وزارة التربية والتعليم

6

أمن وحماية المعلومات

كتاب الطالب

الصف السادس الابتدائي

نحو ثقافة إلكترونية آمنة

هيئة تنظيم الإتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

aeCERT Computer Emergency Response Team

تمهيد

الإنترنت .. عالم واسع .. شبكة عملاقة .. تلف الكرة الارضية شمالا وجنوبا ، شرقا وغربا.. دخول شبكة الإنترنت أشبه بالجولة في مملكة معظم الموجودين فيها سواحٌ ومسافرون من جميع بقاع العالم، والكل يتجول ويتنقل بحرية تامة دون هويات أو تأشيراتٍ للزيارة، حيث لا حدود ولا مراكز جمركية ولا فواصل طبيعية ، والتنقل والتجول فيها ممتعٌ جدا وشيقٌ وهو لا يعدو أكثر من نبضات الكترونية تربط أطراف ومعالم هذه المملكة العامرة..ودخول الشبكة (المملكة) يمثل مغامرة مثيرة للوهلة الأولى، ورغبة شديدة في التعرف على كل شيء والإطلاع عليه ..

هذا الإتساع المترامي لشبكة الإنترنت، صاحبه بروز ظواهر سلبية بين مرتادي الشبكة، وظهور جوانب تستلزم منا أخذ الحيطة والحذر من بعض التهديدات والمخاطر، ولذلك لحماية أنفسنا من التأثيرات المجهولة عبر هذا العالم الإلكتروني الهائل.

قد تكون البداية مجهولة ومشوشة .. ولكن سرعان ما تبدو جميع الأمور طبيعية ومنتظمة، حين إتباع الإرشادات والتعليمات التي ستأخذك لبر الأمان.

هذا المنهج يمثل أحد المصادر الهامة للتوعية بأمن وحماية المعلومات، وهو مادة مساندة للتعريف بكيفية الحد من المخاطر والإستفادة من فرص الإنترنت. كما يهدف إلى تعزيز قدرات وتغيير سلوك الطلاب في التعامل مع الإنترنت. يسعى هذا المنهج في نهاية المطاف الى نشر ثقافة إلكترونية آمنة عبر المؤسسات التربوية والتعليمية بالدولة.

والله ولي التوفيق ،

المقدمة

اصبح التعامل بأمان مع شبكة الإنترنت تحدياً قوياً في زماننا هذا. فشبكة الإنترنت مثل البحر الواسع الملئ بالمعلومات التي تأخذ أشكالا مختلفة مثل الملفات والوثائق وملفات الصوت والفيديو. وهذا الكم الهائل من المعلومات يزيد من خطورة كونها مدمرة أو مضرة أو مضللة. ومن المهم أن نحمي أنفسنا من أي شئ مشبوه في شبكة الإنترنت لأنها لا تقتصر فقط على المعلومات. فشبكة الإنترنت تحتوي أيضاً على أدوات أخرى مثل شبكات التواصل الاجتماعي التي أثرت في حياتنا بشكل أو بآخر، وجعلت من هذا العالم الكبير قرية صغيرة، ثم تأتي بعد ذلك برامج المراسلة الفورية التي لم تعد تتيح للهاتف التقليدي فرصا كثيرة للإستخدام.

يتضمن هذا الكتاب معلومات وتدريبات كثيرة، والتي ستمكنك من تعلم طرق البقاء بأمان وأنت تتجول فى شبكة الإنترنت. ستناقش الدروس شبكات التواصل الاجتماعي، وبرامج المراسلة الفورية، وأمن الإنترنت بشكل عام. سيزودك كل درس ببعض النصائح عن كيفية إستخدام هذه التقنيات لتستمتع بها بشكل آمن.

نواتج التعلم

أن يتمكن الطالب بنهاية المنهج من :

- تعريف شبكات التواصل الاجتماعي
- معرفة كيف يمكن لشبكات التواصل الاجتماعي أن تكون مفيدة
- إستخدام شبكات التواصل الاجتماعي بشكل آمن
- تعريف برامج المراسلة الفورية وكيفية إستخدامها
- مناقشة طرق إستخدام برامج المراسلة الفورية بأمان
- مناقشة طرق حماية نفسك وكيفية التصرف مع التعدي الإلكتروني على الإنترنت
- مناقشة طرق الأمان عند زيارة مواقع الإنترنت
- تعلم عادات مفيدة لإستخدام الإنترنت.

الدرس الاول	شبكات التواصل الاجتماعي Social Networks

تعريفات

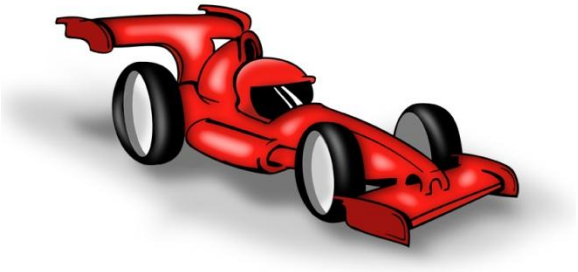
شبكة التواصل الاجتماعي Social Network: مجموعة من الأشخاص الذين يتواصلون ببعضهم على شبكة الانترنت، لهم نفس الإهتمامات أو الأهداف.

الخصوصية Privacy: إبقاء معلومات معينة سراً وعدم مشاركتها أو إخبارها للأخرين.

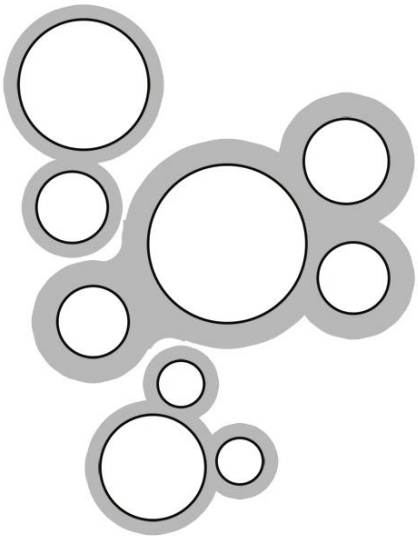
تاريخ شبكات التواصل الاجتماعي

لقد وُجدت شبكات التواصل الاجتماعي لرغبة الناس في التواصل مع بعضهم. شبكات التواصل الاجتماعي هي ببساطة محيط أو بيئة معينة يتمكن الناس من خلالها التفاعل ومشاركة الأفكار ومناقشة الإهتمامات المشتركة والتواصل مع أشخاص آخرين. هناك الآلاف من شبكات التواصل حول العالم، بعضها يتضمن منتديات رياضية، أو مجموعات للعمل الخيري، أومنتديات الهوايات وغيرها، هذه المجموعات تجمع بين الناس ذوي الإهتمامات المشتركة وتعطيهم الفرصة للتعلم وتبادل المعرفة والمشاركة في الأمور التي يستمتعون بها.

قد نلاحظ في الآونة الأخيره وجود هذه المجموعات وانتشارها بكثرة في شبكة الإنترنت. قد تنتمي أنت لبعض تلك المجموعات في شبكة الإنترنت حيث يستطيع الأشخاص الذين لديهم اهتمامات مشتركة الاجتماع معاً والتحدث عن هذه الاهتمامات، ومشاركة الافكار. فقد تكون مثلاً، عضواً في مجموعة خاصة بعشاق كرة القدم حيث يمكنك التحدث عن لاعبيك المفضلين، أو يمكنك أن تكون أحد الأعضاء في مجموعة الفورمولا 1 (Formula 1) لتعرف المزيد عن فريقك المفضل، يمكنك أيضاً أن تنضم لأحدى مجموعات التصوير الفوتوغرافي وتقوم بمشاركة أفكارك حول التصوير الفوتوغرافي مع أناس آخرين حول العالم.



تمتاز شبكات التواصل الاجتماعي في الإنترنت بميزة لم تتوافر في شبكات التواصل الاجتماعي التقليدية وهي أنها تضم أشخاص من مختلف أنحاء العالم. وهذا يعني أنه يمكنك التحدث عن فرق الفورمولا 1 مع شخص ما في أستراليا أو إيطاليا أو كندا، أو يمكنك أن تجد أفكاراً شيقة للتصوير الفوتوغرافي من أحد المصورين المحترفين في الولايات المتحدة الأمريكية، أو من مصوّر مبتدئ في روسيا يطلب مساعدة فنية في المجال نفسه. الآن يمكنك المشاركة بالمعلومات من خلال الشبكات الاجتماعية مع أي شخص حول العالم.



أسئلة:

هناك العديد من شبكات التواصل الاجتماعي الشهيرة في الإنترنت.

- هل أنت عضو في إحدى شبكات التواصل الاجتماعي في مدينتك أو مدرستك؟

- ماهي شبكات التواصل التي تستخدمها في الإنترنت؟

الخصوصية

الجوانب الإيجابية لشبكات التواصل الاجتماعي كثيرة جداً، ولكن لشبكات التواصل الاجتماعي بعض المخاطر التي يجب أن تكون على علم بها قبل إستخدامها، ولعل جانب الخصوصية من الموضوعات الهامة التي يجب التطرق لها حين نتعامل مع شبكات التواصل الاجتماعي في الإنترنت.

لدينا جميعاً معلومات خاصة نريد الإبقاء عليها سراً. صممت شبكات التواصل خصيصاً لنتمكن من مشاركة المعلومات مع الاخرين، ولكن نشر المعلومات الخاصة بك في شبكات التواصل الاجتماعي ليس بفكرة صائبة إذ يجب أن تبقى سرية ولاتنشر، لأن أي شئ تقوم بكتابته أو تنشره في شبكة التواصل سيكون متاحاً للجميع، حين تريد أن تعرض إحدى الصوّر التي قمت بتصويرها، فإن شبكات التواصل هي المكان الأفضل لذلك، بينما هي ليست كذلك لنشر كلمة المرور الخاصة بك أو عنوان منزلك، فالأفضل إبقاء تلك المعلومات سراً.

البيانات أو المعلومات التي يتم نشرها في شبكات التواصل الاجتماعي ستظل هناك لفترة طويلة جداً. قد تقوم بحذف صوّر أو تمسح مشاركات ومحادثات من شبكة التواصل التي تتعامل معها، غير أن العديد من هذه المواقع يقوم بحفظ نسخة منها، وهناك العديد من محركات البحث مثل جوجل Google تقوم بحفظ البيانات لفترة طويلة.

بإمكان أي شخص من الذين اطلعوا على ما قمت بنشره في شبكة التواصل الاجتماعي أن يقوم بحفظه قبل أن تقوم تحذفه، لذلك فإننا ننصحك **ب (فكر جيداً قبل نشر أي شيء في شبكة التواصل الاجتماعي).**

الخصوصية في شبكات التواصل الاجتماعي

الفيسبوك (Facebook) هو احد أمثلة شبكات التواصل الاجتماعي ، وقد تأسس عام 2004 ويعد من أشهر مواقع التواصل الاجتماعي عبر الإنترنت في العالم.

بحسب الإحصائيات فإن عدد مستخدمي الشبكات الاجتماعية يتفوق على عدد مستخدمي البريد الإلكتروني.

ينشر المستخدمون المعلومات والصّور ومقاطع الفيديو في شبكة الفيس بوك، ويقوموا كذلك بالدردشة والمراسلة الفورية مع الأصدقاء وتكوين مجموعات ذات اهتمامات مشتركة، كما يتواصل الناس مع بعضهم من جميع أنحاء العالم، ويتبادلون الأفكار، ويلعبون معاً.

ولكن .. هل تعلم بأنه لا يمكن إنشاء حساب فيسبوك لمن يقل عمره عن 13عاماً !

ما هي الأسباب التي أدت لإدارة شركة الفيسبوك لوضع هذا الشرط؟

عيك أن تقوم بجمع كافة الأسباب التي من شأنها الإبقاء على هذا الشرط الى جانب الأسباب التي تجعل البعض يريدون إلغاء هذا الشرط.

1. إسأل والديك إذا كانا يعتقدان أنه يجب أن يظل هذا الشرط، ولماذا؟
2. أجلس مع والديك وقم بتصفح الإنترنت بحثاً عن أي أخبار تخص هذا الشرط. حاول معرفة الأسباب وراء رغبة بعض الناس بإبقاء هذا الشرط، وأيضا الأسباب وراء رغبة آخرين بإلغاءه.
3. كن مستعداً لعرض أسباب تأييد ومعارضة هذا الشرط أمام زملاءك في الفصل.

نصائح سريعة- حول شبكات التواصل الاجتماعي

من المهم جداً أن تتحكم فيما تقوم به خلال إستخدامك لشبكات التواصل الاجتماعي. يمكنك أن تختار أي معلومات تنشرها وماذا تقول، وماذا تحب أن ترى، أو تقرأ في شبكات التواصل الاجتماعي.

1. تحدث مع والديك قبل إستخدامك لأي من شبكات التواصل الاجتماعي، حيث يمكنهما مساعدتك في إستخدامها بصورة سليمة وآمنة أو توجيهك عند تعرضك لمشكلة ما.
2. اختر شبكات التواصل التي تجد فيها اهتماماتك أو أشخاص من نفس عمرك. استعن بوالديك لمساعدتك على اختيار شبكة التواصل المناسبة لك. استخدم شبكات التواصل للمتعة وكذلك لتعلم الأشياء الجديدة والمفيدة.
3. يجب الحرص على عدم تبادل أو مشاركة المعلومات الخاصة أو السرية في شبكات التواصل الاجتماعي. هناك قاعدة هامة تقول: ما لا تستطيع الإفصاح به أمام معارفك وأصدقائك فلا تقم بنشره في شبكات التواصل الاجتماعي.
4. كن حذراً حين تتحدث وتتبادل المعلومات، فأنت لاتعرف حقاً من بالطرف الآخر وهوية الشخص الذي يقوم بالتحدث معك.

الدرس الثاني	المراسلة الفورية Instant Messaging

تعريفات

برنامج المراسلة الفورية Instant Messaging: برنامج يسمح لك بإرسال رسائل نصية فورية إلى شخص آخر عبر شبكة الإنترنت أو عن طريق شبكات الهواتف المحمولة.

البرامج الخبيثة Malware: البرامج التي تتسلل لجهاز الحاسب الآلي الخاص بك دون علمك. معظم البرامج الخبيثة مصممة بغرض تخريب جهازك أو سرقة المعلومات والملفات أو مهاجمة أجهزة الحاسبات الأخرى.

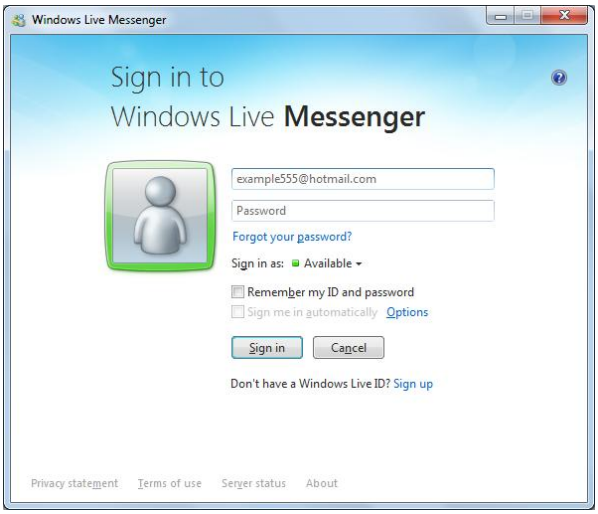
مُختَصِر الروابط – URL Shortener: خدمة على الأنترنت تستخدم لاختصار عناوين المواقع الإلكترونية، وتستخدم عادة حين يكون لديك عدد محدد من الحروف لإرسال رسالة للآخرين، أو بغرض إخفاء العنوان الحقيقي للموقع المرسل إليك. وعليه يجب ان تحترس من الضغط على روابطها ان كان المرسل مجهولاً .

ما هي المراسلة الفورية؟

برامج المراسلة الفورية (IM) هي برامج تسمح لك بالتواصل الفوري مع آخرين عن طريق كتابة رسائل نصية قصيرة لهم، كما أن بعض برامج المراسلة تسمح بإرسال صور أو مقاطع الفيديو. إن برامج المراسلة مريحة للغاية لأنها تسمح بإرسال رسائل فورية لشخص آخر ويمكنه الرد حين الإستطاعة أو إذا أتيح له الإتصال بالإنترنت، كما أنها أيضا مناسبة لأنه يمكن إستخدامها من خلال أجهزة الحاسب الآلي والهواتف النقالة وغيرها من الأجهزة الذكية.

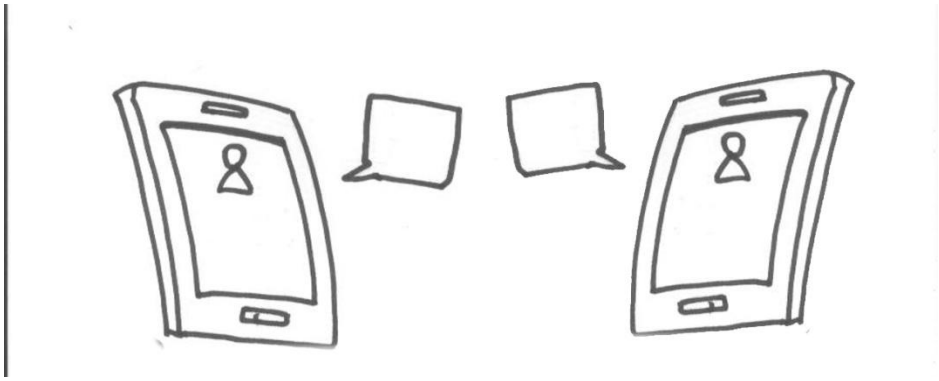
ظهرت على مر السنين أنواع مختلفة من برامج المراسلة الفورية، ومن أشهرها :

- AOL Instant Messenger
- Microsoft Messenger or Windows Live Messenger
- ICQ
- Google Chat
- Yahoo Messenger
- Facebook Messaging
- Whats App
- iMessage
- Skype
- Blackberry Messenger



ما هو برنامج المراسلة الفورية الذي تستخدمه؟ ولماذا إخترته ؟

برامج المراسلة الفورية تتيح لك فرصة إرسال الرسائل إلى أصدقائك البعيدين أو القريبين، بالإضافة إلى توفير إمكانية التحدث مع بعضكم البعض دون إزعاج الآخرين. مثلاً، أثناء التواجد في المكتبات العامة أو عند وجود أناس يتحدثون، إلى جانب إرسال الرسائل التي يمكن أن يرد عليها الطرف الآخر متى ما تمكن من ذلك. تحظى برامج المراسلة الفورية بشعبية كبيرة خصوصاً تلك الموجودة على الهواتف الذكية الحديثة، لأنها سهلة الإستخدام وقادرة على إرسال رسالة لأي شخص في أي وقت حتى وإن لم يكن الهاتف أو جهاز الحاسب الآلي معه.



انتقال الرسالة

يقسم المعلم طلاب الفصل لأربع مجموعات بحيث تتكوّن كل مجموعة من خمسة طلاب. يقوم كل طالب باختيار رقم مختلف عن زميله ابتداءً من الرقم 1 وتكون أرقام متسلسلة – مثل 1، 2، 3....وهكذا. يقف الطلاب بجانب بعضهم حسب تسلسل أرقامهم ابتداءً بالرقم 1. ويُعطى آخر طالب في كل مجموعة ورقة وقلم. يقوم المعلم بإعطاء الطالب رقم 1 من كل فريق ورقة صغيرة بها رسالة قصيرة من جملتين.

1. يهمس الطالب الأول بمحتوى الرسالة في أذن زميله رقم 2 الذي يليه وبسرعة ولكن ينبغي أن يحتفظ بالورقة التي معه.
2. يقوم الطالب رقم 2 بتكرار العملية مع زميله رقم 3 وهكذا، إلى أن تصل الرسالة إلى آخر طالب في المجموعة.
3. يقوم الطالب الأخير الذي يحمل الورقة والقلم بكتابة الرسالة التي وصلته ثم يقوم الطلاب بمقارنتها بورقة الرسالة الاولى
4. على الطلاب مقارنة الرسالتين وأن يحاولوا معرفة متى تغير محتوى الرسالة التي كانوا يتناقلونها من واحد لآخر.

أسئلة

1. ماهي المشاكل التي واجهها الطلاب عند تمرير الرسالة من حيث سماعها ونقلها بوضوح وتذكرها؟
2. هل كان من الأسهل أن يسمح المعلم بتمرير الورقة التي أعطاها للطالب رقم 1؟
3. ماهي المشاكل التي من المحتمل أن تواجهها أثناء مشاركتك الرسائل مع الآخرين من حيث سماعها أو نقلها بوضوح أو تذكرها أو أن يكون قد سمعها آخرون؟

كما رأينا في نشاط انتقال الرسالة، فأنه من الصعب نقل المعلومات بسرعة ودقة. وعندما نسمع رسالة ثم نكررها، فإننا غالباً لا نتذكر كل كلماتها بالضبط. على العقل أن يقوم بمعالجة المعلومات فيصبح من الأسهل تغيير كلمة أو كلمتين لتنتقل الرسالة وتصل بشكل أسرع.

إن برامج المراسلة الفورية هي إحدى الطرق التي تتغلب على تلك المشاكل لأنه من الأسهل كتابة النص أو المعلومة التي تريد إرسالها بطريقة مبسطة ومرتبه، ومن ثم فإن مستلم الرسالة يمكنه أن يعيد إرسال الرسالة لشخص آخر كما هي، ومع ذلك فأن برامج الدردشة وبرامج المراسلة الفورية لا تستطيع إظهار أي عواطف أو أحاسيس مثل الغضب والضحك والفرح والحزن، الأمر الذي قد يجعل المستلم لا يفهم الرسالة بشكل صحيح.

الإستخدام الآمن لبرامج المراسلة الفورية

تعلمنا فيما سبق كيف تكون برامج المراسلة الفورية مفيدة ويمكن الإستمتاع بها، فتتاح لنا فرصة التواصل مع أقاربنا وأصدقائنا الذين يعيشون بعيداً عنا. يمكننا مشاركتهم كل اللحظات الجميلة في نفس الوقت بإستخدام المراسلة الفورية بالفيديو ويمكن أيضاً إرسال واستقبال صوّر المناسبات السعيدة والخاصة. ولكن كغيرها من وسائل التواصل في شبكة الإنترنت، هناك بعض المخاطر التي يجب تعلم بها والتي من شأنها الحفاظ على بقائك آمناً.

الخصوصية

كما في شبكات التواصل الاجتماعي، فإنه يجب عليك أن تكون حذراَ عند إرسال الرسائل عبر برنامج المراسلة الفورية. قد يكون لديك محادثات مع أشخاص من عائلتك و تريد أن تبقيها سريه نظراً لخصوصيتها. بعض برامج المراسلة الفورية تحتفظ بمحادثاتك السابقة مع الآخرين فقد تحتاج أن ترجع إليها في وقت لاحق ولكن للأسف ذلك يعني أنه يمكن لأي شخص أن يقرأ تلك المحادثات لطالما كان من المسموح له إستخدام جهازك، لذا ينصح دائماً بعدم حفظ المحادثات..

الإلتهـــــاء

إستخدام برامج المراسلة الفورية شئ ممتع جداً، والإفراط في إستخدامها قد يلهينا عن معرفة مايجري حولنا، فقد لاتسمع والديك وهما ينادونك لتناول العشاء أو عدم الإنتباه أثناء عبور شارع مزدحم بالسيارات

عند إستخدامك لبرامج المراسلة الفورية، يجب أن تكون حذراً ومنتبهاً لمن حولك، فإذا كنت تقود دراجتك أو تسير على الطريق وأردت أن تقرأ رساله أو ترد على رسالة ما، فيجب أن تقف في مكان مناسب للقيام بالقراءة أو الرد. تجنب أيضاً الإلتهاء في الاوقات التي تتطلب التركيز.

معنى التواصل

تعتبر برامج المراسلة الفورية مفيدة جداً لإرسال الرسائل بمحتواها الأصلي دون تغيير، ولكن لايمكن التعبير عن العواطف أو المشاعر أو إرسال تعابيير وجوهنا من خلال الكلمات. عندما نتحدث وجهاً لوجه مع الآخرين يمكننا أن نرى تعبيرات الوجه ولغة أجسادهم، الأمر الذي يجعلنا نستنتج بسهولة ما إذا كانوا يشعرون بالسعادة أو الحزن، وبالرضا أو الغضب حيث يمكننا أن نغيّر ما نقول أو كيفية الحديث مستعينين بهذه التعابير. على عكس ما يوجد في برامج المراسلة الفورية التي لا تتيح هذا الشيء مما يجعل معرفة مشاعر الآخرين صعباً في بعض الأحيان.

تذكر أن تسأل عن مشاعر الطرف الآخر عند إستخدامك لبرنامج المراسلة الفورية، ما إذا كان مازحاً أو غاضباً، وإذا أردت محادثة شخص ما حول موضوع هام، فإنه من الأفضل القيام بالمحادثة وجهاً لوجه.

الضيوف أو المتعدّين غير المرغوب بهم

قد تتلقى دعوة من شخص ما عبر إحدى برامج المراسلة الفورية للمحادثة أو تبادل المعلومات رغم أنك لا تعرف حقيقة ذلك الشخص. من حيث المبدأ، من الأفضل تجنب الحديث مع أي شخص لا تعرفه، وكن حذراً بشأن المعلومات التي تتناقلها عبر برامج المراسلة الفورية، وإذا وجه لك أي شخص أسئلة غير ملائمة أو غريبة أو تجعلك تشعر بالحرج، فلا تجيب عليها واقطع الاتصال فوراً، كما ينبغي إخبار ولي أمرك بالموضوع.

قد تكون في بعض الحالات جزءاً من محادثة على برنامج المراسلة الفورية مع مجموعة من أصدقائك المقربين وأصدقاء آخرين لست على علاقة قوية معهم، ولشدة تركيزك في المحادثة قد تنسى تواجد الآخرين معك في هذه المحادثة الجماعية لذلك انتبه لما تكتب في المحادثات على برامج المراسلة الفورية. تأكد دائماً مما تكتب واحرص أن يكون الطرف الآخر قد فهم ما تقصد.

إذا تلقيت رسائل من شخص في لعبة من ألعاب الإنترنت، فإننا ننصحك أن تكون أكثر اهتماماً بالحديث معه عن اللعبة بدلاً من تفكيرك فيما إن كان هذا الشخص صادقا فيما يدعيه عن نفسه، وقد يؤدي إلى خداعك عندما يتبين لك أن الشخص الذي تتحدث معه غير مايدعيه ويظهره بالمحادثة.

من جانب آخر فقد تُستخدم برامج المراسلة الفورية لأغراض سيئة كإرسال الرسائل المزعجة أو التعدي، وقد تكون رسائل تهديد وإبتزاز. عليك أن تعلم أن مثل تلك الرسائل قد تشكل تهديداً خطيراً وعليك إخبار ولي أمرك فورا بشأنها وسنناقش لاحقاً كيفية التعامل مع هذه المشاكل.

الروابط والملفات الخبيثة

تمكنك بعض برامج المراسلة الفورية من إرسال الملفات وأفلام الفيديو للآخرين. إذا تم إرسال أي ملفات إليك، فكن حذراً عند قبول تثبيتها في جهازك، وإن لم تعرف مرسل تلك الملفات فالأفضل أن تتجاهلها لأنها قد تحتوي على برامج خبيثة من شأنها أحداث ضرر بالغ بجهازك وملفاتك المخزنة. في بعض الأحيان قد لا يكون المُرسل على علم بأن تلك الملفات تحتوي على شفرات ضارة، خاصةً إذا كان نوع الجهاز المُرسل مختلف عن جهازك، فإنه من المحتمل ألا تضر هذه الملفات جهازه بينما يحدث العكس مع جهازك.

وفي أحيانٍ أخرى قد تتلقى من صديقك رسالة بها وصلة لموقع في الإنترنت وينصحك أن تزوره، أو أن تتلقى رسالة من شخص غريب ينصحك بزيارة موقع يوجد به قسائم تخفيض لأحد محلات الملابس المشهورة وتود حقاً مشاهدتها. مجمل الأمر أنه يجب عليك أن تتحقق من الوصلة قبل الضغط عليها.

معظم الوصلات لها الشكل العادي الذي نعرفه. فعلى سبيل المثال، إذا نظرنا لعنوان هذا الموقع

http://www.aecert.ae/download-ar.php

فإن هذا العنوان من المرجح أن يأخذك لموقع aeCERT، ومن الواضح أن هذا الجزء "download-ar.php " سيأخذك لمكان ما في الموقع حيث يمكنك تنزيل ملفات معينة. العنوان الكامل يتيح لنا التحقق الأولي من سلامة الموقع وإمكانية الوثوق به، ولكن في الجانب الآخر، فإن بعض تقنيات التواصل مثل تويتر Twitter تعتمد على عنوان التراسل المختصر، فإذا قمت بوضع وصلة لموقع في مثل هذه الأنظمة، فإنه يتم إختصارها لوصلة قصيرة، توفيراً لعدد حروف الرسالة، مما يجعل من الصعب التعرف على الوصلة أو معرفة ما تشير إليها. فإذا أخذنا رابط موقع aeCERT وكتبناه في برنامج مختصر الوصلات، فإنه سيبدو هكذا

http://bit.ly/PbzpuC

لن تتمكن أبداً من معرفة ما إذا كانت الوصلة لموقع رسمي أو لموقع يحتوي على فيروسات أو خطر آخر قد يشكل تهديداً على جهازك.

يُنصح بعدم الضغط على أي وصلات قصيرة مرسلة إليك، وقم بالتحقق من عنوان الموقع قبل الضغط على الوصلة وتأكد أنه موقع آمن. إحذر أن تضغط على أية وصلات مرسلة إليك من شخص لا تعرفه، وإذا شعرت أن الموقع الذي أُرسل لك حقيقي فلا تضغط عليه مباشرة ولكن من الأفضل أن تكتبه بسطر العنوان في متصفح الإنترنت .

نصائح سريعة- حول برامج المراسلة الفورية

من المهم أثناء إستخدام برامج المراسلة الفورية أن تكون على وعي تام بما تختار ومتى تتحدث ومع أي شخص وماذا تقول وكيف تجيب الآخرين وماذا تفعل بشأن الوصلات والمرفقات.

1. لا تنسى أن تنتبه لما هو حولك أثناء إستخدامك برنامج المراسلة الفورية حتى لا تقع أي مشكلة سببها فقدان التركيز.
2. احرص على عدم تبادل المعلومات الخاصة أو السرية من خلال برامج المراسلة الفورية لأنك تجهل ماذا يمكن للطرف الآخر أن يفعل بتلك المعلومات.
3. كن حذراً بشأن مع من تتحدث أو تتبادل المعلومات معه لأنك لا تعرف الهوية الحقيقية للشخص الذي يحدثك في الطرف الآخر.
4. كن شديد الحذر أثناء التعامل مع أي ملفات يتم إرسالها لك عبر برامج المراسلة الفورية.
5. قم بالتحقق من أية وصلة أو عنوان موقع يرسل إليك قبل الضغط عليه لاسيما العناوين القصيرة

الدرس الثالث	كيف تتعامل مع التعدّي الإلكتروني؟

تعريفات :

التعدّي الإلكتروني Cyber-Bullying: هو إستخدام الإنترنت للتهديد أو الإساءة أو مضايقة الآخرين عبر شبكات التواصل الاجتماعي أو البريد الإلكتروني أو برامج المراسلة الفورية أو أي وسيلة أخرى.

ماهو التعدي الإلكتروني؟

لقد تعلمنا من الدروس السابقة كيف يتواصل الناس إجتماعياً في شبكة الإنترنت من خلال ما يعرف "بشبكات التواصل الاجتماعي". هذه الشبكات تقرب العائلات والأصدقاء من بعضهم خصوصاً إن كانوا في مناطق بعيدة مختلفة، كما تمكّن الناس من التحدث وتبادل المعلومات والصوّر والأخبار والأفكار في نفس الوقت.

غير أن هناك قلة من الناس يستخدمونها لإحراج ومضايقة الآخرين، وهناك بعض الحالات والقصص لأطفال وشباب عاشوا أوقاتاً صعبة وحالات نفسية سيئة، بل وصل البعض لمراحل متقدمة من اليأس والتفكير بالانتحار نتيجة لتعرضهم لهذا النوع من التعدي.

يحدث التعدي الإلكتروني عند إرسال رسائل أو صوّر سيئة للآخرين، أو أن يتم نشرها في شبكات التواصل الاجتماعي بغرض مضايقة شخص ما. بعض أولئك المتعدّين يستخدمون أسماء وحسابات وهمية أو مزيفة لاعتقادهم بأنه بتلك الطريقة لن يتم كشفهم أو تعقبهم.

يظن ضحية التعدي الإلكتروني أنه لا مفر من هذا النوع من التعدي لأن شبكة الإنترنت تبدو مكاناً كبيراً وواسعاً، فقد يقرأ آخرون الرسالة التي قام بنشرها المتعدي ويصدقوها ويعيدوا إرسالها لآخرين وهكذا، ومن ثم يشاركون التعدي نفسه.

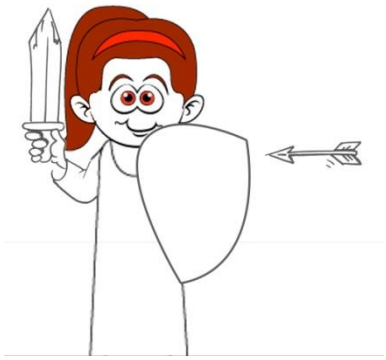
من المهم التعرف على بعض الأمور الهامة حول كيفية تجنب التعدي الإلكتروني أو كيفية التصرف تجاهه.

كيف تتجنب التعدي الإلكتروني

- لا تتحدث أو ترسل رسائل أو تتواصل إلا مع من تعرفهم وتجنب الغرباء ولا ترد على أية رسائل فيها تهديد أو تخويف أو ذات محتوى غير ملائم.
- تحدث مع ولي أمرك عن كيفية إستخدامك للانترنت إذ يمكنهما توجيهك للإستخدام الأفضل عبر مجموعة قواعد وتوجيهات تساعدك في تجنب التعدي الإلكتروني والتركيز على الأمور الهامة.
- كن شخصاً عاقلاً، بمعنى ألّا تقحم نفسك في أي ممارسات للتعدي أو المحادثات السلبية عن آخرين.
- لا تنشر بياناتك الشخصية أو تشارك بمعلومات سرية أو خاصة حتى لا يتم استغلالها ضدك.

كيفية التصرف تجاه التعدي الإلكتروني

- قم فوراً بإبلاغ والديك إذا تعرضت للتعدي الإلكتروني أو قام أحدهم بإرسال رسائل تهديد أو بها محتوى غير ملائم.
- لا تقوم بالرد على رسائل التعدي لأن الرد لن يغير غالباً رأي المتعدي ويجعله يتوقف عنها. إن أولئك المتعدين لا يهمهم إن كان ما ينشرونه صحيح أم لا وهدفهم الأساسي هو إزعاج الآخرين فقط حتى وإن كان ما ينشرونه سيئاً وليس صحيحاً.
- قم بالإحتفاظ بورقة واكتب فيها وقت وتاريخ حدوث حادثة التعدي الإلكتروني، وقم بحفظ وطباعة أي رسائل أو بريد إلكتروني أو أي دليل للتعدي الإلكتروني.
- قم بمنع المتعدّي من الوصول إليك بإستخدام خاصية المنع Block ولا تعيره أي إهتمام أو تسمح له بالاستمرار في مضايقتك.



- لابد لوالديك من الإبلاغ عن حادثة التعدي الإلكتروني فوراً، فإن معظم المدارس والكثير من شركات خدمات الإنترنت وشركات الهواتف المحمولة إلى جانب جهاز الشرطة لديهم الأدوات اللازمة للتعامل مع حالات التعدي الإلكتروني عند تقديم البلاغ وفي حال تواجد الدليل.

عرض تمثيلي

سيقوم المعلم بتقسيم الفصل لمجموعات، وعلى كل مجموعة أن تصمم مشهداً أو مسرحية تعرض موقفاً يتعرض فيه شخص للتعدي الإلكتروني على إحدى شبكات التواصل الاجتماعي وسيقوم باقي أفراد الفريق بمساعدة الضحية.

تكلم في العرض عن الآتي:

1. ماذا فعل المتعدّي لمضايقة الضحية ؟
2. لماذا كان تأثير المتعدّي قوي على الضحية؟
3. ما الأثر الذي يتركه التعدي الإلكتروني على الضحية؟
4. ماذا يجب على الضحية فعله لحل هذه المشكلة؟
5. كيف يمكن للأصدقاء أو أفراد العائلة مساعدة الضحية في الإبلاغ عن التعدي الإلكتروني؟
6. إشرح كيفية إستخدام شبكات التواصل الاجتماعي بأمان لتجنب التعرض للتعدي الإلكتروني.

التواصل الاجتماعي والتعدي الإلكتروني

لقد قمت اليوم في الفصل بتصميم وعرض مشهد قصير عن التعدي الإلكتروني. قم بكتابة ما تعلمته من خلال هذا النشاط عن طريق إجابة الأسئلة التالية.

1. ما هي طريقة التعدي الإلكتروني التي قامت مجموعتك بتأديتها؟

2. لماذا اختارت مجموعتك هذه الطريقة؟

3. ماهو أصعب جزء من المشهد من حيث التحضير؟

4. ما هو الشيء المختلف الذي ستقوم به من الآن فصاعداً عند إستخدامك لشبكات التواصل الاجتماعي؟

سياسة المدرسة تجاه شبكات التواصل الاجتماعي والتعدي الإلكتروني

تعرف على سياسة وقوانين مدرستك تجاه التعدي الإلكتروني وحاول إيجاد وثيقة مطبوعة أو متواجدة في الإنترنت.

1. قم بإيجاد الجزء الذي يذكر التعدّي الإلكتروني في الإنترنت أو عبر إستخدام الشبكات الاجتماعية مثل الرسائل النصية والمحادثات وشبكات التواصل الاجتماعي
2. ما هي الإجراءات التي يجب أن يتخذها الطالب للإبلاغ عن تعرضه للتعدي الإلكتروني حسب سياسة المدرسة؟
3. في بعض الأحيان، يجب توافر دليل قوي ضد التعدي الإلكتروني، غير أن أخذ لقطات بإستخدام الهاتف المحمول قد يكون صعباً بعض الشئ. وضّح خطوة بخطوة كيفية أخذ اللقطات بإستخدام هاتفك المحمول؟

الدرس الرابع	أمن الشبكة

تعريفات

الموقع الإلكتروني Website: هو مكان في الإنترنت لمشاركة المعلومات مع أشخاص آخرين أو أجهزة كمبيوتر أخرى مثل النصوص والصور وملفات الصوت وأفلام الفيديو. ويمكن فتح أي موقع بإستخدام ما يسمى بـ "متصفح الإنترنت"

متصفح الإنترنت Web Browser: هو برنامج يسمح لك بفتح مواقع الإنترنت حيث يوجد به مساحة لعرض موقع أو صفحة في الإنترنت إلى جانب أزرار مساعدة للتنقل بين الصفحات.

نافذة المتصفح المنبثقة – Browser Pop-up window : هي نافذة جديدة من نوافذ متصفح الإنترنت التي تظهر فجأة، تظهر تلك النوافذ أحياناً عندما تزور موقع معين فيُطلب من المتصفح أن يفتح نافذة جديدة.

HTTPS : هي اللغة التي تتواصل بها متصفحات الإنترنت والمواقع الالكترونية بطريقة آمنة بحيث تشفر المعلومات المتبادلة بينهما ولا تكون قابلة للقراءة عند حدوث إختراق ما أثناء عملية تبادل المعلومات.

التحديثات الإلكترونية Patches : هي عبارة عن تحديثات لبرامج الحاسب الآلي. تقوم الشركات التي تطور البرامج بإصدار هذه التحديثات الالكترونية لإصلاح أي مشاكل قد تظهر في البرامج، أو سد ثغرات أمنية تهدد أمن الجهاز ومستخدميه.

مواقع مشاركة الملفات – File Sharing Websites : هي مواقع تتضمن ملفات أفلام ومقاطع صوتيه وبرامج وتطبيقات يمكن تنزيلها من هذه المواقع ولكن عادة ما تكون نسخ هذه الملفات غير مرخصة أي نسخاً غير أصلية مما يزيد احتمالية إحتواءها على فيروسات أو برامج خبيثة.

أمن الشبكة

تمتلئ شبكة الإنترنت بالمواقع الإلكترونية وشبكات التواصل الاجتماعي والبرامج وملايين من الناس الذين يتبادلون الأفكار والمعلومات ويقومون بشراء السلع من مواقع التسوق المختلفة، كما يمكننا أيضاً مشاهدة الأفلام مباشرة في الإنترنت وتبادل ملفات الفيديو واللعب مع آلاف المشتركين الآخرين الذين يبعدون عنا آلاف الأميال. كل تلك الأنشطة يمكننا القيام بها بينما نحن نستمتع بالراحة في المنزل.

صرحت شركة تسمى Netcraft في مارس 2012 أنه يوجد حوالي 644 مليون موقع إلكتروني في شبكة الإنترنت وزاد عدد المواقع بعد مارس 2012 بفارق 31,4 مليون موقع، وهناك العديد من المواضيع الممتعه والمفيدة في شبكة الإنترنت ولكن في المقابل توجد بعض المواقع والأمور ذات المحتوى السيء.

سنناقش في هذا الدرس كيفية حماية نفسك عند زيارة المواقع في شبكة الإنترنت حتى تكون مستمتعاً ولكن بسلامة وأمان.

احمي نفسك في شبكة الإنترنت

كن حذراً عند زيارتك مواقع الإنترنت – قم فقط بزيارة المواقع التي تعرفها وتجنب المواقع التي تحتوي على أمور سيئة أو غير لائقة. إن العديد من تلك المواقع تحتوي أيضاً على برامج خبيثة، وعندما تقوم بزيارتها فإنها تقوم بتثبيت تلك البرامج في متصفح الإنترنت الخاص بك دون علمك وتتسبب في أضرار بالغة بالجهاز.

تجنب الإعلانات والرسائل التي تظهر في نوافذ المتصفح المنبثقة – عند الضغط على هذه النوافذ فإنها تأخذك إلى مواقع إعلانية، أو مواقع خبيثة، حتى أن بعض هذه النوافذ قد تخبرك بأن جهازك مصاب بفيروس ما وقد تحاول أيضا إقناعك بعمل المسح للكشف عن الفيروسات. يتوجب عليك فقط الإعتماد على برنامج مكافحة الفيروسات الخاص بك وإذا صادفتك مثل تلك النوافذ فقم بإغلاقها في الحال.

تسوق فقط عن طريق المواقع الموثوقة و الأكثر تداولاً بين الناس – من الخطأ أن تتسوق في موقع لم تسمع عنه من قبل، فقد تدفع مالاً مقابل ما أشتريت ولكن الأمر خدعة ولن يتم إرسال البضاعة لك أبداً، وعليه فمن المهم أن تتسوّق من المواقع التي تثق بها أو التي قام بإستخدامها أصدقائك أو أي من أفراد عائلتك. تأكد أن موقع التسوق الذي تشتري منه يستخدم نظام HTTPS قبل إدخال بيانات بطاقة الإئتمان أو كلمة المرور أو أي معلومات خاصة.

Photo

لا تستخدم نفس كلمة المرور لحساباتك المختلفة في المواقع – إن السبب الرئيسي لإستخدام كلمة المرور هو منع الآخرين من إستخدام حساباتك الخاصة بمواقع الإنترنت، فهي تحمي حسابك في شبكة التواصل الاجتماعي أوحساب البريد الإلكتروني أو حساب موقع التسوق، حتى لا يستطيع أحد اختراق تلك الحسابات. هناك بعض المواقع التي تفتقر لإجراءات الأمن الصحيحة مما يعرضها للقرصنة وسرقة ما بها من حسابات خاصة بعملائها وقد يكون حسابك واحداً منهم، فإذا كنت تستخدم نفس اسم المستخدم ونفس كلمة المرور لجميع حساباتك الموجودة في مواقع إلكترونية مختلفة، فمن السهل إختراق جميع هذه الحسابات.

لا تنشر بياناتك الشخصية أو معلوماتك الخاصة - المعلومات مثل كلمات المرور ورقم هاتفك وعنوان بيتك ورقم بطاقتك الشخصية وأرقام البطاقات الإئتمانية تعتبرجميعها من المعلومات الخاصة والحساسة ولا يجب نشرها في شبكة الإنترنت. قد تطلب منك بعض المواقع إدخال مثل هذه المعلومات أو قد تظهر لك إحدى النوافذ المنبثقة التي تطلب منك إدخال هذه البيانات، فلا تفعل ذلك أبداً وابقِ معلوماتك الخاصة طي الكتمان.

احرص أن يكون بحاسبك الآلي آخر تحديث – يقوم مطوروا برامج الحاسب الآلي بإصدار بعض الإصلاحات لعيوب ومشاكل أو لسد ثغرات أمنية في برامج الحاسب أو نظام التشغيل وتسمى "بالتحديثات الإلكترونية". قم بضبط جهازك على أن يقوم بتنزيل وتثبيت هذه التحديثات بإستمرار ومتى ما توافرت. استشر والديك ومن تثق به بهذا الخصوص واحرص على تفعيل هذه الخاصية بصورة تلقائية.

تأكد من أن برنامج مكافحة الفيروسات مُفَعَّل في جهازك، فهو يساعد على حماية جهازك من الفيروسات والبرامج الخبيثة التي قد تتواجد في المواقع الإلكترونية. يمكن لبرامج الحماية أن تحذرك من تهديدات المواقع غير الآمنة، لاسيما إذا زرت أياً منها بمحض الصدفة.

تجنب تنزيل البرامج الموجودة للمشاركة في المواقع العامة – هناك الكثير من شركات البرامج التي تسمح بتنزيل برامجها عبر شبكة الإنترنت. كما أن هناك مواقع تعرض تنزيل نسخاً لبرامج غير مرخصة. في بعض الأحيان قد يعرض عليك موقع ما تنزيل برامج بقيمة أقل بكثير من تحميلها من المواقع الأصلية، فكن حذراً عند التعامل مع هذه المواقع فقد تحتوي البرامج الموجودة بها على فيروسات أو يحتوي الموقع نفسه على شفرات خبيثة.

عادة ماتكون تلك النسخ الرخيصة لبرامج غير أصلية أو غير مرخصة أو غير معتمدة من شركات البرامج المطورة، وعليه فقد لاتتمكن من تحديث البرنامج أو الحصول على الدعم إذا واجهتك مشكلة ما أثناء إستخدامه، لذلك من الأفضل تجنُب تلك النسخ من البرامج.

تبادل إستخدام أجهزة الحاسب الآلي

حين تستخدم حاسباً آليا في مكان عام كمقاهي الإنترنت والمكتبات أو من خلال جهاز يخص صديق لك، فإنه ينبغي أن تكون أكثر حذراً، فقد لا يقوم صديقك بحماية جهازه مثل ما تقوم أنت. إن أجهزة الحاسب الآلي المتواجدة في الأماكن العامه مثل مقاهي الإنترنت والمراكز التجارية تستخدم من قبل الكثير من الناس الذين قد لا يكونوا حذرين مثلك عند إستخدامها، الأمر الذي قد يجعلها عرضه للإصابة ببرامج التجسس التي من الممكن أن تحفظ كل ما تكتبه بما في ذلك كلمات المرور.

من الأفضل عدم زيارة المواقع التي تطلب منك كلمة المرور أو أي معلومات خاصة أثناء إستخدامك للأجهزة الموجودة في الأماكن العامة.

من جانب آخر فإن إستخدام الآخرين لجهازك قد يشكل تهديداً أمنيا من جانبين:.

الأول : ليس كل من يستخدم جهازك سيحرص عليه على قدر حرصك أنت، لأنه قد يزور مواقع غير آمنة أو يقوم بتنزيل ملفات مصابة بفيروسات قد تضر بجهازك. إن وجود نسخة محدثة من برنامج مكافحة الفيروسات سيكون مفيداً جداً ولكن لايمكن الإعتماد عليه تماماً. والأهم أن نرتقي بسلوكنا تجاه امن المعلومات ونعرف التصرف الصواب عند إستخدامنا للحاسب الآلي ودخولنا شبكة الإنترنت.

الثاني: قد تكون معظم البرامج الموجودة على جهازك أو تلك المواقع التي عادةً ما تقوم بزيارتها في شبكة الإنترنت مُعدة لتفتح حساباتك الخاصة مباشرة وبشكل تلقائي، مثل بريدك الالكتروني أو حسابك في شبكة التواصل الاجتماعي. فإذا سمحت لأحد بإستخدام جهازك وقام هذا الشخص بفتح نفس الموقع فإنه سيتمكن من رؤية صفحة حسابك أو الأطلاع على رسائل بريدك الالكتروني. ننصحك بتسجيل الخروج عند إنتهائك من العمل أو عند إغلاق حاسبك الشخصي.

كن صاحب مبدأ

إن إستخدام شبكة الإنترنت يتطلب منك الكثير من الحيطة والحذر، لذلك من الضروري ممارسة هذه الأساليب واتخاذها كعادات...

1. أكتب قائمة ببعض الأمور الجديدة التي تعلمتها والتي تنوي أن تتخذها كعادة.
2. أكتب قائمة أخرى بطرق لتذكير نفسك بتطبيق هذه الأمور بانتظام.
3. ضع علامة أو ملصق أو أي أدوات تذكير أخرى حيث يمكن وضعها على مكتبك أو لصقها على جهاز الحاسب الآلي الخاص بك.

نصائح سريعة

1. كن حذراً في إختيار المواقع التي تزورها في شبكة الإنترنت.
2. تجنب الإعلانات أو الرسائل التي تظهر لك من خلال النوافذ المنبثقة بمتصفح الإنترنت.
3. تسوق فقط في المواقع الموثوقة والأكثر تداولا بين الناس.
4. استخدم كلمة مرور مختلفة لكل موقع أو حساب لك في شبكة الإنترنت.
5. لا تنشر أو تشارك أي من المعلومات الخاصة أو الحساسة.
6. احرص على أن يكون تحديث نظام التشغيل وبرنامج مكافحة الفيروسات والبرامج المستخدمة بشكل تلقائي ودوري.
7. لاتقم بتنزيل الملفات من المواقع المشبوهة.
8. لا تقم بإدخال كلمة المرور الخاصة بك عند إستخدامك أجهزة الحاسب الموجودة في الأماكن العامة.

إختبر معلوماتك	

شبكات التواصل الاجتماعي

1. ماهي شبكات التواصل الاجتماعي؟
2. ما الذي يمكن أن تفعله في شبكات التواصل الاجتماعي المتواجدة في شبكة الإنترنت؟
3. إذا طُلِب منك أن تنشر كلمة المرور الخاصة بك في شبكة التواصل الاجتماعي من قِبَل شخص تعرفه. ماذا ستفعل؟ ولماذا؟

برامج المراسلة الفورية

1. ماهي برامج المراسلة الفورية ؟
2. ما هي إستخدامات برامج المراسلة الفورية ؟
3. ماذا ستفعل إن جاءتك رسالة من شخص لا تعرفه؟
4. ماذا ستفعل إن طلب منك أحدهم إرسال كلمة المرور الخاصة بك عبر برنامج المراسلة الفورية ؟ ولماذا؟

أمن الشبكة

1. لما يجب عليك إستخدام كلمة مرور مختلفة لكل موقع؟
2. إذا قمت بإستخدام أجهزة الحاسب الآلي في الأماكن العامة، فأي من مواقع شبكة الإنترنت يمكنك زيارتها وأيها يجب الا تزور؟
3. ماهي التحديثات الإلكترونية؟ ما هي أهمية التأكد من وجود خاصية التحديث التلقائي ؟
4. ماهي النافذة المنبثقة في المتصفح؟ ولماذا يجب تجنبها؟

إختبار عام

اختر الاجابة أو الاجابات الصحيحة من بين البدائل في الاسئلة التالية :

1. ماهي شبكات التواصل الاجتماعي؟ اختر الإجابة الصحيحة.
   أ. هو موقع أو مكان يجتمع به الناس للتواصل بشأن الإهتمامات المشتركة
   ب. تكنولوجيا تواصل الأقمار الصناعية في الفضاء الخارجي
   ج. اختراع جديد لم يسبق أن وجد من قبل
2. ما هي المعلومات التي لا يجب تناقلها عبر شبكة التواصل الاجتماعي؟ اختر جميع الإجابات الصحيحة.
   أ. كلمات المرور
   ب. البيانات الشخصية
   ج. المعلومات الخاصة
   د. أي شئ لا يمكنك الإفصاح عنه أمام الناس في العلن
3. ماذا يعني مصطلح IM؟
4. ما الذي يجب الحذر منه أثناء إستخدام المراسلة الفورية؟ اختر جميع الإجابات الصحيحة.
   أ. كن يقظاً في المواقف التي تتطلب منك الانتباه ولا تدع أي شئ يتسبب في فقدان تركيزك
   ب. لا تقم بنشر البيانات الشخصية أو المعلومات الخاصة عند إستخدام المراسلة الفورية
   ج. أبلغ عن المتعدين عند إستلامك أية رسائل ذات محتوى غير ملائم
   د. افتح روابط المواقع التي يرسلها لك من لا تعرفه
   ه. قم دائماً بفتح الروابط القصيرة
5. إذا جاءتك رسالة غير مهذبة عبر المراسلة الفورية. ماذا يجب عليك أن تفعل؟ اختر جميع الإجابات الصحيحة.
   أ. قم بالرد على الرسالة
   ب. أجب عن أي أسئلة يرسلها لك أي شخص مجهول
   ج. احذف أو امنع الشخص المجهول
   د. أخبر والديك بشأن الرسالة

6. ما هي الطرق التي يمكن بها حماية نفسك أثناء زيارة المواقع الإلكترونية؟ اختر جميع الإجابات الصحيحة.
   أ. قم بزيارة المواقع الآمنة فقط
   ب. تجنب المواقع ذات المحتوى غير الملائم
   ج. تجنب الإعلانات التي تظهر في النوافذ المنبثقة
   د. تسوق من المواقع التي تعرفها جيداً أو التي تعرف لها السمعة الطيبة
   ه. استخدم نفس كلمة المرور لكل المواقع
   و. قم بتنزيل البرامج الموجودة على مواقع مشاركة الملفات
7. ما هي التحديثات الإلكترونية ؟
   أ. ما تلبسه لتحمي عينيك
   ب. ما تقوم بإستخدامه لإصلاح القطع التالفة
   ج. إصلاحات للتطبيقات وبرامج الحاسب الآلي
8. ما الذي يجب أن تحذره أثناء إستخدام أجهزة الحاسب الآلي المتواجدة في الأماكن العامة؟ اختر جميع الإجابات الصحيحة.
   أ. لا داعي للحذر
   ب. يمكن أن تحتوي على البرامج الخبيثة
   ج. لا تعرف إن كان الجهاز آمناً ويحتوي على برنامج مكافحة الفيروسات
9. اشرح بأسلوبك الحماية وأهميتها.