تثق به ليساعدك في الإبلاغ عن الرسالة على أنها رسالة غير مرغوب فيها أو رسالة بريد إلكتروني مزعجة.

تحقق من ماهية المعلومات التي يريد تطبيق ما الوصول إليها - قبل أن تقوم بتحميله. تطلب بعض التطبيقات إذنًا للوصول إلى معلومات أو ميزات لا تحتاج إليها مثل قائمة جهات الاتصال الخاصة بك والكاميرا الخاصة بك ومساحة التخزين الخاصة بك وموقعك والميكروفون الخاص بك. اطلب من شخص بالغ تثق به أن يساعدك في قراءة سياسة الخصوصية الخاصة بالتطبيق لمعرفة كيف ستستخدم بياناتك وما إذا كان سيتم مشاركتها أم لا. ثم قرر ما إذا كانت تلك اللعبة القائمة على معرفة اللغة تحتاج حقًا إلى الوصول إلى صورتك أم لا.

تحدث مع شخص بالغ تثق به قبل القيام بعمليات شراء داخل التطبيقات - وخصوصًا إذا كان يدفع ثمن الاشتراك بها.

احمي حساباتك

أنت تحتفظ بالكثير من المعلومات الشخصية في حساباتك عبر الإنترنت. وإليك بعض الخطوات التي يجب عليك اتخاذها لإبعاد الأشخاص الآخرين عن حساباتك.

إنشاء كلمات مرور قوية.

كلمات إزداد عدد حروف كلمة المرور الخاصة بك، إزدادت صعوبة اختراقها. استخدم كلمة مرور مُكوّنة من 12 حرفًا على الأقل عبارة عن مزيج من أحرف هجائية كبيرة وأحرف هجائية صغيرة وأرقام ورموز. وفكر في استخدام عبارة مرور مُكوّنة من كلمات عشوائية لجعل تذكّرها

أكثر سهولةً. ولكن لا تستخدم العبارات أو كلمات الأغاني أو اقتباسات الأفلام السينمائية الشائعة التي يمكن تخمينها بسهولة.

كن فريداً. ابتكر كلمات مرور مختلفة لحساباتك المختلفة.
وبهذه الطريقة، إذا حصل شخص ما على كلمة المرور الخاصة بك لحساب واحد، فإنه لا يمكنه استخدامها للدخول إلى حساباتك الأخرى. وإحدى الطرق المستخدمة للحفاظ على تتبع جميع كلمات المرور المختلفة الخاصة بك هي استخدام أحد تطبيقات مدير كلمات المرور.

حافظ على خصوصية كلمات المرور الخاصة بك. لا تشارك كلمات المرور الخاصة بك مع أي شخص حتى مع أفضل أصدقائك أو شخص ما تواعده

كن انتقائياً بشأن الأسئلة الأمنية. حاول ألا تختار سوى الأسئلة الأمنية

التي يمكنك الإجابة عليها. وتخطى الأسئلة التي لها إجابات يمكن أن يعثر عليها شخص ما عبر الإنترنت - مثل الرمز البريدي الخاص بك أو محل ميلادك أو



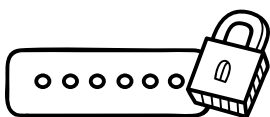
اسم والدتك قبل الزواج. إذا لم تتمكن من تجنب تلك الأسئلة، كن مبتكراً في الإجابة عليها! عاملها وكأنها كلمات مرور واستخدم إجابات عشوائية وطويلة. فقط تأكد من أنك تتذكر إجاباتك.

استخدم المصادقة متعددة العوامل. توفر العديد من الحسابات حماية إضافية لحسابتك باستخدام "المصادقة متعددة العوامل" - التي تتطلب شيئاً آخر بالإضافة إلى مجرد كلمة مرور. وتجمع المصادقة متعددة العوامل

بين شيء تعرفه (مثل كلمة مرور) وشيء لديك (مثل رمز مرور يتم إنشاؤه من خلال أحد التطبيقات) أو شيء يخصك أنت (مثل بصمة الإصبع).

قم بتغيير كلمات المرور بسرعة في حالة تعرضها لاختراق.

إذا أخبرتك إحدى الشركات بحدوث حالة اختراق للبيانات تمكن فيها أحد المتسللين من الحصول على كلمة المرور الخاصة بك، قم بتغيير كلمة المرور التي تستخدمها مع ذلك الحساب على الفور. وقم بتغييرها مع أي حساب يستخدم نفس كلمة المرور أيضًا.



احمي أجهزتك

ما هي أفضل طريقة للتمتع بالبقاء عبر الإنترنت؟ هي التأكد من أن جميع أجهزتك آمنة ومأمونة. فابدأ من هنا:

اضبط إعدادات برنامج الأمان الخاص بك على التحديث التلقائي

لجميع أجهزتك ومتصفحات الإنترنت الخاصة بك وبرنامج التشغيل الخاص بك. وهذا يساعدك على حمايتها من التهديدات الأمنية الجديدة.

لا تنقر فوق روابط أو تفتح مرفقات. إذا تلقيت رسالة نصية أو رسالة بريد إلكتروني أو رسالة عبر الإنترنت غير متوقعة تخبرك بأن تنقر فوق رابط أو بأن تفتح أحد المرفقات، فلا تفعل ذلك! حتى لو كان عرضًا للحصول على شيء مجاني. فرمًا تخفي الروابط والمرفقات فيروسات أو برامج تجسس يمكنها أن تتسبب في إتلاف هاتفك أو جهاز الكمبيوتر الخاص بك أو الجهاز اللوحي الخاص بك.

احمي أجهزتك بكلمة مرور. سيساعدك ذلك في الحفاظ على
منع وقوع صورك ورسائلك وحساباتك في الأيدي الخطأ.

احتفظ بأجهزتك في مكان آمن. سواء كان الجهاز هاتفك أو جهاز الكمبيوتر المحمول الخاص بك أو الجهاز اللوحي الخاص بك. لا تتركه في مكان عام - حتى لو كان ذلك لمدة دقيقة واحدة.



يمكنك معرفة المزيد
من خلال هذا الموقع

This booklet helps kids socialize safely online.
There's help on how to share with care, be
kind online, stand up to cyberbullying, and
protect their personal information Get free
copies in English or Spanish at

ftc.gov/bulkorder



**FEDERAL TRADE
COMMISSION**

أغسطس 2023