وزارة التربية والتعليم

11

أمن وحماية المعلومات

كتاب الطالب

الصف الحادي عشر

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

يحتوي هذا الكتاب على العديد من المعلومات والتدريبات حول الموضوعات المتعلقة بأمن المعلومات وأهم طرق التواصل التي تستخدمها. وستناقش الدروس فوائد المراسلة الفورية وشبكات التواصل الاجتماعي ومخاطرها وكيفية حماية أنفسنا. وستشمل الدروس البرامج الخبيثة المتقدمة أو الحديثة إلى جانب تهديدات أخرى على شبكة الإنترنت. كما تهدف هذه الدروس الى مساعدتك في فهم كيفية حماية نفسك من هذه المخاطر أو التهديدات لتستمتع باستخدام الإنترنت والمراسلة الفورية ووسائل التواصل الإجتماعي.

المخرجات

يهدف هذا الكتاب الى تناول النقاط الآتية :

- رفع مستوى الوعي بشأن بعض المخاطر المرتبطة بالمراسلة الفورية.
- مناقشة فوائد ومخاطر استخدام قنوات وشبكات التواصل الإجتماعي.
- التعرف على البرامج الخبيثة المتطورة – بوتنت "Botnets".
- زيادة التوعية الوعي بتأثير التهديدات على شبكة الإنترنت.

جدول المحتويات

الدرس الاول	المراسلة الفورية على الهواتف الجوالة

تعريفات

المراسلة الفورية Instant Messaging (IM): برنامج يتيح لك إرسال رسائل فورية لشخص آخر من خلال الشبكات المختلفة، مثل شبكة الإنترنت أو شبكات الهواتف الجوالة.

التعبيرات Emoticon: مجموعة من الرموز المقصود بها اظهار تعبيرات الوجه أو توضيح إحساس أو مشاعر أو سلوك.

التعدّي الإلكتروني Cyber-Bullying: هو استخدام الإنترنت أو الهواتف الجوالة أو أي تقنية أخرى ، للتهديد أو الإساءة أو مضايقة الآخرين عبر شبكات التواصل الإجتماعي أو البريد الإلكتروني أو المراسلة الفورية أو أي وسيلة أخرى لتخويف أو إذلال أي شخص...

المراسلة الفورية على الهواتف النقالة

أصبحت برامج المراسلة الفورية متوفرة في مختلف أنواع الأجهزة الجوالة من هواتف نقالة وأجهزة لوحية صغيرة والحاسب المحمول والحاسب المكتبي .

تستخدم المراسلة الفورية لأغراض جيدة وأسباب عديدة :

التواجد في الأماكن التي بها ضوضاء - سيكون من الصعب إجراء مكالمة هاتفية أثناء التواجد في أماكن بها الكثير من الضوضاء كمباراة كرة القدم مثلا. إذا كنت متواجداً في مكان مزدحم وملئ بالضوضاء أو موقع للبناء مثلا، فإن الضوضاء لن تمكنك من محادثة أحدهم بواسطة الهاتف النقال. لذلك فإن المراسلة الفورية هي الحل الأنسب في مثل هذه الظروف.

إرسال وإستقبال معلومات لإستخدامها في وقت لاحق – في بعض الأحيان تحتاج إلى ارسال أو استقبال معلومة صغيرة مثل رقم هاتف، أو عنوان بريد إلكتروني، ومن أجل الحصول عليه بدقة فإنه من الأسهل إستخدام المراسلة الفورية. هناك بعض برامج المراسلة الفورية التي تخزن الرسائل المتبادلة لدى كل مستخدم فيسهل الرجوع إليها في أي وقت.

من أجل الخصوصية – الأشخاص الذين يريدون القيام بمناقشات أو محادثات ولكن في نطاق سري.

امكانية الرد لاحقاً – مع استخدام المراسلة الفورية يمكنك أن تتوقف عن المحادثة ثم الرجوع إليها في وقت لاحق. إذا اعترضك أحدهم في وقت محادثتك بالمراسلة الفورية، فيمكنك التوقف لبضع دقائق حتى ينصرف، وترجع مرة أخرى للمحادثة.

المراسلة الفورية شئ مفيد ويمكن الاستمتاع بها ولكنك يجب أن تعلم أنه من الصعب الإنتباه لأمور عدة في نفس الوقت. وهناك تجارب ممتعة توضح لنا ذلك.

Activity	**تجارب على المراسلة الفورية**

العدد الصادر في ديسمبر من جريدة علم النفس التطبيقي وكذلك العدد الصادر في صيف 2006 من مجلة العناصر البشرية وجمعية بيئة العمل، يحتوي على دراسة عن آثار استخدام الهاتف النقال أثناء انجاز مهام أخرى. وفي كلتا الدراستين وجد أن الأشخاص الذين يستخدمون الهاتف أثناء أداء أعمال أخرى، تقل قدرتهم على انجاز الاشياء البسيطة عكس الأشخاص الذين لا يستخدمون الهاتف وقت أداء أعمالهم. ووجد الباحثون في الدراسة الأولى أن الأشخاص الذين يستخدمون الهواتف المحمولة أكثر عرضة لضياع لحظات نادرة وسريعة، في حين أثبتت الدراسة الثانية أن إستخدام الهاتف النقال أثناء القيادة يؤثر على أداء سائق السيارة تماماً كتأثير المخدرات. فالذين يستخدمون الهاتف أثناء القيادة تقل استجابتهم لسرعة استخدام المكابح ويعجزون عن تقدير المسافات بينهم وبين السيارات الأخرى ويصبحون أبطأ عند مواصلة السير بعد الضغط على المكابح .

هذه الظاهرة تسمى "Inactive Blindness". ادرس هذه التجارب وقم بمناقشة الأسئلة الآتية مع زملائك في الصف .

1. في اعتقادك، لماذا يتشتت انتباه الأشخاص الذين يستخدمون الهاتف النقال ؟

2. هل لاحظت هذه الظاهرة بنفسك؟ صف تجربتك.

3. ما هي المواقف التي قد تكون خطرة بسبب عدم الإنتباه نتيجة استخدام الهاتف النقال؟

مخاطر استخدام المراسلة الفورية على الأجهزة المحمولة

مثلما لاحظنا فإن هناك بعض المخاطر في استخدام المراسلة الفورية، مثل عدم الانتباه لما حولنا. وهناك العديد من المخاطر الأخرى مثل طريقة التواصل والخصوصية وأمن أجهزة الحاسب الآلي والأجهزة المحمولة. و يعبر العديد من الناس عن أنفسهم بالكتابة بطريقة تختلف عن التحدث وجهاً لوجه مما يؤدي لبعض سوء الفهم أحيانا .

سوء الفهم

يواجه الكثير من الناس عند استخدام المراسلة الفورية صعوبة في معرفة ما إذا كان الشخص في الطرف الآخر حزين أو غاضب أو سعيد اكثر من التواصل وجهاً لوجه. وحتى مع استخدام الرموز للتعبير عن المشاعر فإنه من الصعب توصيل الإحساس أو المشاعر الحقيقية. ومن المعروف أن التحدث أسرع من الكتابة ولذلك فإننا أحياناً نلجأ لاستخدام كلمات أقل في المراسلة الفورية مما قد يؤدي إلى ضياع المعنى المقصود من الرسالة.

الجرأة والتحرر من القيود

يجد العديد من الناس التواصل عبر المراسلة الفورية أسهل بكثير من التواصل وجهاً لوجه مع الآخرين. والبعض يستطيعون التعبير عن أنفسهم بحرية أكثر باستخدام المراسلة الفورية، فيصبحون أكثر جرأة ولسبب ما يكونون أكثر قدرة على كتابة كل ما يريدون. وقد يكون ذلك سيئا لأنه يمكن أن يؤدي إلى كتابة أشياء لا ينبغي التصريح بها للأصدقاء أو الزملاء أو العائلة. فإذا لم ينتبه الشخص لما يكتب ، فقد يؤدي إلى البوح بمعلومات خاصة أو شخصية لأحد الأصدقاء، الأمر الذي قد يجعل هذا الصديق يُحدّث بها ربما لمن لا يجب أن يعلم هذه المعلومات.

هوية المتحدث

عندما تستخدم المراسلة الفورية الموجودة على الهواتف الجوالة بشكل خاص، قد يكون من الصعب التأكد من أنك تتواصل مع صديقك. فإذا كنت تتراسل معه عبر المراسلة الفورية، فهل أنت فعلاً متأكد فعلاً من أن من يتواصل معك على الجانب الآخر هو صديقك أم شخصٌ آخر قريب منه يستخدم جهازه ؟

روابط البرامج الخبيثة

المراسلة الفورية يمكن أن تستخدم لإرسال الملفات وروابط المواقع الإلكترونية، ولكن للأسف هذه البرامج لا تتفحص الملفات لتتأكد من خلوها من البرامج الخبيثة أو أن الروابط صحيحة. فقد تبدو مرسلة من صديق، خاصة اذا كانت تحمل عنوان مثل "شاهد" أو "افتح" فيدفعك فضولك لفتحها، فيصاب هاتفك بالبرامج الخبيثة. وقد أظهرت الدراسات أن الأشخاص الذين يستخدمون الهواتف المحمولة هم الأكثر ضغطاً على الروابط ومن ثم الأكثر عرضة لأن تصاب هواتفهم بالبرامج الخبيثة.

أفضل الممارسات للمراسلة الفورية

نستمتع كثيراً عند استخدام المراسلة الفورية ولكن يجب الحرص عند استخدامها. ونعرض هنا بعض الإرشادات الهامة التي يجب اتباعها أثناء استخدام المراسلة الفورية على الهاتف المحمول.

1. إذا كنت تسير أو تقود سيارتك فيجب عليك ان تتوقف لترسل أو تستقبل أي رسائل عند استخدامك الهاتف المحمول. فمن الصعب أن تكون في كامل تركيزك عند القيام بعملين في الوقت نفسه مما قد يؤدي إلى عواقب وخيمة. يجب ألا تستخدم الهاتف المحمول أثناء القيادة أو أثناء السير في طريق مزدحم.
2. كن أكثر صبرا وتفهماً عند استخدام المراسلة الفورية للتواصل مع الآخرين. فالشخص الذي تتواصل معه على الجانب الآخر قد لا يفهم مشاعرك الحقيقية وقد لايقدر هو أيضاً على توصيل مشاعره عبر المراسلة الفورية. فعلى سبيل المثال، إذا كنت تمزح فعليك أن توضح للطرف الآخر أنك تمزح كي لا يأخذ كلامك مأخذ الجد.
3. لا تضايق أحداً باستخدام المراسلة الفورية. فقد يؤدي هذا التصرف لمشاكل أو عواقب لم تكن في الحسبان. وإذا كنت أحد ضحايا التعدي الإلكتروني، فيجب عليك إخبار ولي أمرك أو المسئولين في مدرستك ليساعدوك على التصرف وحمايتك من التعدي.
4. لا ترسل معلومات خاصة أو شخصية عبر المراسلة الفورية لأنها لا تضمن السرية، فأنت لا تدري من يقرأ هذه المعلومات على الجانب الآخر، و قد لا يكون صديقك الذي تعتقد أنه يقرأ رسائلك.
5. لا تخبر أحد بكلمة المرور الخاصة بحسابك على المراسلة الفورية. فقد تقع في يد شخص سئ فيستخدمها وينتحل شخصيتك ويفعل أشياء قد تحرجك أو تضرك أو لا تعجبك.
6. لا يجب الضغط على أي روابط مرسلة من أشخاص مجهولين، لأنها قد تحتوي على برامج خبيثة تصيب جهازك. احترس من الروابط التي تثير انتباهك بموضوعات تهمك، فهذه هي الطريقة التي يستخدمها المهندسون الإجتماعيون (المخادعون على الإنترنت) لخداعك حتى تقوم بفتح تلك الروابط التي غالباً ما تكون مصابة بالبرامج الخبيثة.

واجب منزلي

المراسلة الفورية

إن إحدى الاستخدامات الضارة للمراسلة الفورية هي مضايقة أو تخويف الآخرين. فإن استخدام البريد الإلكتروني والمراسلة الفورية ومواقع التواصل الإجتماعي لمضايقة أحد ما، يسمى **بالتعدي الإلكتروني**. إستخدم الإنترنت لتبحث عن قصتين مختلفتين عن ممارسات التعدي الإلكتروني سواءً بإستخدام الإنترنت أو المراسلة الفورية أو مواقع التواصل الإجتماعي، وبعد قراءة هذه القصص، أجب عن الأسئلة الآتية:

1. لماذا يقوم بعض الطلاب بمضايقة الآخرين فقط عن طريق الإنترنت وليس في حياتهم اليومية؟
2. كيف يمكن استخدام المراسلة الفورية للقيام بالتعدي الإلكتروني؟
3. لماذا قد يكون لها تأثير كبير؟
4. ما الذي يجب فعله لحماية أنفسنا عند استقبال رسائل تعدي من آخرين؟

الدرس الثاني	شبكات التواصل الإجتماعي

تعريفات

شبكة التواصل الإجتماعي Social Network– تواصُل الناس مع بعضهم عن طريق برامج ومواقع معينة عبر الإنترنت، بهدف تبادل اهتماماتهم المشتركة وعلاقاتهم والتواصل لاغرض إجتماعية.

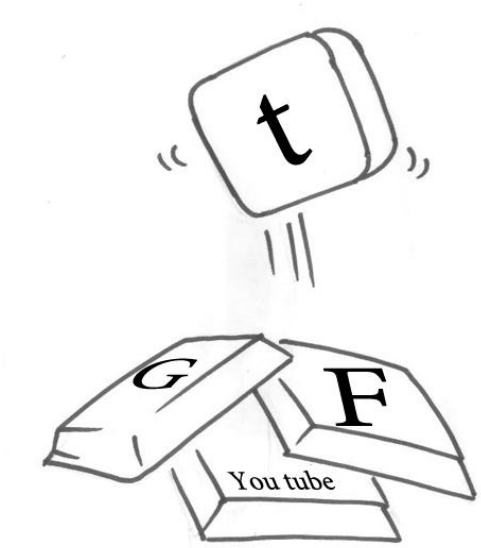
قنوات التواصل الإجتماعي - Social Media أشكال الاتصالات الإلكترونية التي يتم استخدامها لإنشاء المجموعات الإلكترونية. وهي تختلف عن شبكات التواصل الإجتماعي، حيث أنها تعد من الأدوات المستخدمة لتكوين شبكات التواصل والطرق المستخدمة التي من خلالها يتم التواصل. ومثال ذلك برامج الفيس بوك أو التويتر أو الانستغرام ، وغيرها ..

محرك البحث Search engine – هو موقع إلكتروني يقوم بجمع محتويات باقي المواقع ويقدمها بشكل منظم، ويساعد المستخدمين في البحث و ترشيح معلومات معينة.

معلومات شخصية Personal Information– هي تلك المعلومات التي يمكن استخدامها للتعرف على هوية أي شخص مثل الاسم أو رقم الهوية الشخصية أو الصفات الجسدية أو العنوان أو تاريخ ومحل الميلاد.

معلومات خاصة Private Information– هي أي معلومات لا يرغب صاحبها في الإفصاح عنها لأحد وتتضمن الأسرار والعلاقات الشخصية والأحوال المادية وما إلى ذلك.

نشأة شبكات و قنوات التواصل الإجتماعي



تواجدت شبكات التواصل الإجتماعي طويلاً قبل نشأة الإنترنت. فلطالما كانت متواجدة بسبب رغبة البشر في التواصل مع بعضهم. فببساطة شبكات التواصل الإجتماعي هي بيئة أو مجال أو وضع يتمكن الناس من خلاله التفاعل ومشاركة الأفكار ومناقشة الإهتمامات الخاصة والتواصل مع بعضهم. وهناك الكثير من الشبكات الإجتماعية التي لا تتطلب وجود الإنترنت.

شبكات التواصل الإجتماعي

أ- اكتب قائمة تضم عشر شبكات للتواصل الإجتماعي التي لا تستلزم وجود الإنترنت.

أ-1- اكتب الغرض من كل نوع لهذا الشبكات. يمكن للأمثلة أن تتضمن أعمال خيرية ومجموعات تبادل المعرفة والمعلومات، أوالإشتراك في ألعاب رياضية معينة.

أ-2- اكتب تحت كل شبكة الأمور الممكن مناقشتها أو فعلها لو كنت عضواً بها

ب- تعرف على شبكة تواصل إجتماعي على الإنترنت، والتي قد تشبه إحدى الشبكات التي لا تستلزم الإنترنت والتي كتبتها مسبقاً. ويمكن أن تتضمن تلك الشبكة مجموعة هي جزء من شبكة أكبر مثل فريق موسيقي أو مجموعة للأعمال الخيرية التي لها صفحة على موقع التواصل الإجتماعي Facebook

ت- مستخدماً المثال الذي كتبته في إجابة السؤال السابق، اشرح الغرض من الاشتراك في شبكات التواصل الإجتماعي على الإنترنت

ث- "شبكات التواصل الإجتماعي هي فقط للطلاب والمراهقين للدردشة مع بعضهم"، ناقش هذه الجملة.

استخدامات شبكات وقنوات التواصل الإجتماعي

ما الذي يجعل شبكات التواصل الإجتماعي على الإنترنت تشبه الشبكات الإجتماعية في حياتنا ؟

كلاهما يجمع الأشخاص ذوي الاهتمامات المتشابة. فعلى سبيل المثال لو أردت التحدث عن مساعدة الأطفال المرضى في حياتنا العادية أو على الإنترنت، ففي الحالتين هدفك واحد.

يمكنك مشاركة الأفكار والآراء سواء على الإنترنت أو في الحياه العادية. ويمكنك الإلتقاء بالآخرين ونشر صورك وبطاقة عملك ونشر الثقافة والمعرفة. ويمكنك أيضاً استعراض صورك التي قمت بإلتقاطها أثناء جلوسك مع آخرين أو عرضها على شاشة عرض وذلك في حياتنا العادية. ويمكنك أيضاً نشرها على الإنترنت ليراها الجميع، إلى جانب نشر قصيدة شعر كتبتها أو بحثا أجريته أو حتى العزف على آلتك الموسيقية المفضلة ليسمعها كل الناس. فالمعلومات والصور والأفكار والموسيقى سهلة المشاركة في كلا المحيطين.

ما هو الفرق بين شبكات التواصل الإجتماعي على الإنترنت والأخرى في حياتنا؟ هناك بعض الإختلافات بين الإثنين.

الأول :عن طريق الإنترنت ستتمكن من اللقاء بعدد أكبر من الناس من الذين يمكن أن تتلتقي بهم في الحياة العادية. فالإنترنت يتيح لك التواصل مع مستخدمين من شتى أنحاء العالم بدلاً من التواصل مع جماعة من الأشخاص المعدودين حولنا. وهذا يجعل تبادل الحوارات حول الاهتمامات المشتركة والأفكار أسهل بكثير، حيث يمكن لأي شخص الإطلاع على معلوماتك بما فيهم الأشخاص غير المرغوب بهم. وقد لا تفكر بالعواقب الناجمة عن نشر صورك أو معلومات تخصك على الإنترنت. فقد يجد صورك أي شخص من أي مكان بالعالم ثم يحورها أو ينشر رسائل تضايقك، أو قد تكتب تعليقاً في إحدى المجموعات الخاصة معتقداً أنه لن يراها أحد سوى أعضاء المجموعة، ولكن إذا صادف ورآها أحد من خارج المجموعة، فلن تصبح لها خصوصيتها. لذلك يجب عليك توفير الخصوصية والحماية لمعلوماتك لتجنب تلك الأمور المزعجة.

الثاني : عندما تكتب أو تنشر أي شئ على الإنترنت فإنه يبقى هناك لفترة طويلة. تقوم محركات البحث بجمع كل ما ينشره أو يكتبه مستخدمي الإنترنت ثم تحفظه لاستخدامه فيما بعد لعمليات البحث من قبل مستخدمي الإنترنت حول العالم. لذلك قد يظل ما قمت بنشره محفوظاً وموثقا لفترة طويلة على عكس الحال في الحياه العادية، حيث يمكنك إخبار أحد بشئ ما، ثم ينساه بعد فترة. ولكن ماهو موجود على الإنترنت يمكن دائما الرجوع إليه في أي وقت. فقد تكتب شيئاً ثم تندم أو تخجل من نشره، فتتمنى لو تتمكن من تغييره، حتى وإن فعلت فيبقى ما نشرته من قبل على الإنترنت. وقد تكررت مثل هذه الأخطاء، وأحياناً قد تكون أخطاء خطيرة. فيتمنى من نشرها لو أنها لم تحدث أو يتمنى إزالتها من الإنترنت.

دراسة شبكات وقنوات التواصل الإجتماعي

تعرف على مصدرين لقنوات التواصل الإجتماعي على شبكة الإنترنت.

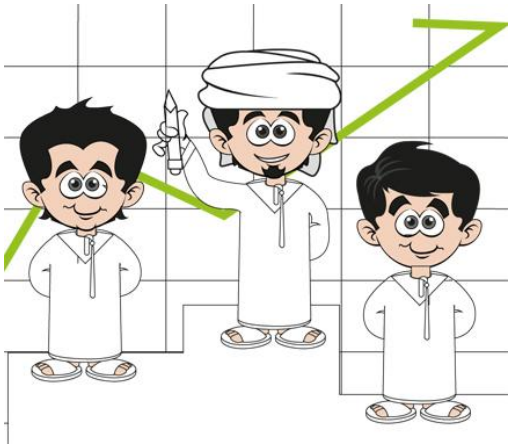
- اعرض ثلاث طرق لاستخدام كل من شبكات التواصل الإجتماعي وقنوات التواصل الإجتماعي – النشاطات التي يقوم بها المستخدمون والأدوات التي يستخدمونها. وضح إجاباتك مستخدماً صوراً لكيفية الإستخدام واعرض امثلة مختلفة للمستخدمين.
- اعرض ثلاث طرق تستخدمها الشركات لكل من شبكات التواصل وقنوات التواصل الإجتماعي – النشاطات والأدوات المستخدمة. وضح إجاباتك مستخدماً صوراً لكيفية الاستخدام واعرض أمثلة مختلفة لاستخدامات الشركات.

الآن بعد عرض زملائك لأعمالهم عن استخدامات شبكات وقنوات التواصل الإجتماعي. ما الأمثلة التي تناسب استخدام **الأفراد** ولماذا. وما الأمثلة التي لا تناسب استخدام الأفراد ولماذا؟ وهل أي من الأمثلة يشكل تهديداً على الأفراد؟ ولماذا؟

والآن بعد عرض زملائك لأعمالهم عن استخدامات شبكات وقنوات التواصل الإجتماعي. ما الأمثلة التي تناسب استخدام **الشركات** ولماذا. وما الأمثلة التي لا تناسب استخدام الشركات ولماذا؟ وهل أي من الأمثلة يشكل تهديداً على الشركات؟ ولماذا؟

شبكات وقنوات التواصل الإجتماعي الحالية للأعمال

تنامت شعبية شبكات التواصل الإجتماعي بشكل سريع. وبناءً على التقرير الذي أصدرته شركة نيلسن للأبحاث أن ثلاثة أرباع مستخدمي الإنترنت يستخدمون شبكات التواصل الإجتماعي.



إن إحدى أهم الأدوات بالنسبة للشركات و الأعمال هي التسويق والإعلان. والهدف هو تعريف العملاء بالشركة ومنتجاتها. فعلى سبيل المثال حينما تعلن شركة BMW عن سياراتها الجديدة لتعرف الناس على الميزات الحديثة في موديلات كل فئة ، فعليها إبراز أهم العوامل التي تشجع لضرورة شرائها.

كما تعلن شركتي Pepsi و Coca Cola عن مشروباتهما وتعلن المحال الكبيرة عن عروضها الضخمة حول بعض منتجاتها. وتسعى بعض الشركات أيضاً للإعلان عن خدماتها وهدفهم الأول هو إقناعك بأنها الشركة المُثلى للتعامل معها.

تُمكن شبكات التواصل الإجتماعي هذه الشركات من الإعلان عن منتجاتها وخدماتها. حيث عمل موقع Mashable استطلاعاً للرأي، ووُجد أن 77% من المستهلكين يتفاعلون مع العلامات التجارية عن طريق موقع فيسبوك بقراءة المشاركات وتعليقات المتابعين لصفحتهم . وذكر 17% أنهم يتفاعلون مع العلامات التجارية بتناقل التجارب الشخصية بينما ذكر 13% أنهم يقومون بنشر تحديثات للعلامات التجارية التي يفضلونها أو التي تعجبهم. وهذا ما يحدث في الواقع على العديد من شبكات ومواقع التواصل الإجتماعي.

ولا تقتصر الإستفادة من قنوات التواصل الإجتماعي على الشركات الكبرى فقط، بل استفادت أيضاً العديد من الشركات الصغيرة من هذه القنوات والإنترنت وبالتالي ساعد ذلك في تحويل عدد من الشركات الصغيرة إلى شركات عالمية. الفائدة الكبرى التي تلاحظها شركات الأعمال هو سعر التكلفة المنخفض، إذ يمكنهم إنشاء حساب مجاني على إحدى شبكات التواصل الإجتماعي، ثم نشر المعلومات والصور والفيديوهات لجذب العملاء وكسب متابعين أكثر. وتمكنت شركات صناعة الجبن من الوصول إلى مبيعات تصل إلى 70% نتيجة استخدام شبكات التواصل الإجتماعي. وهناك الكثير من المقالات المنشورة على شبكة الإنترنت عن مصورين ومصنعين واستشاريين وشركات المثلجات - أيس كريم – قد حققوا نجاحاً ملحوظاً بعد اشتراكهم في شبكات التواصل الإجتماعي. وقد حققت العديد من هذه الشركات نجاحاً أكبر عند نشر نشاطاتهم على شبكات التواصل مقارنة بنشرها فقط على مواقعهم الخاصة على الإنترنت.

إستخدام المؤسسات لقنوات التواصل الإجتماعي

ابحث عن موقع لقنوات التواصل الإجتماعي لإحدى الشركات أو المؤسسات الصغيرة.

1. اشرح نشاط الشركة والأعمال التي تؤديها.
2. اشرح كيفية استخدامها لقنوات التواصل الإجتماعي.
3. في رأيك، ما مدي فعالية ذلك لجذب الإنتباه لنشاط الشركة؟ وضح.

الاستخدام الآمن لقنوات وشبكات التواصل الإجتماعي

لقد ناقشنا سوياً شبكات وقنوات التواصل الإجتماعي وكيفية استخدامها من قبل المستخدمين العاديين وأصحاب الأعمال، كما ناقشنا من خلال الانشطة في الفصل بعض الإستخدامات الصحيحة والخاطئة لشبكات وقنوات التواصل الإجتماعي. والآن سنستعرض بعض الطرق السليمة لاستخدام شبكات التواصل بشكل آمن.

1. فكر جيداً قبل نشر أي شئ على مواقع التواصل الإجتماعي، لأنه وقتما يتم نشر ماتريد فاعلم أنها ستظل هناك لفترة طويلة جداً.
2. لا تنشر أي معلومات خاصة أو شخصية على شبكات التواصل الإجتماعي، مثل كلمات السر أو أرقام الحسابات البنكية أو أرقام هويتك الشخصية أو أي معلومات متعلقة بك شخصيا، هناك العديد من المراقبين والمهندسين الاجتماعيين الذين يبحثون ويحللون هذه المعلومات لاستخدامها في عمليات الإحتيال الإلكتروني.
3. لا تنشر خططك بشأن اجازات أو رحلات مستقبلية.
4. قبل نشر أي شئ بشأن شخص آخر، استأذنه أولاً. فقد لا يرغب في نشر صوره على شبكات التواصل الإجتماعي أو اطلاع الآخرين على أسراره. فقد تبدو لك الأمور غير ما تبدو له. وقد تنشر للآخرين صورا أو فيديوهات يظهرون فيه بشكل لا يرغبون أن يراهم الآخرين عليه فتتسبب في احراجهم. لذلك فكر في النتائج المترتبة على نشر تلك الأشياء.
5. تحقق من ما تقرأه على شبكات التواصل الإجتماعي، لأنه ليس كل ما ينشر فيها صحيح أو حقيقي. لذلك تأكد مما يتم نشره قبل أن تعيد نشره. فهناك الكثير من القصص التي تم نشرها على فيسبوك وتويتر ومواقع أخرى والتي تبين بعد ذلك أنها زائفة أو كذب للدعاية والتشهير ونشر المعلومات المغلوطة. وفي بعض الحالات، يحدث أن تنشر بعض الصحف والمدونات قصصاً من هذا النوع على أنها قصصاً حقيقية. فمن الأفضل القيام بدورك في البحث والتدقيق.

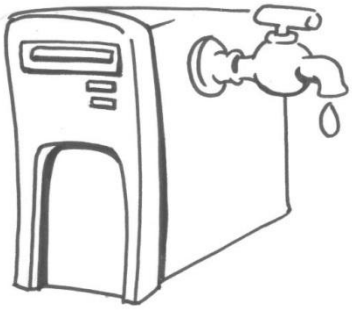
الاستخدام الآمن لشبكات وقنوات التواصل الإجتماعي

أسئلة :

1. لماذا يعد نشر أخبارا عن الخطط المستقبلية لقضاء الإجازات والعطلات خارج البيت أمراً يشكل تهديداً على أمننا الشخصي؟
2. اذكر مثالاً لموقف من خلاله يقوم شخص بغير قصد نشر معلومات الحساب البنكي أو أي بيانات أخرى لها نفس الحساسية على موقع للتواصل الإجتماعي.
3. لماذا تعد شبكة الإنترنت طريقة فعالة لنشر الشائعات والاخبار المكذوبة – خصوصاً عن الشخصيات المشهورة؟

واجب منزلي

تسريب المعلومات على شبكات التواصل الإجتماعي



استخدم الإنترنت للبحث عن قصص تسريب المعلومات الخاصة بالمؤسسات عن طريق استخدام العاملين بها لشبكات التواصل الإجتماعي. وبناءاً على هذه القصص،

أجب على السؤال التالي:

إذا نشر شخصٌ ما معلومات سرية تخص شركة ما، مثل المنتج الذي ستعرضه هذه الشركة في الأسواق العام القادم، أو حجم الأرباح التي ستحققها هذه الشركة في العام القادم. فهل يضر ذلك بالشركة؟ وضح إجابتك ؟

انتبه للنقاط التالية في المناقشة.

1. تستثمر الشركات أموال كثيرة لتطوير أفكار ومنتجات جديدة. فالمنتجات الإلكترونية مثل الهواتف الذكية أو الحاسب الآلي المحمول أو التطبيقات تستهلك الكثير من الوقت والمال (رواتب ومعدات ووقت وجهد) لتطويرها. فإذا تم نشر تسريبات حولها على شبكات التواصل الإجتماعي، فقد تصل تلك الأخبار للشركة المنافسة فتبدأ في تطوير منتجها المشابه. وقد يكون المنافس إحدى الشركات الكبرى التي بإمكانها العمل على تطوير منتجها بصورة أكبر أو تسويقه بشكل أوسع مما يؤدي لخسارة الشركة الأولى.
2. عندما تطرح شركة اسهمها للاكتتاب فتبدأ عملية البيع والشراء للأسهم في البورصة. وقيمة هذه الأسهم تعكس حجم الشركة ويشتري الناس أسهم الشركة ليستثمروا فيها. فإذا تم نشر معلومات تخص تقارير مالية للشركة قبل طرح أسهمها في البورصة، فإن ذلك سيؤثر بالسلب أو الإيجاب على حركة بيع الأسهم الخاصة بالشركة.
3. قد يتكلم أي موظف بشكل سئ عن شركة ما، مما قد يسبب الإحراج لتلك الشركة. قد يكون ما قاله غير صحيح أو غير ملائم فيعطي ذلك فكرة سيئة عن الشركة وقد يصدقه البعض فعلاً وهو ما يكون عكس الواقع تماماً. وهذا كله حتماً سيقضي على سمعة الشركة.

الدرس الثالث	مخاطر على شبكة الإنترنت

تعريفات

البرامج الخبيثة Malware : برامج مصممة لتدمير أجهزة الحاسب الآلي. وهناك العديد منها مثل الفيروسات وبرامج التجسس والديدان وحصان طروادة والبوتنت وغيرها .

بوتنت Botnet: هي شبكة مكونة من مجموعة من أجهزة الحاسب الآلي التي تحتوي على برامج خبيثة يتم التحكم بها وتوجيهها لتنفيذ مهام مختلفة.

المُغَيّب Zombie: هو جهاز حاسب آلي أو نظام ضمن شبكة بوتنت.

مزودات التحكم والسيطرة: هو جهاز أو مجموعة من أجهزة الحاسب الآلي التي تتحكم بالمغيب Zombie وتوجهه ليقوم بالمهام المطلوبة منه.

برامج مكافحة الفيروسات Anti-Virus Software: هي برامج مصممة للتعرف على الفيروسات والبرامج الخبيثة وإزالتها من أجهزة الحاسب الآلي.

البريد المزعج Spam email: هي رسائل تصل إلى بريدك الإلكتروني بدون إذنك أو بدون أن تطلب أن ترسل إليك. وأغلبها رسائل غير مرغوب بها ، وعادة ما ترسل هذه الرسائل لعدد كبير من الناس.

توقف الخدمة Denial of Service: هي الحالة التي لايستجيب فيها جهاز الحاسب الآلي أو موقع إلكتروني أو أي نظام آخر للأوامر العادية. التوقف المتعمد للخدمة يحدث عندما يتعمد شخص ما فعل شئ مما يجعل النظام يتوقف عن الإستجابة للتشغيل أو الأوامر.

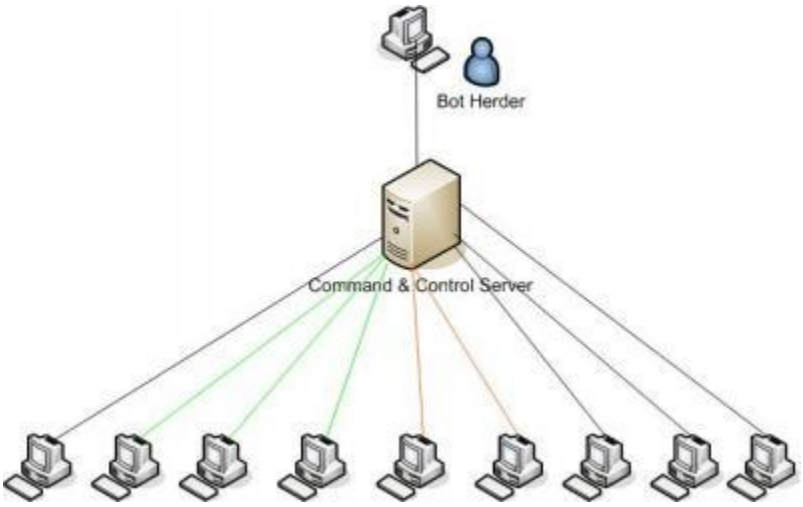
الهندسة الإجتماعية Social Engineer: هي مجموعة من التقنيات التي تجعل البعض يقومون بعمل ما أو يفضون بمعلومات خاصة أو سرية وتستخدم ضمن احتيال الإنترنت وهدفها طرح اسئلة بسيطة أو تافهة عن طريق الهاتف أو البريد الإلكتروني لتحقيق الغرض المنشود من الضحية

المخاطر على شبكة الإنترنت

البوتنت

تخيل أنك تملك عدداً كبيراً من أجهزة الربوتات التي تعمل لديك وتتحكم وتسيطر عليها بما تشاء. فتنجز لك المهام الصعبة وتقود لك سيارتك وتعد لك الطعام وتعمل على إصلاحات في المنزل. فيمكنك إنجاز الكثير من الأعمال بأقل جهد.

البوتنت هي شبكة الحاسبات الخاصة بالمخترق. أي أنها شبكة من أجهزة الحاسب الآلي التي أصابتها البرامج الخبيثة والتي يتحكم بها المخترق باستخدام حاسب آلي مركزي للتحكم بشبكة الأجهزة المصابة. من خلال الجهاز المركزي، يعطي المخترق الأوامر للبرامج الخبيثة الموجودة على أجهزة الحاسب الآلي المصابة لإنجاز بعض المهام. ويسعى المخترق لنشر البرامج الخبيثة على جميع الأجهزة في العالم ليفعل ما يشاء. بعض هذه الشبكات يشمل آلاف الأجهزة وبعضها يشمل الملايين.



يتم تحميل البرنامج الخبيث "المغيب" Zombie على الأجهزة الموجودة على الإنترنت، ثم ينتظر هذا البرنامج الأوامر من المسيطر أو المتحكم في الشبكة لينفذ ما يطلب منه.

كيف تصاب أجهزة الكمبيوتر ببرنامج "المغيب" Zombie ؟

تصاب أجهزة الكمبيوتر ببرنامج "المغيب" Zombie بعدة طرق، غالباً مايستخدمها المخترق جميعاً.

1. يقوم المخترق بتحميل البرنامج الخبيث على أحد المواقع الإلكترونية وعندما يزور أي مستخدم هذا الموقع، يتم تحميل هذا البرنامج على جهاز المستخدم.
2. يقوم المخترق بارسال بريد إلكتروني للعديد من الناس والتي تتضمن ملفات مصابة بالبرامج الخبيثة. ويحرص المخترق على أن يبدو البريد الإلكتروني مهما ويستدعى التجاوب معه من قبل المستخدم.
3. يقوم المخترق بارسال رسائل عبر برامج المراسلة الفورية منتحلاً شخصية صديق أو يقدم فيه شيئاً شيقاً ويطلب من المرسل إليه أن يقوم بتحميل الملف المرفق بالرسالة والذي يبدو مثيراً للاهتمام، ولكنه في الواقع يحمل البرامج الخبيثة.

بمجرد تحميل برنامج "المغيب" Zombie على الجهاز المستهدف، يحاول الإتصال بالجهاز المسيطر وتسجيل نفسه. وإذا كان البرنامج Zombie معقداً، فيمكنه الإختباء من برنامج مكافحة الفيروسات والبرامج الخبيثة ثم يقوم بتفعيل الجهاز المصاب أو الشبكة في غياب المستخدم.

واجب منزلي **البوتنت**	

استخدم الإنترنت للبحث عن قصص حول البوتنت. ابحث عن أمثلة عدة للبوتنت التي تم اكتشافها واغلاقها في عامي 2011 و2012.

1. اكتب الطرق المختلفة التي يستخدمها المخترقون ومجرمو الإنترنت في استخدام البوتنت.

2. ما هي الطرق الأكثر ضرراً و التي يستخدمها المخترقون ومجرمو الإنترنت؟

تأثيرات المخاطر الموجودة على شبكة الإنترنت

البرامج الخبيثة مثل الفيروسات، وملفات التجسس ، والبوتنت لها مخاطر رهيبة. دعونا نلقي نظرة على الطرق التي يمكن أن تؤثر على مستخدمي الإنترنت.

يمكن للبرامج الخبيثة أن تدمر الملفات الموجودة على أجهزة الحاسب الآلي سواء باتلافها أو حذفها أو حتى إغلاقها بحيث لا يقدر صاحبها على فتحها إلا بدفع فدية. تختلف أهمية تلك الملفات بحسب إختلاف مستخدمها. فعلى سبيل المثال، قد لا يهتم رجل أعمال بضياع الصور العائلية الخاصة به ولكن إذا كان رجل له روابط عائلية قوية، فإن ضياع تلك الصور قد يسبب له ألماً نفسياً سيئاً. ولكن قد يغضب رجل الأعمال إذا قام فيروس بحذف أحد الملفات الهامة أو تسبب في توقف أحد التطبيقات المهمة.

يمكن للبرامج الخبيثة سرقة كلمات السر وبيانات حسابات البنوك والأموال والملكية الفكرية. استخدام البرامج الخبيثة للإحتيال هو تصرف إجرامي ويسبب للضحية أضرار جسيمة. إن استخدام البرامج الخبيثة للاحتيال يعد جريمة وتترك أثراً سيئاً على الضحية. ماذا سيكون شعورك إذا علمت بسرقة أموال من حسابك البنكي؟ ناهيك عن محاولات إثبات أنك لم تقم بأي عمليات شراء على هذا الحساب والتي قد تضيع وقتاً طويلا أنت بحاجة إليه لقضاءه مع عائلتك أو للعمل أو لإنجاز أي مهام ضرورية أخرى. إذا فقدت كلمة السر الخاصة بك لحساباتك المختلفة مثل بطاقة الإئتمان وحساب صفحتك على شبكة التواصل الإجتماعي أو بريدك الإلكتروني، فقد يستغل أحدهم ذلك وينتحل شخصيتك مستخدماً حساباتك، ويقوم بتخريبها أو تدمير أعمالك وقد تتأثر سمعتك بسبب ذلك.

يمكن أن يُستخدم البوتنت في ملئ البريد الإلكتروني بالرسائل المزعجة وتعطيل ومهاجمة المواقع الإلكترونية. ومن الممكن أن يصبح موقع أحد الشركات غير متاح بسبب هجمات توقف الخدمة التي تشغل الموقع أكثر من طاقته. ومن الممكن أن يتشبع نظام البريد الإلكتروني الخاص بالشركة بالبريد المزعج في حين يحاول المغيب خفية بمهاجمة النظام نفسه. وعليه يتأثر مستخدمي الشبكة الخاصة بالشركة لأن الأجهزة مصابة بالبرامج الخبيثة وتصبح الأجهزة بطيئة ولا تعمل بشكل جيد مما يأثر سلبا على أداءهم الوظيفي والاداري.

تؤثر البرامج الخبيثة علينا جميعاً ويستفيد فقط المجرمون المتخفين في شبكة الإنترنت لأنهم يربحون منها وتضر الأفراد والشركات الذين ينفقون المال والوقت لحماية أنفسهم.

البوتنت والبرامج الخبيثة

قم بعمل مناقشة في فصلك عن الأسباب التي تجعل البعض يستخدمون البوتنت Botnets ومدى تأثيرها علينا.

1. لماذا قد يلجأ أي شخص لإنشاء البوتنت؟ ماذا يمكن أن يفعل؟
2. لماذا قد يستهدف أحد أي موقع باستخدام هجمات توقف الخدمة denial of service ؟
3. ماذا يمكن أن يحدث لك إذا تعرض جهازك لعدوى المغيب Zombie؟

مخاطر على شبكات التواصل الإجتماعي

المخاطر الخاصة بشبكات التواصل الإجتماعي لا تكون واضحة مثل فيروسات أجهزة الحاسب الآلي، فمعظمها من الهندسة الإجتماعية ويحاول من خلالها المهندس الإجتماعي إقناعنا بفعل أشياء لا نفعلها في أغلب الأحيان. ويستغل المهندس الإجتماعي النقاط التالية لإيقاع ضحيته وجمع أكبر قدر ممكن من معلوماته الخاصة والشخصية:

- **الطمع** – قد يجذب المهندس الإجتماعي الضحية بزعم الحصول على هدايا مجانية أو أموال كثيرة
- **الفضول** – ارسال مرفقات أو روابط مصحوبة بكلمة للترغيب في فتحها مثل "مفاجأة " أو "لا يفوتك هذا العرض"
- **المساعدة** – هناك أعداد هائلة من الناس تتصرف بحسن نية وتبدي استعدادها لمساعدة الآخرين عبر الإنترنت من جانب إنساني.

شبكات التواصل الإجتماعي مصممة لتكون آمنة ومساعِدة للمستخدم وليست محل شكوك بتواجد إعلانات أو أي إغراءات أخرى.

تويتر Twitter

التغريدات المزعجة : عندما يتم إختصار عنوان أي موقع في نص التغريدة، فإنه يصبح من الصعب تحديد إذا كان لموقع حقيقي أم لا. لذلك قد يضغط أي شخص على رابط فيتم تحميل برامج خبيثة.

فيس بوك Facebook

اصطياد الإعجاب : يقوم المتعدي بنشر شئ ما مثير للاهتمام وبه فيديو أو رابط موقع، فيضغط المستخدمون على خيار الاعجاب (Like) ، فيظهر بعد ذلك على صفحاتهم الخاصة فيراها أصدقائهم ويضغطوا أعجنبي ، وتتكرر العملية، وقتها يتم تحميل البرامج الخبيثة على أجهزة الحاسب الآلي الخاصة بكل ما شارك في الاعجاب.

تطبيقات الإحتيال: الفيسبوك لا يتحقق من التطبيقات التي يروج لها على موقعه فينتهز المتعدون هذه الفرصة وينشئوا تطبيقات مماثلة تطلب الدخول لأماكن معينة على صفحتك مثل قائمة معارفك أو حتى تطلب الإذن لنشر موضوعات على صفحتك. ولذلك يمكن استخدام هذه التطبيقات لتحميل البرامج الخبيثة أو سرقة هويتك ومعلوماتك الخاصة.

الدردشة: كما قلنا من قبل فإن مستخدمي المراسلة الفورية يمكن خداعهم بالمرفقات وروابط المواقع التي أحياناً لا يترددون في الضغط عليها من باب الفضول و هو أقوى دافع.

احمي نفسك

لقد ناقشنا من قبل الطرق المختلفة التي يمكن أن نحمي أنفسنا بها ضد المخاطر السابقة. ولذلك تذكر الآتي :

- لا تنشر معلوماتك الخاصة والشخصية عند استخدام وسائل مثل البريد الإلكتروني والمراسلة الفورية وشبكات التواصل الإجتماعي لأنها وسائل تواصل علنية ويمكن لأي برنامج تجسس أوشخص رؤية ما فيها.
- تعرف على محاولات الهندسة الإجتماعية وحاول مقاومتها، وفكر جيداً قبل فتح أي مرفقات أو روابط أو نشر أي معلومات حتى لا تندم فيما بعد.
- تأكد من تحديث برنامج مكافحة الفيروسات الموجود على جهازك وأنه يعمل بشكل جيد.
- استخدم الإنترنت بشكل لائق وفكر دائماً في عواقب أي شئ تقوم به.

نصائح سريعة

- لا تستخدم المراسلة الفورية أو الهاتف الجوال أثناء إنشغالك بأعمال تتطلب انتباهك. فقيادة السيارة أو السير على الطريق أثناء استخدام الهاتف الجوال قد يشكل خطراً على حياتك.
- لا ترسل بياناتك الشخصية أو الخاصة باستخدام المراسلة الفورية أو البريد الإلكتروني أو شبكات التواصل الإجتماعي.
- لا تشارك أحداً كلمات السر الخاصة بك.
- لا تفتح أي روابط أو مرفقات مرسلة من أشخاص مجهولين. كن حذراً في التعامل مع المرفقات المرسلة من أي شخص أو من أصدقائك لأنها قد تحتوي على برامج خبيثة.
- فعّل برنامج مكافحة الفيروسات على جهازك وقم بتحديثه بشكل مستمر.
- فكر جيداً قبل التعليق على أي شئ منشور على شبكات التواصل الإجتماعي فقد تكون محاولة للهندسة الإجتماعية، لذلك من الأفضل التحقق من الأمر قبل التعليق عليه.

إختبر معلوماتك	

1. ما المقصود بالمراسلة الفورية؟

2. ما الذي يجب أن تحذره عند استخدامك المراسلة الفورية؟ اختر جميع الإجابات الصحيحة.
   a. لا تشتت تفكيرك في المواقف التي تحتاج انتباهك
   b. لا ترسل أي بيانات خاصة أو شخصية عند استخدامك المراسلة الفورية
   c. بلّغ عن المتعدين أو الرسائل غير اللائقة
   d. إفتح الروابط المرسلة من مجهولين
   e. لا تفتح المرفقات المرسله من مجهولين
   f. إفتح الروابط القصيرة للمواقع الإلكترونية دائماً

3. لماذا يجب الانتباه لما يدورمن حولنا عند استخدام المراسلة الفورية؟ وضح إجابتك ؟.
4. ما التصرف الصحيح الذي يجب اتباعه عندما تصلك رسائل غير لائقة من شخص مجهول عبر المراسلة الفورية؟ اختر جميع الإجابات الصحيحة.
   a. قم بالرد على الرسائل
   b. أجب عن أي أسئلة يوجهها لك الشخص المجهول
   c. امنع الشخص المجهول من الوصول إليك
   d. اخبر والديك بشأن الرسائل
5. ما هي شبكة التواصل الإجتماعي؟ اختر الإجابة الصحيحة.
   a. هو مكان حيث يتواصل الناس مع بعضهم لمشاركة اهتماماتهم
   b. هي نوع من التكنولوجيا يمكن الأقمار الصناعية بالتواصل
   c. هو ابتكار جديد لم يكن يتواجد من قبل

6. إن شبكات التواصل الإجتماعي هي ابتكار جديد.
   a. صحيح
   b. خطأ
7. كيف يمكن استخدام شبكات التواصل الإجتماعي وقنوات التواصل الإجتماعي لمساعدة الناس؟ اختر جميع الإجابات الصحيحة.
   a. تجعل من الصعب على مستخدمي الإنترنت التعرف على طبيعة عملك
   b. تجعل من السهل على مستخدميها التعرف على أفكار جديدة لهواياتهم
   c. هي وسيلة أقل تكلفة لتسويق الأعمال
   d. تتيح الفرصة للعديد من المستخدمين حول العالم مشاركة الأفكار الهادفة
8. ما نوع المعلومات التي لا يجب نشرها أو مشاركتها على شبكات التواصل الإجتماعي؟ اختر جميع الإجابات الصحيحة.
   a. كلمات السر
   b. البيانات الشخصية
   c. المعلومات الخاصة
   d. أي شئ لا يمكنك الإفصاح عنه أمام الناس
   e. اسم حيوانك الأليف
9. كيف يمكنك حماية نفسك عند استخدام شبكات التواصل الأجتماعي؟ اختر جميع الإجابات الصحيحة.
   a. نشر أي شئ يخطر ببالك على شبكات التواصل الإجتماعي
   b. عدم نشر أو مشاركة البيانات الشخصية على شبكات التواصل الإجتماعي
   c. عدم نشر خططك المستقبلية للسفر
   d. قبل نشر أي معلومات عن شخص آخر، استأذنه أولاً
10. ما هو البوتنت؟ وضح بأسلوبك.