الرخصة الأوروبية لقيادة الحاسب الآلي"ECDL" و الرخصة الدولية لقيادة الحاسب الآلي "ICDL"و"المواطن الإلكتروني "e-Citizen" و شعار المؤسسة هي علامات تجارية مسجلة لمؤسسة الرخصة الأوروبية لقيادة الحاسب الآلي المحدودة في أيرلندا وبلدان أخرى.

أي سي دي أل – العربية تعمل قانونياً تحت اسم أي سي دي ال جي سي فاونديشن وهي علامة تجارية موحدة تغطي مناطق ICDL التالية الإمارات العربية المتحدة، البحرين، السعودية، العراق، الكويت، عمان، قطر ومصر.

DM3 هي كيان مستقل عن مؤسسة الرخصة الأوروبية لقيادة الحاسب الآلي المحدودة وليست تابعة لها بأي شكل من الأشكال. وقد تستخدم البرامج التعليمية للرخصة الأوروبية لقيادة الحاسب الآلي/الرخصة الدولية لقيادة الحاسب الآلي من DM3 لمساعدة الطلاب في التحضير للحصول على مؤهل الرخصة الدولية لقيادة الحاسب الآلي. كما أن مؤسسة الرخصة الأوروبية لقيادة الحاسب الآلي المحدودة أي سي دي أل – العربية وكذلكDM3 لا يقدمون أي ضمانات تفيد بـأن استخدام البرامج التعليمية للرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي منDM3 يضمن اجتياز مؤهل الرخصة الدولية لقيادة الحاسب الآلي. ويفيد وضع الشعار المعتمد للبرامج التعليمية لمؤسسة الرخصة الأوروبية لقيادة الحاسب الآلي على هذا المنتج بأنه قد تمت مراجعته والموافقة عليه بشكل مستقل من قبل أي سي دي أل – العربية بما يتناسب مع المعايير التالية:

التغطية المقبولة لجميع محتويات البرامج التعليمية المتعلقة بالإصدار الجديد من المنهاج الرئيسي لبرامجICDL.

لم تتم مراجعة مادة البرامج التعليمية هذه للتأكد من دقة المعلومات التقنية، كما أنها لا تضمن نجاح المستخدم النهائي في اجتياز امتحانات مؤهل الرخصة الدولية لقيادة الحاسب الآلي. تتعلق كل بنود التقييم و/أو تمارين الأداء التي تتضمنها البرامج التعليمية للرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي من DM3 فقط بهذه البرامج ولا تمثل أو تشمل أي من برامج مؤسسة الرخصة الأوروبية لقيادة الحاسب الآلي أو أي سي دي أل – العربية فيما يتعلق بأي من امتحانات الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي. للحصول على التفاصيل بشأن الخضوع لامتحانات الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي في بلدك، يرجى الاتصال ب أي سي دي أل – العربية علىwww.icdlarabia.org أوinfo@icdlarabia.org.

يتعين على المرشحين الذين يستخدمون مواد البرامج التعليمية هذه أن تكون بحوزتهم بطاقة مهارات الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي سارية. وبدون بطاقة المهارات تلك، لن يتمكن المرشح من الخضوع لامتحانات الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي أو الحصول على شهادتها أو على أي شكل من أشكال الاعتراف به.

يمكن الحصول على بطاقة مهارات الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي من أي مركز معتمد لامتحانات الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي.

تتضمن الإشارة إلى الرخصة الأوروبية لقيادة الحاسب الآلي (ECDL/ICDL) الإشارة إلى الرخصة الدولية لقيادة الحاسب الآلي .(ICDL) وقد تم نشر الإصدار الجديد من المنهاج الرئيسي لبرامج ICDL باعتباره المنهج الرسمي للاستخدام ضمن برنامج شهادة الرخصة الأوروبية لقيادة الحاسب الآلي (ECDL/ICDL) والرخصة الدولية لقيادة الحاسب الآلي (ICDL).

جدول المحتويات

الفصل 2-1 الحماية 4

2-1-1 الهوية 5

2-1-2 المصادقة 10

2-1-3 مكافحة الفيروسات 12

2-1-4 مكافحة التجسس 15

الفصل 2-2 الأمان 19

2-2-1 النسخ الاحتياطي 20

2-2-2 البريد الإلكتروني 23

2-2-3 الشبكات اللاسلكية 25

2-2-4 الأمن المادي للأجهزة 27

2-2-5 الأجهزة الذكية 29

الفصل 2-3 توخ الحذر 37

2-3-1 مخاطر الإنترنت 38

2-3-2 التسوق عبر الإنترنت 41

2-3-3 الدفع عبر الإنترنت 45

الفصل 2-4 التفكير أولاً 49

2-4-1 الهوية الشخصية 50

2-4-2 أجهزة المشاركة 53

2-4-3 شبكات التواصل الاجتماعي 55

2-4-4 البريد الالكتروني غير المرغوب فيه والتصيد الاحتيالي على مواقع شبكة التواصل الاجتماعي 58

2-4-5 الهويات الزائفة على وسائل التواصل الاجتماعي 60

الفصل 2-5 العالم الافتراضي 63

2-5-1 المراسلة الفورية/غرف الدردشة 64

2-5-2 الفيديوها، المدونات 67

2-5-3 ألعاب الإنترنت 71

2-5-4 تولي المسؤولية 73

الفصل 2-6 التعلم سويًا 77
2-6-1 المناقشة 78
2-6-2 المراقبة الأبوية 81
2-6-3 إدمان الإنترنت 91
الفصل 2-7 السلوك الافتراضي 97
2-7-1 التواصل 98
2-7-2 التسلط عبر الإنترنت 100
الفصل 2-8 السياسة 107
2-8-1 الاستخدام 108
2-8-2 حقوق الطبع والنشر 111
الفصل 2 - تمارين 114
2-ت-1 فيس بوك 115
2-ت-2 تويتر 120
2-ت-3 يوتيوب 124
2-ت-4 جوجل+ 125
2-ت-5 لينكدإن 129
2-ت-6 المدونات 134

الأهداف

يزود مقرر **السلامة على الإنترنت**المستخدمين بالمهارات والمعارف المطلوبة للتعامل مع أجهزة الكمبيوتر والأجهزة المحمولة لتوخ الحذر من مخاطر الإنترنت، حيث سيدرك المرشحون أهمية حماية المعلومات الشخصية على أجهزة الكمبيوتر والأجهزة المحمولة وسيتعرفون على التهديدات التي تشكلها عمليات الإجرام والاحتيال على الإنترنت.

كما سيتعرف المرشحون على التهديدات التي تشكلها الفيروسات، وسيدركون أهمية استخدام برامج مكافحة الفيروسات وجدران الحماية، وسيتعرفون أيضًا على إجراءات النسخ الاحتياطي واستخدام كلمات المرور الجيدة وكيفية تصفية الرسائل غير المرغوب فيها من البريد الإلكتروني جنبًا إلى جنب مع إدراك أهمية فحص مرفقات البريد الإلكتروني قبل فتحها.

وسيتعرف المرشحون أيضًا على المعلومات الواردة في الأجهزة الذكية وكيفية تبادلها عبر الانترنت وكيفية تعيين ميزات الأمان المناسبة للأجهزة الذكية للوقاية من التهديدات الأمنية ومنع الوصول غير المصرح به إلى الجهاز والبيانات التي يحتوي عليها.

وسيتعرف المرشحون بجانب ذلك على المخاطر الكامنة في الاستخدام اليومي للإنترنت، وكيفية حماية أنفسهم عند التسوق عبر الإنترنت، وكذلك الآثار المترتبة على وضع المعلومات الشخصية على مواقع التواصل الاجتماعي، بالإضافة إلى الأمور المتعلقة بالخصوصية، والأجهزة التي يمكن استخدامها لتبادل المعلومات جنبًا إلى جنب مع كيفية إمكان استخدام ميزات الصور والفيديوهات لتسجيل ومشاركة المعلومات غير اللائقة.

هذا وسيتعرف المرشحون على بعض المخاطر المرتبطة بشبكات التواصل الاجتماعي التي من بينها: المحتوى غير اللائق، وقضايا التحقق من السن، والوصول إلى الملفات التعريفية، واحتمالية التعرض للمعتدين، والتهديدات التي تشكلها هجمات الهندسة الاجتماعية، والتهديدات السيبرانية التي يتعرض لها الأطفال عن طريق استخدام هويات زائفة على وسائل الاعلام الاجتماعي.

وبالإضافة إلى ذلك سيتعرف المرشحون على الممارسات السلوكية المسؤولة عند الانخراط في نشاط على الإنترنت والتي من بينها: أهمية عدم تداول المواد التي قد تضر الآخرين، ومعرفة كيفية رفض أو منع الغرباء والاتصالات غير المرغوب فيها، واستخدام كاميرا الويب مع الأشخاص الذين تعرفهم فقط، ومعاملة الآخرين عبر الإنترنت بالاحترام.

كما سيتعرف المرشحون على مختلف الموضوعات التي تدور حول السلامة على الإنترنت وسيكونون قادرين على فهم كيفية حماية أنفسهم بشكل أفضل على الإنترنت، وسيتعلم المرشحون أيضًا كيفية إعداد ضوابط المراقبة الأبوية لحماية أنشطة أطفالهم على الإنترنت, واختيار برامج التنقية والمراقبة واستخدامها, وذلك جنبًا إلى جنب مع إدراك مفهوم إدمان الإنترنت, وكيفية التعرف على أعراض هذه المشكلة والتعامل معها, فضلاً عن معرفة مفهوم التسلط عبر الإنترنت وفهم الوسائل التي يمكن أن يحدث من خلالها, وكذلك التعرف على علامات التحذير من التسلط عبر الإنترنت ومعرفة كيفية مواجهته, بالإضافة إلى معرفة أسباب دعوة المؤسسات إلى إرساء سياسات الاستخدام المقبول (AUP's) وتبنيها، جنبًا إلى جنب مع التعرف على عناصر السياسات الفعالة.

الفصل 2-1

الحماية

2-1-1 الهوية

2-1-2المصادقة

2-1-3مكافحة الفيروسات

2-1-4مكافحة التجسس

1-2 الحماية

1-1-2 الهوية

1-1-1-2 إدراك أهمية حماية المعلومات الشخصية الموجودة على جهاز الكمبيوتر الخاص بك

نحن نستخدم أجهزة الكمبيوتر الشخصية والمحمولة واللوحية والهواتف الذكية بصفة يومية لإجراء أنشطة شخصية على الإنترنت، فأنشطة كاستخدام شبكات التواصل الاجتماعي والتسوق عبر الإنترنت وإجراء أبحاث متعلقة بالفروض المنزلية هي جزء لا يتجزأ من حياة الطلاب، وتقوم المؤسسات المختصة أثناء تنفيذنا لهذه الأنشطة بجمع المعلومات الشخصية واستخدامها، ومن ثم تتحمل مسؤولية المعلومات المنوطة بحمايتها، كما أن هناك أيضًا احتياطات يمكننا اتخاذها لحماية معلوماتنا الشخصية وتأمين الوصول إلى المعلومات المخزنة على أجهزة الكمبيوتر وأجهزة المحمول الخاصة بنا.

لحماية الكمبيوتر الخاص بك - وبالتالي معلوماتك الشخصية - ينبغي عليك إجراء بعض الأمور التي من بينها:

- تثبيت برامج أمان لحمايتك من الهجمات والفيروسات.
- تحديث البرامج الخاصة بك باستمرار.
- مسح سجل المتصفح الخاص بك وملفات تعريف الارتباط على أساس منتظم.
- عدم تبادل كلمات المرور.
- توخ الحذر عند فتح مرفقات البريد الإلكتروني.
- الحرص الدائم على عمل نسخ احتياطية من الملفات والمستندات المهمة وغيرها في جهاز خارجي آمن.
- عدم تنزيل برامج أو تطبيقات غير معروفة من الإنترنت.

تتوفر سياسات الخصوصية والأمان في برامج التواصل الاجتماعي من أجل حماية معلوماتك الشخصية عند التواصل على الإنترنت، انظر الشكل 1 أدناه الذي يوضح صفحة إعدادات أمان موقع الفيس بوك:

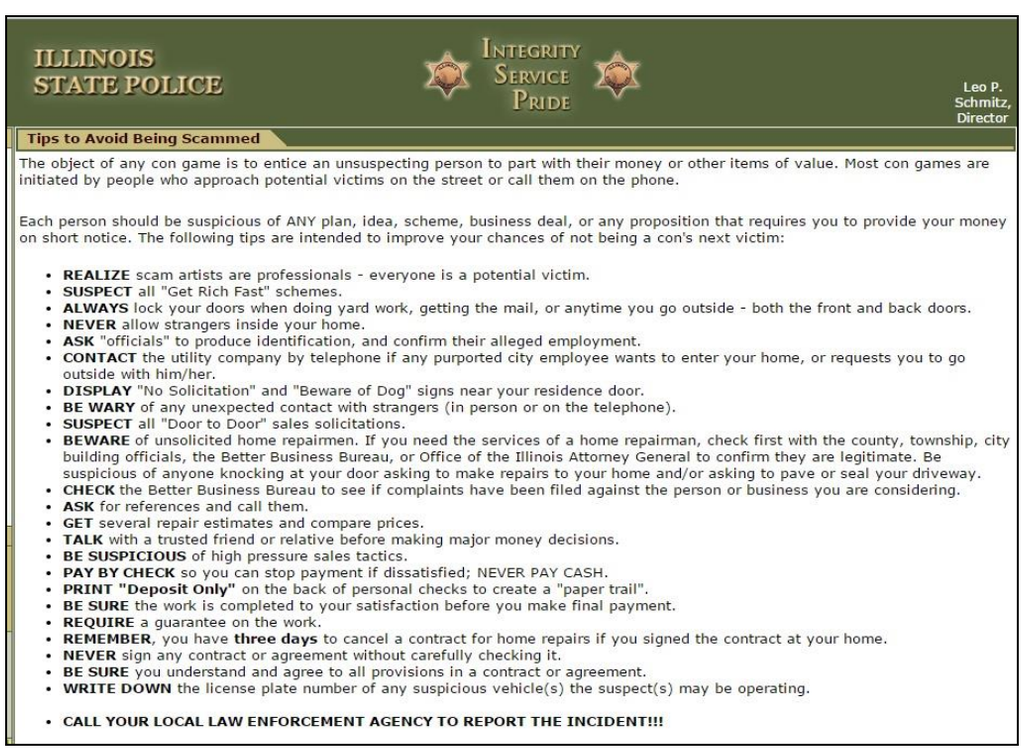
الشكل 1: صفحة إعدادات أمان موقع الفيس بوك (https://www.facebook.com/security/).

2-1-1-2 التعرف على التهديدات التي تشكلها عمليات الإجرام والاحتيال على الإنترنت

يتعرض أي شخص يستخدم الإنترنت إلى خطر جرائم الإنترنت، فالإنترنت وسيلة سهلة للمجرمين لأخذ أموال الناس بالخداع عن طريق سرقة معلوماتهم الشخصية، ويحدث الاستغلال الإجرامي للإنترنت - الذي يشار إلى أحيانا باسم "جرائم الإنترنت" أو "الجرائم الالكترونية" - عندما ترتكب الجرائم في حق أفراد أو مجموعات من الأفراد ممن يستخدمون شبكات الاتصالات الحديثة مثل غرف الدردشة والبريد الإلكتروني وبرامج التواصل الاجتماعي وخدمات والمراسلة النصية والرسائل القصيرة،ومن الأساليب الشائعة في ذلك:

- برامج الفيروسات - إفساد ملفات البيانات أو حذفها
- سرقة الهوية - سرقة المعلومات الشخصية لشخص ما
- تزوير العناوين: محاولة إعادة تحويل زوار موقع معين إلى موقع مزيف
- القرصنة - الدخول على الشبكات الحاسوبية من خلال تخطي أنظمة الأمان
- التجسس - برامج تتعقب المعلومات الشخصية للأشخاص وترسلها إلى أطراف أخرى
- التصيد الاحتيالي - موقع مزيف على شبكة الإنترنت يبدو كأنه موقع حقيقي

تقدم الحكومات والشركات المساعدة للمستخدمين عبر الإنترنت لحمايتهم من الوقوع كفريسة للجرائم الالكترونية، والشكل ٢ الوارد أدناه عبارة عن مثال من "سلطة دبي للخدمات المالية" لتقديم النصيحة للمستخدمين بشأن كيفية تجنب تعرض أموالهم للسرقة بالإحتيال، كل ما عليك فعله هو أن تدخل على الموقع وتنقر فوق الرابط للحصول على مزيد من المعلومات، هذه الصفحة متوفرة باللغة الإنجليزية فقط (https://www.dfsa.ae/Your-Resources/DFSA-Alerts/How-to-avoid-being-scammedisp.state.il.us/crime/avoidscamtips.cfm)



ILLINOIS STATE POLICE

INTEGRITY SERVICE PRIDE

Leo P. Schmitz, Director

Tips to Avoid Being Scammed

The object of any con game is to entice an unsuspecting person to part with their money or other items of value. Most con games are initiated by people who approach potential victims on the street or call them on the phone.

Each person should be suspicious of ANY plan, idea, scheme, business deal, or any proposition that requires you to provide your money on short notice. The following tips are intended to improve your chances of not being a con's next victim:

- **REALIZE** scam artists are professionals - everyone is a potential victim.
- **SUSPECT** all "Get Rich Fast" schemes.
- **ALWAYS** lock your doors when doing yard work, getting the mail, or anytime you go outside - both the front and back doors.
- **NEVER** allow strangers inside your home.
- **ASK** "officials" to produce identification, and confirm their alleged employment.
- **CONTACT** the utility company by telephone if any purported city employee wants to enter your home, or requests you to go outside with him/her.
- **DISPLAY** "No Solicitation" and "Beware of Dog" signs near your residence door.
- **BE WARY** of any unexpected contact with strangers (in person or on the telephone).
- **SUSPECT** all "Door to Door" sales solicitations.
- **BEWARE** of unsolicited home repairmen. If you need the services of a home repairman, check first with the county, township, city building officials, the Better Business Bureau, or Office of the Illinois Attorney General to confirm they are legitimate. Be suspicious of anyone knocking at your door asking to make repairs to your home and/or asking to pave or seal your driveway.
- **CHECK** the Better Business Bureau to see if complaints have been filed against the person or business you are considering.
- **ASK** for references and call them.
- **GET** several repair estimates and compare prices.
- **TALK** with a trusted friend or relative before making major money decisions.
- **BE SUSPICIOUS** of high pressure sales tactics.
- **PAY BY CHECK** so you can stop payment if dissatisfied; NEVER PAY CASH.
- **PRINT "Deposit Only"** on the back of personal checks to create a "paper trail".
- **BE SURE** the work is completed to your satisfaction before you make final payment.
- **REQUIRE** a guarantee on the work.
- **REMEMBER**, you have **three days** to cancel a contract for home repairs if you signed the contract at your home.
- **NEVER** sign any contract or agreement without carefully checking it.
- **BE SURE** you understand and agree to all provisions in a contract or agreement.
- **WRITE DOWN** the license plate number of any suspicious vehicle(s) the suspect(s) may be operating.

- **CALL YOUR LOCAL LAW ENFORCEMENT AGENCY TO REPORT THE INCIDENT!!!**

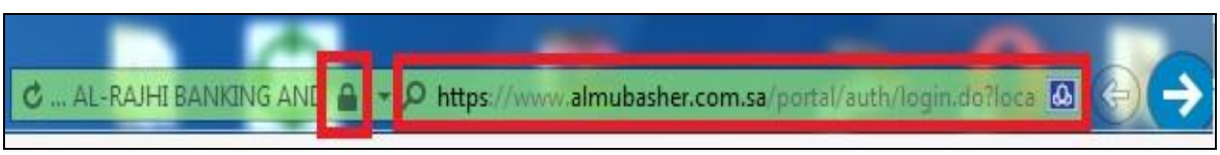
الشكل 2: سلطة دبي للخدمات المالية، كيفية تجنب التعرض للاحتيال

3-1-1-2 استيعاب معنى سرقة الهوية وماهية المخاطر

يقصد بسرقة الهوية أن يتم سرقة بياناتك الشخصية (مثل اسمك أو تاريخ ميلادك أو عنوانك الحالي أو السابق) ويتم تزوير الهوية عندما يستخدم شخص آخر هذه البيانات في عمل إجرامي، فإذا وقعت ضحية لسرقة الهوية، قد يؤدي ذلك إلى تزوير هويتك مما قد يكون له تأثير مباشر على عائلتك من الناحية المالية، ويجعل من الصعب عليك القيام بأعمالك الروتينية كاستخدام بطاقة الائتمان الخاصة بك حتى يتم حل هذه المشكلة، حيث يمكن للمحتالين استخدام بيانات والديك الشخصية لفتح حساباتهم البنكية أو الحصول على بطاقات ائتمان أو قروض أو طلب بضائع دون الحصول على موافقة والديك، ومن ثم فإنك قد تُنبأ لأول مرة بحدوث ذلك الفعل عندما تتلقى إيصالات أو فواتير خاصة بأشياء لم تطلبها، أو عندما يطلب منك محصلو الديون سداد ديون ليست عليك.

لحماية والديك اجعل الأنشطة التالية عادة منتظمة:

- مزق أي مستندات تحتوي على بيانات شخصية أو مالية قبل أن تتخلص منها.
- في حالة تلقي رسائل بريد إلكتروني غير عادية من إحدى المؤسسات وكانت الرسائل تطلب منك معلومات أمان خاصة بك, فلا تفصح عن كلمة المرور أو بيانات تسجيل الدخول بالكامل.
- إذا راودك الشك والقلق إزاء مصدر مكالمة هاتفية تدّعي أنها من البنك الذي تتعامل معه، أنهي المكالمة، ثم اطلب من والديك أن يتصلا بالبنك مرة أخرى.
- تحقق من التقارير البنكية والمالية الخاصة بك بعناية وأبلغ البنك الذي تتعامل معه أو مزود الخدمات المالية عن أي شيء تشتبه به.
- تخلص من أجهزة الكمبيوتر أو الهواتف الذكية القديمة بتحطيم القرص الصلب تمامًا.
- التزم بقواعد الخصوصية على مواقع التواصل الاجتماعي.
- توخ الحذر عند إرسال معلومات شخصية عبر الإنترنت أو عبر هاتفك الذكي.
- احذر من أي شخص يطلب منك بيانات تتعلق بالبنك الذي يتعامل معه والديك أو بطاقة الائتمان الخاصة بهما.
- لا تستخدم سوى المواقع الآمنة عند التسوق عبر الإنترنت، حيث يجب أن تحمل المواقع الآمنة رمز القفل أو عنوان URL يبدأ بـ (https) حتى يتسنى لك معرفة إمكانيةإدخال التفاصيل الخاصة بك بثقة (انظر المثال الموجود بالشكل 3 أدناه).
- عند اختيار كلمة مرور، تجنب استخدام الخيارات الواضحة مثل اسم الأم أو الحيوان الأليف أو غيرها من الخيارات التي يمكن لأي أحد تخمينها أو العثور عليها بسهولة, وحاول أن تستخدم مجموعة عشوائية من الحروف الكبيرة والصغيرة والأرقام.



الشكل 3: متصفح Internet Explorer - مثال لرمز القفل

4-1-1-2 تجنب عمليات الاحتيال والخداع مثل: التصيد الاحتيالي وتزوير العناوين والقرصنة

التصيد الاحتيالي هو نوع من أنواع الاحتيال الذي يستهدف المعلومات, ومثال ذلك أن تتسلم أنت وآلاف من الناس رسالة بريد إلكتروني تبدو أنها من البنك الذي تتعامل معه أو إحدى شركات الدفع عبر الإنترنت، ولا يهم ما إذا كنت تعرف هذه الشركة أم لا، فهناك احتمالات بأن تكون جزءًا من قائمة بريدية كبيرة، وتوضح رسالة البريد الإلكتروني أن الشركة قامت بتحديث نظامها الخاص وتطلب منك تأكيد معلومات تسجيل الدخول الخاصة بك، ويوجد بالرسالة رابط يحولك إلى موقع ويب غير الموقع الحقيقي، **!**لكن ليس هناك موقع حقيقي**!** وفي نهاية المطاف يتم تحويلك إلى موقع إلكتروني احتيالي مشابه تمامًا للموقع الأصلي حيث يتم تسجيل كل شيء تكتبه بما في ذلك اسم المستخدم وكلمة المرور، وبذلك يمكن للّص أن يدخل على حسابك، وعندئذٍ ينبغي عليك إثبات أن شخصا آخر كان يستخدم اسم المستخدم وكلمة المرور الخاصين بك دون إذنك.

سوف تخاطبك رسائل البريد الإلكتروني الحقيقية باسمك وليس باسم "عزيزي العميل" أو ما شابه، أما رسائل التصيد الاحتيالي فتحتوي في أغلب الأحيان على أخطاء إملائية ونحوية، كما أن الرابط الموجود في الرسالة سوف يوجهك عادةً إلى عنوان URL يختلف عن العنوان الموضح في الرسالة.

أدى التزايد المستمر في عدد الأشخاص المستخدمين لشبكات التواصل الاجتماعي في العالم إلى سلسلة من الانتهاكات الأمنية وحيل التصيد فيما يتعلق بالحسابات البنكية، فقد حدث وأن أصدر بنك "إتش إس بي سي" تحذيرات تتعلق بمجرم يرغب في معرفة البيانات البنكية وبيانات بطاقة الائتمان الخاصة بشخص ما وكلمات المرور والمعلومات المالية المخزنة على جهاز الكمبيوتر الشخصي أو المحمول أو الهاتف الذكي الخاص بك.

يتجه المتصيدون (الذين يرسلون رسائل تصيد) في أوروبا والشرق الأوسط وأفريقيا إلى طرق احتيال أكثر تطورًا مثل التصيد الاحتيالي الموجه الذي تتلقى فيه رسالة بريد إلكتروني تبدو مرسلة من شخص تعرفه، لكنها في الواقع مرسلة من مجرم يرغب في معرفة البيانات البنكية وبيانات بطاقة الائتمان الخاصة بك وكلمات المرور والمعلومات المالية المخزنة على جهاز الكمبيوتر الشخصي أو المحمول أو الهاتف الذكي الخاص بك.

توخّ الحذر واحرص على عدم إرسال كثير من المعلومات الشخصية على مواقع التواصل الاجتماعي، فإذا أرسل صديق لك رسالة بريد إلكترونية يطلب منك معرفة كلمة المرور أو معلومات أخرى، فاتصل بهذا الصديق أو أرسل إليه رسالة منفصلة للتحقق من صحة الرسالة.

وتزوير العناوين يتم عندما يتسلل أحد المجرمين إلى موقع إلكتروني حقيقي ويعمل على إعادة توجيه جميع الزوار إلى موقع مزيف مشابه لهذا الموقع تمامًا بحيث يقتنع المستخدم بأنه موقع حقيقي ويمكن خداعه حتى يقدم معلومات شخصية،وحتى لو أدخلت عنوان موقع حقيقي في متصفح الإنترنت، يمكن لهجمات تزوير العناوين أن تعيد توجيهك إلى الموقع المزيف.

والقرصنة تعني الدخول على الأنظمة الحاسوبية للآخرين عن طريق كسر نظام الأمان، وكان القراصنة في السابق يقومون بهذه الأعمال ليثبتوا قدرتهم على فعلها وليظهروا مدى مهارتهم، لكنهم يركزون الآن على سرقة المعلومات الشخصية والمالية،وتعد القرصنة غير المرخص بها جريمة في معظم الدول.

وفيما يلي مثال لأحد حوادث القرصنة الشهيرة البارزة:
تسلل القراصنة إلى نظام الكمبيوتر الخاص بمدرستهم لتغيير درجات وجداول 300 طالب

انظر الشكل 4 أدناه لقراءة القصة كاملة على الموقع الإلكتروني لصحيفة ديلي ميل.
(http://www.dailymail.co.uk/news/article-3281805/Three-students-charged-hacking-school-computer-change-grades-schedules.html)

الشكل 4: صحيفة ديلي ميل: 3 طلاب متهمون بالتسلل إلى نظام الكمبيوتر الخاص بمدرستهم

1-2 الحماية

2-1-2 المصادقة

1-2-1-2إدراك مفهوم المصادقة على دخول المستخدم

المصادقة على دخول المستخدم هي وسيلة لفحص هوية المستخدم والتحقق من أنه مسموح له بالدخول على خدمة مقيدة، وغالبًا ما تستخدم المصادقة معلومات سرية، فعندما ترغب في الدخول على الخدمة المقيدة، يتعين عليك إدخال اسم مستخدم يعرّف هوية الشخص وكلمة مرور تؤكد أن المستخدم هو صاحب الحساب، انظر الشكل 5 الذي يوضح شاشة تسجيل دخول المستخدم على موقع تويتر، وفيها يتطلب إدخال اسم المستخدم وكلمة المرور.

الشكل 5: تسجيل دخول المستخدم على موقع تويتر

2-1-2-2 معرفة آليات وضع ممارسات جيدة لتعيين كلمات مرور من حيث طول كلمة المرور والرموز الأبجدية الرقمية وتكرار التغيير

يجب أن تكون كلمات المرور مكونة من سبعة رموز على الأقل وتحتوي على مزيج من الحروف الكبيرة (A - Z) والحروف الصغيرة (a - z) والأرقام (0 - 9) والرموز الخاصة (&)،?_ ،! ،$ ،# ،(% or ، وكلمة المرور الجيدة هي التي لا تتكون من كلمة، بل تتكون من مجموعة رموز يسهل عليك تذكرها، أما كلمة المرور الضعيفة فتتألف إما من أسماء أفراد العائلة أو أسماء الحيوانات أو الفرق الرياضية أو أي شيء يمكن لأي شخص يعرفك تخمينه.
ملاحظة: لا يسمح دائمًا باستخدام الرموز الخاصة (&)،?_ ،! ،$ ،# ،(% or في كلمات المرور على جميع المواقع الإلكترونية نظرًا لقيود النظام.

لا تستخدم نفس كلمة المرور لعدة حسابات مختلفة، ومن الممارسات الجيدة أيضًا تغيير كلمة المرور على نحو منتظم، وتغيير كلمات المرور المرتبطة بالعمل بشكل متكرر.

3-2-1-2 فهم معنى المصادقة الثنائية: الرموز والبطاقات الذكية والمقاييس الحيوية

تنقسم أساليب التحقق من هوية شخص ما إلى ثلاث فئات هي: شيء تعرفه (*عامل المعرفة*)، شيء تمتلكه (*عامل الملكية*)، شيء يمثلك (*عامل الملازمة*)، وتسمى هذه الفئات مجموعات عوامل المصادقة.

- الشيء الذي تعرفه يمكن أن يكون كلمة مرور أو رقم تعريف شخصي PIN أو تاريخ ميلاد أو اسم الأم.
- الشيء الملموس الذي تملكه قد يكون بطاقة ATM أو بطاقة ذكية أو رمز أمان.
- الشيء الذي يمثلك (المعروف أيضًا باسم المقاييس الحيوية) قد يكون بصمة إصبع أو تعرف على الوجه أو بصمة صوت.

يجب أن يتألف العاملان من مجموعتان مختلفتان، وتعتبر المصادقة ثلاثية العوامل هي الأقوى وتعني وجود عامل من كل مجموعة،أما المصادقة الثنائية فهي الأكثر شيوعًا، إلا أن العاملَين يجب أن يكونا من مجموعات عوامل مختلفة، ولتعزيز الأمان ينبغي عليك الجمع بين عاملين على الأقل (شيء تعرفه [رمز PIN] مع شيء تملكه [بطاقة ATM]) مما يزيد من حمايتك من الاحتيال.
غالبًا ما تستخدم البنوك اجهزة صغيرة مزودة بلوحة ارقام وشاشه تعمل على انشاء رموز الحماية كذلك المبين في الصورة ادناه. حسث يستخدم كعامل مصادقة اخر، ويكون الرمز المعطى بواسطه هذه الاجهزة ذو صلاحية للاستخدام لمرة واحدة فقط.

2-1-3 مكافحة الفيروسات

2-1-3-1 استيعاب معنى مصطلح فيروس والتمييز بين الأنواع المختلفة من الفيروسات مثل الديدان وأحصنة طروادة

فيروس الكمبيوتر هو برنامج يمكنه إعادة نسخ نفسه والانتقال من جهاز كمبيوتر لآخر عبر الشبكات، كما يمكنه تدمير النظام المضيف عن طريق تدمير البيانات أو إرسال بيانات إلى أنظمة أخرى، إضافة إلى قدرته على إرسال نفسه إلى أي شخص موجود في سجل عناوين البريد الإلكتروني الخاص بك ثم تكرار الضرر، ولمكافحة الفيروسات يمكنك استخدام برامج مكافحة الفيروسات ومكافحة التجسس التي ستساعدك على ذلك، لكن يجب تحديثها بشكل منتظم لضمان الحماية.

البرامج الخبيثة هي برامج ضارة يستخدمها القراصنة لمهاجمة الأنظمة الحاسوبية، وتعتبر الديدان وأحصنة طروادة من الأمثلة الاكثر شيوعا على تلك البرامج.

ديدان الحاسوب هي برامج ضارة لها القدرة على نسخ نفسها والانتشار عبر شبكات الكمبيوتر إضافة إلى إنشاء رسائل بريد إلكتروني تحتوي على نسخ من نفسها، وتعمل هذه البرامج على إتلاف موارد النظام وإبطاء المهام الأخرى أو إيقافها، ويمكن أيضًا أن تفتح مدخلاً للقراصنة للتحكم في الكمبيوتر، وتجدر الإشارة إلى أن مصطلح "ديدان الحاسوب" تم اقتباسه من قصة الخيال العلمي The Shockwave Rider التي كتبها جون برونر عام 1975، حيث تحكي هذه القصة عن إحدى الحكومات التي تتحكم في مواطنيها من خلال شبكة حاسوبية قوية فقام أحد المناضلين من أجل الحرية بغزو الشبكة عن طريق برنامج يسمى "tapeworm" مما اضطر الحكومة إلى إيقاف تشغيل الشبكة وبالتالي تدمير مركز قوتها.

حصان طروادة هو نوع آخر من البرامج الضارة التي لا تنسخ نفسها بل يتم تحميله على جهاز الكمبيوتر عن طريق التظاهر بأنه برنامج عادي مثل الألعاب أو البرامج المجانية، وبمجرد تحميله، يستقر في الخلفية ويمكن استخدامه لإرسال رسائل بريد إلكتروني غير مرغوب فيها (عشوائية) أو لفتح مدخل، وقد تم اقتباس مصطلح "طروادة" أو "حصان طروادة" من قصة الحصان الخشبي المذكور في الأساطير اليونانية والذي خدع مدافعي مدينة طروادة عن طريق حمل المحاربين المختبئين إلى داخل المدينة، وبذلك تبدو هذه الأحصنة وكأنها غير ضار بل وكأنها هدايا نافعة بغرض إقناع الضحايا بتثبيتها على أجهزة الكمبيوتر الخاصة بهم، وتتضمن بعض العمليات التي يمكن للقرصان تنفيذها باستخدام حصان طروادة حصول القرصان على إمكانية الدخول عن بُعد وسرقة البيانات وجعل الكمبيوتر يتسبب في إتلاف الملفات أو تعديلها أو حذفها أو رصد لوحة المفاتيح،ومن هذه البرامج على سبيل المثال Netbus وSub7وBeastوZeusوProRatوZeroAccess، وتجدر الإشارة إلى أن برنامج رصد لوحة المفاتيح هو جهاز أو برنامج حاسوبي يعمل على تسجيل النشاط الفعلي للمستخدم بما في ذلك المفاتيح التي يضغط عليها في لوحة المفاتيح.

بعض الأنواع الأخرى لبرامج الفيروسات:

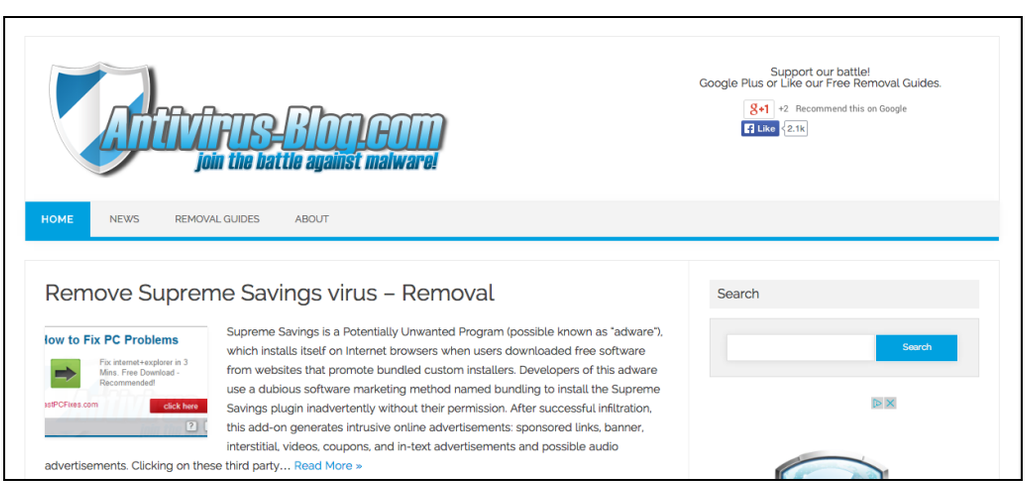
- **القنابل المنطقية/القنابل الموقوتة** - هي فيروسات مبرمجة للعمل في موعد محدد.
- **فيروسات الماكرو** - هي فيروسات تستخدم لغة برمجة ماكرو في تطبيق آخر لنشر نفسها، وتصيب ملفات MS Word أو MS Excel و عادة ما تنتشر إلى ملفات أخرى مماثلة.
- **الفيروس متعدد الأشكال** - هو فيروس لا يقوم فقط بنسخ نفسه بإنشاء ملفات عديدة مماثلة، بل يعمل أيضًا على تغيير التوقيع الرقمي الخاص به كل مرة ينسخ نفسه فيها.

2-3-1-2 استيعاب الغرض من برامج مكافحة الفيروسات

تستخدم **برامج مكافحة الفيروسات** لمنع البرامج الضارة بما في ذلك فيروسات الكمبيوتر والديدان وأحصنة طروادة من على أجهزة الكمبيوتر العادية والمحمولة واللوحية والهواتف الذكية واكتشافها وإزالتها،وينبغي تثبيت برنامج لمكافحة الفيروسات على كل جهاز كمبيوتر أو هاتف ذكي،فبرامج مكافحة الفيروسات تفحص الأقراص الثابتة لاكتشاف البرامج الضارة ويمكنها إزالة الفيروسات والفيروسات المتنقلة أو عزلها ويشار إلى هذه العملية أحيانًا باسم التطهير، ويعمل برنامج مكافحة الفيروسات عن طريق تحديد أنماط الملفات ونشاطها مما يكشف عن أي نوع من أنواع الهجوم على الجهاز باستهداف أي من الملفات المخزنة على الجهاز

وهناك عدة برامج مختلفة لمكافحة الفيروسات بعضها مجاني ولكن معظمها غير مجاني، فعندما تقوم بشراء برنامج لمكافحة الفيروسات، ينبغي أن تدفع مقابل الحفاظ على تحديثه، ومع ذلك تتيح بعض الشركات الموردة نسخة مجانية من برامجها للاستخدام الشخصي إلا أنها تحتوي على وظائف أقل من النسخة المدفوعة،وينبغي تحديث البرامج كل بضعة أيام على الأقل لضمان حماية الكمبيوتر الشخصي أو المحمول أو اللوحي أو الهاتف الذكي الخاص بك ضد أحدث البرمجيات الخبيثة.

كما أن مواقع مدونة مكافحة الفيروسات تزود المستخدمين بأحدث المعلومات عن الفيروسات، على سبيل المثال، قم بزيارة موقع Antivirus-Blog.com أو (http://www.antivirus-blog.com) للحصول على مزيد من المعلومات وأحدث مشاركات الأخبار الأمنية، انظر الشكل 6:



الشكل 6: مدونة مكافحة الفيروسات - antivirus-blog.com

3-3-1-2 استيعاب ضرورة المواظبة على تحديث برنامج مكافحة الفيروسات

تتعرف معظم برامج مكافحة الفيروسات على الفيروسات بالبحث عن أنماط معروفة من رموز البرمجة داخل الملفات وتعرف هذه الأنماط باسم توقيع الفيروس، ومن المعروف أنه يتم إصدار فيروسات جديدة باستمرار، ولذا يجب على منتجي برامج مكافحة الفيروسات تحديث برامجهم بشكل دائم لمواجهة التهديدات الناجمة، وعادةً ما يتم تحديث برامج مكافحة الفيروسات تلقائيًا إضافة إلى تحديث الشركات المنتجة لهذه البرامج المخزنة على جهاز الكمبيوتر الشخصي أو المحمول أو اللوحي أو الهاتف الذكي الخاص بالمستخدم لضمان وجود أحدث المعلومات المتعلقة بالفيروسات ومن حماية بيانات المستخدم.

4-3-1-2 التعرف على عمل جدار الحماية ومدى أهميته

عند توصيل جهاز كمبيوتر بالإنترنت يظهر هذا الجهاز لكل جهاز متصل بالإنترنت، وعندما تتصل بالإنترنت يتم تعريف جهازك برقم مميز يسمى عنوان IP (بروتوكول الإنترنت) ويمكن أن يظهر لأي شخص آخر متصل بالإنترنت.

وقد تكون هذه فرصة سانحة للأشخاص الراغبين في الوصول إلى معلوماتك وبياناتك الشخصية لإساءة الاستخدام، ويعتبر جدار الحماية نظام قائم على البرامج أو الأجهزة للتحكم في تدفق المعلومات عبر شبكات الكمبيوتر عن طريق التحقق من مصدرها ووجهتها ونوعها ومقارنتها بالقوائم المحددة مسبقًا الخاصة بالعمليات المسموح بها وغير المسموح بها، ويعمل على حظر الوصول إلى جهاز الكمبيوتر الخاص بك أو السماح به مما يوفر لك مزيدًا من الأمان، حيث يمكنه إخفاء جهازك من على الإنترنت إضافة إلى المحاولات غير المشروعة للوصول إلى جهاز الكمبيوتر والبيانات الخاصة بك.

1-2 الحماية

4-1-2 مكافحة التجسس

1-4-1-2 استيعاب مصطلح برامج التجسس والمخاطر المرتبطة بها

برامج التجسس هي برامج ضارة تعمل على جمع معلومات عن استخدام الكمبيوتر دون علمك، ويمكن أن تأتي مجمعة في صورة عنصر مخفي في البرامج المجانية التي يتم تنزيلها من الإنترنت ويمكن أن تقوم بتتبع تحركاتك على الويب لأغراض إعلانية، وقد تشتمل بعض برامج التجسس على "راصد ضربات لوحة المفاتيح" لمعرفة كلشيء يتم إدخاله بواسطة لوحة المفاتيح، وهو الأمر الذي يتضمن تسجيل كلمات المرور وأرقام بطاقات الائتمان ثم إرسال المعلومات للمجرمين، وتجدر الإشارة إلى أن راصد ضربات لوحة المفاتيح هو جهاز أو برنامج حاسوبي يعمل على تسجيل النشاط الفعلي للمستخدم بما في ذلك المفاتيح التي يضغط عليها في لوحة المفاتيح،ويمكن لمعظم برامج مكافحة الفيروسات إزالة برامج التجسس.

2-4-1-2 معرفة كيفية تشغيل برامج مكافحة التجسس وكيفية إزالة برامج التجسس من الكمبيوتر

يشبه تشغيل برامج مكافحة التجسس تشغيل أي من برامج مكافحة الفيروسات، وعادةً ما يتم تشغيل هذه البرامج في الخلفية لترصد أي نشاط مشبوه.

تمرين - إجراء فحص باستخدام برنامج لمكافحة التجسس

لإجراء فحص يلزمك أولاً التأكد من تثبيت برنامج لمكافحة التجسس على جهاز الكمبيوتر الخاص بك.
1- ابحث عن رمز برنامج مكافحة الفيروسات على شريط المهام، فقد يكون مضافاً الى الشريط.
2-اضغط على رمز البرنامج على شريط المهام.
3-اختر Scan (فحص) أو Scan Now (فحص الآن) من القائمة.
4-اضغط على Full Scan (فحص كامل)، ثم OK (موافق).
إذا عثرت على أي برنامج تجسس، فسيكون أمامك خيارات إما بحذف هذا البرنامج الضار أو نقله أو عزله.

3-4-1-2 التعرف على علامات التحذير التي تشير إلى احتمالية وجود برنامج تجسس على جهازك

قد يشير أحد الأمور التالية أو كلها على أن جهازك مصاب ببرنامج تجسس:

- تغير الصفحة الرئيسية المحددة في المتصفح إلى موقع غير معروف دون علمك.
- حدوث أعطال في الجهاز أو توقفه مع أنك لم تقم بتغيير أي شيء مؤخرا.
- ظهور رسائل بريد إلكتروني غريبة في مجلد "الرسائل الصادرة" لم تقم بإرسالها.
- ملاحظة كثير من الإعلانات المنبثقة عند التصفح.
- عمل القرص الصلب حتى في حالة عدم عملك على جهاز الكمبيوتر، أو عمل القرص ببطء شديد أثناء استخدامه.
- وجود كثير من أشرطة الأدوات في المتصفح مع عدم إمكانية إزالتها.
- إجراء بحث على شبكة الإنترنت وقيام محرك بحث أو متصفح آخر باستكمال هذا البحث.
- ظهور ملفات غامضة على نظام الكمبيوتر الخاص بك

عندما تشك في إصابة جهازك ببرامج تجسس، ادخل على برنامج مكافحة التجسس وقم بإجراء فحص، وسوف يمكنك هذا الإجراء من التعرف على برنامج التجسس ويتيح لك خيارات إما بحذفه أو نقله أو عزله.

اختبار

س1- بعد سرقة الكمبيوتر المحمول الخاص بك تم إجراء سحب غير متوقع من بطاقة الائتمان الخاصة بوالدتك. فما الذي حدث؟

أ- تصيد احتيالي
ب- تزوير عناوين
ج- سرقة هوية
د- استخدام برامج تجسس

س2- وصلت رسالة بريد إلكتروني إلى صندوق الوارد الخاص بأخيك الأكبر، ويبدو أنها من البنك حيث تطلب منه إعادة إدخال بيانات كلمة المرور إلا أن بها أخطاء نحوية وإملائية وراودك الشك بشأنها. ماذا يحتمل أن يكون ذلك؟

أ- محاولة تصيد احتيالي
ب-فيروس
ج- محاولة قرصنة
د- خدعة

س3- أي كلمات المرور أكثر أمانًا؟

أ-latitude
ب-Lat1tude3#
ج- LATITUDE
د-latitude5

س4-ما هي طريقة المصادقة التي تعتمد على القياسات الحيوية؟

أ- رمز PIN
ب- بطاقة ATM
ج- بصمة الإصبع
د- اسم الأم

الإجابات في الصفحة التالية

الإجابات

س1-ج- سرقة هوية
س2-ب- محاولة تصيد احتيالي
س3-ب-Lat1tude3#
س4-ج- بصمة الإصبع

الفصل 2-2

الأمان

2-2-1 النسخ الاحتياطي

2-2-2 البريد الإلكتروني

2-2-3 الشبكات اللاسلكية

2-2-4 الأمن المادي للأجهزة

2-2-5 الأجهزة الذكية

2-2 الأمان

2-2-1 النسخ الاحتياطي

2-2-1-1فهم معنى النسخ الاحتياطي وأسباب أهميته

النسخ الاحتياطي هو عبارة عن عمل نسخ احتياطية من البيانات الخاصة بك لاسترجاعها في حالة فقدانها، حيث تفقد البيانات للعديد من الأسباب التي منها: الحذف عن طريق الخطأ، وتعطل الأجهزة ، والمخاطر الطبيعية مثل أضرار النار والماء، وهجمات الفيروسات،والسرقة أو الفقدان، وغيرها الكثير، فالحذف عن طريق الخطأ يضع المحذوفات في سلة المهملات مما يتيح استرجاعها بكل سهولة ويسر، أما الحف العمد فيجعل مهمة استرجاعها مستهلكة للوقت مع عدم ضمان نجاح تلك العملية،وفي حال تم حذف الملفات إثر هجوم للفيروسات، فهناك فرصة ضئيلة جدًا لاسترجاعها مرةً أخرى، إذ أن الأقراص الصلبة تخفق في بعض الأحيان، وفي حال إخفاق الجهاز؛ ستتطلب عملية استعادة البيانات مساعدة أحد المحترفين، مما يكلف تكلفة باهظة.

ينبغي أن تطبق مدرستك إجراء النسخ الاحتياطي والذي يضع خطة منتظمة من النسخ والنسخ الاحتياطي لملفات البيانات والبرامج الهامة، وتغطي إجراءات النسخ الاحتياطي، التي تطبقها العديد من المدارس، المتطلبات الأساسية: البيانات والمعلومات والبرامج المدرسية الأساسية (بما في ذلك درجات الطلاب وسجلات حضورهم وغيرها من المعلومات الشخصية)، وإذا لم توفر مدرستك إجراء النسخ الاحتياطي للملفات التي تقوم بإنشائها في فصلك، فيوصى بعمل نسخ احتياطية من خطط التدريس وصفحات موارد المناهج الدراسية والاختبارات وغيرها من أنواع الملفات الأخرى التي تمثل سنوات من العمل الشاق.

إن فقدان البيانات شيءٌ لا يمكن التنبؤ به، لذا ينبغي لك دائمًا الاحتفاظ بنسخة احتياطية حديثة، وأفضل طريقة للتأكد من ذلك هي إعداد جدول منتظم للنسخ الاحتياطي، وكلما كانت عمليات النسخ الاحتياطي كثيرة؛ انخفض معدل فقد البيانات، فاستغراق بضع دقائق أسبوعيًا لإجراء ذلك أفضل من إعادة كتابة تقارير العمل الشهرية، أو فقدان جميع ملفاتك أو إعادة كتابة التقارير المرحلية لكل طالب في صفك.
كما أن معظم أجهزة الكمبيوتر الشخصية بها برامج نسخ احتياطي خاصة بها، الشكل 7 في الصفحة التالية يعرض مثالا لعملية النسخ الاحتياطي في Windows 7 والتي تعطيك معلومات حول خيارات النسخ الاحتياطي.

الشكل 7: مثال مدير النسخ الاحتياطي

2-1-2-2 التعرف على أجهزة النسخ الاحتياطي الشائعة مثل: تطبيقات التخزين السحابي ومشغلات USB ومشغلات الأقراص الصلبة الخارجية، ومعرفة السعات المختلفة

إن أسهل الطرق وأكثرها جدوى لعملية النسخ الاحتياطي للملفات خاصتك (الوثائق، الصور، وما إلى ذلك) هي أن تنسخ تلك الملفات على محركات فلاش USB أو محركات أقراص صلبة خارجية أو أحد تطبيقات التخزين السحابي, كما حجم محركات فلاش USB صغير ويمكنها تخزين معلومات يصل حجمها إلى عدد كبير من الجيجابايت، أما محركات الأقراص الصلبة الخارجية فهي خيار أغلى ثمنًا، إلا أنه يمكن استخدامها في عملية النسخ الاحتياطي لكافة المحتويات المخزنة على جهاز الكمبيوتر الخاص بك بما في ذلك محرك القرص الصلب بالكامل والبرامج ونظام التشغيل، وتُمكِنُك تطبيقات التخزين السحابي من التحميل والتخزين والوصول إلى البيانات على الإنترنت، على سبيل المثال، يمكنك حفظ أمر ما باستخدام الحوسبة السحابية على أحد الأجهزة ويمكنك الوصول إليه بسهولة عبر هاتفك.

يوضح الجدول 1 أدناه السعة التخزينية القصوى النموذجية لأجهزة التخزين الشائعة:

الجهاز	السعة التخزينية القصوى
محركات الأقراص الصلبة الخارجية	تصل إلى 2 تيرا بايت أو أكثر
محركات فلاش USB	تصل في الغالب إلى 128 جيجابايت
تطبيقات التخزين السحابي	تصل إلى 15 جيجا بايت مجانًا، وتتفاوت إذا كانت هناك حاجة لمزيد من المساحة

الجدول1 السعة التخزينية القصوى لأجهزة التخزين الشائعة

بغض النظر عن المكان الذي تحفظ فيه النسخ الاحتياطية لبياناتك، ينبغي لك حفظها في مكان مستقل عن مكانها الأصلي لأنه إذا ما نشب حريق أو جاء فيضان، على سبيل المثال، فمن الممكن أن تفقد البيانات الخاصة بك إذا تم تخزينها في مكان واحد.

3-1-2-2 استيعاب مفهوم النسخ الاحتياطي السحابي

الحوسبة السحابية هي استخدام موارد الكمبيوتر التي تكون في شكل خدمات عبر الشبكة، وعادة ما تكون الإنترنت، وهذا الاسم مشتق من الاستخدام الشائع للرمز المتخذ شكل سحابة، والمستخدم في تبسيط المواقف المعقدة،يدخل المستخدمون إلى التطبيقات السحابية عبر أحد المتصفحات أو تطبيقات الهاتف المحمول، ويتم تخزين بيانات المستخدم على خوادمٍ في موقع بعيدة،وعادةً ما يكون لدى المستخدمين حجم محدود من المساحة التخزينية الخالية، التي إذا ما نفذت؛ سيفرض موفرو الخدمة رسومًا إضافية،كما أن الخدمات المدفوعة توفر مساحة تخزينية أكبر ونَسخًا احتياطيًا خاصًا للبرامج من أجل أتمتة العملية،ويتميز التخزين السحابي بأنه غير مكلف - مجانيّ غالبًا - ويمكن الوصول إليها بسهولة من خلال مجموعة من الأجهزة، كما أنه يتضمن أنظمة نسخ احتياطي تلقائي وأنظمة استعادة، فضلا عن أنه مثالي لأغراض التعاون، بالإضافة إلى كونه أكثر أمانًا بسبب نقل النسخ الاحتياطية من الملفات الأصلية، جنبًا إلى جنب مع كونه غير مرئي وليس له وجود مادي ويسمح بالتحديثات التلقائية لملفاتك في كل الأجهزة الخاصة بك.

ومن أمثلة الخدمات المجانية ما يلي:Data Bagg "داتا باج" (https://www.databagg.com)،وDropbox "دروبوكس" (www.dropbox.com)،وGoogleDrive "جوجل درايف" (يمكن الوصول إليه من خلال حساب Gmail الخاص بك).

يوضح الشكل8 أدناه خدمة تسجيل الدخول إلى Data Bagg الذي من خلاله يمكن الوصول إلى الملفات خاصتك من أي مكان:

الشكل 8: التخزين السحابي - للتخزين السحابي ادخل على (https://www.databagg.com)

4-1-2-2استخدام خصائص النسخ الاحتياطي على جهاز الكمبيوتر الخاص بك، وفهم معنى "استعادة" النسخة الاحتياطية

تتضمن أنظمة التشغيل خيارات مختلفة لعمليات النسخ الاحتياطي، ويوضح لك التمرين التالي الخطوات المتبعة لإكمال عملية النسخ الاحتياطي لجهاز كمبيوتر يعمل بنظام Windows 7:

تمرين - إكمال عملية النسخ الاحتياطي لجهاز كمبيوتر يعمل بنظام Windows 7

1- اضغط على زر Start (بدء) ثم افتح Control Panel (لوحة التحكم).
2- اضغط الخيارBack up and Restore (النسخ الاحتياطى و الاستعادة)
3- اضغط الامر إعداد النسخ الاحتياطى
4- حدد جهاز التخزين الذي ترغب بحفظ النسخه الاحتياطية عليه ثم حدد المجلدات والملفات المراد نسخها.
5- اضغط على Backup Now (نسخ احتياطي الآن)

استعادة الملفات المنسوخة احتياطيًا

يمكن استعادة الملفات المنسوخة احتياطيًا المفقودة أو التالفة أو التي تغيرت بطريق الصدفة، كما يمكن استعادة الملفات الفردية أو مجموعات الملفات أو كافة الملفات التي نسختها احتياطيًا،ولإمكانية الاستفادة من خيار استعادة الملفات، يجب المواظبة على النسخ الاحتياطي.

2-2-2 البريد الإلكتروني

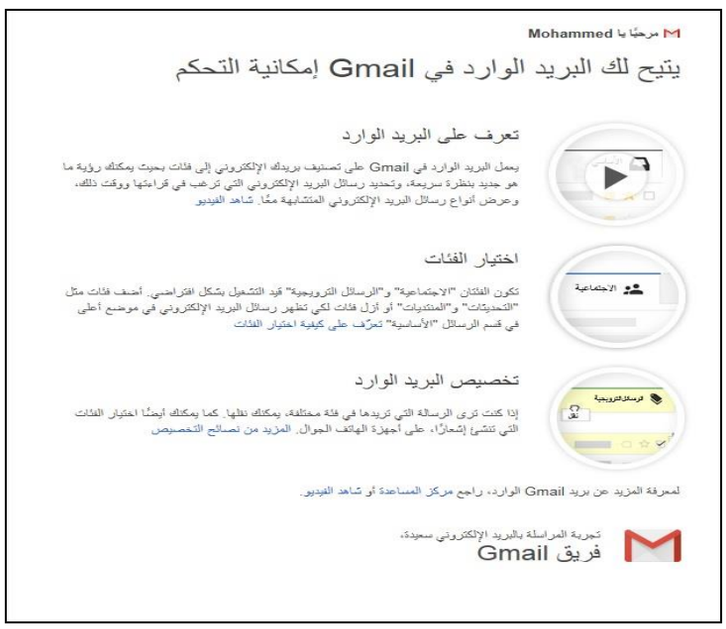
2-2-2-1 استيعاب مفهوم رسائل البريد الإلكتروني غير المرغوب فيها / المزعجة وضرورة تنقية البريد الإلكتروني

عادةً ما تكون رسائل البريد الإلكتروني المزعجة رسائل غير مطلوبة أو منشورات من مجموعة أخبار غير مرغوبة - وتكون في الأعم هي رسائل إلكترونية غير مرغوبة تستخدم في الإعلان عن أحد المنتجات أو الخدمات لإحدى الشركات أو المواقع الإلكترونية.

يقوم مزودو خدمة الإنترنت بحظر معظم الرسائل المزعجة قبل وصولها إلى صندوق الوارد باستخدام فلاتر الرسائل المزعجة التي تعتبر من ضمن البرامج القائمة على فرز الرسائل الواردة للبريد الإلكتروني لتحديد ومنع الرسائل غير المرغوب فيها / المزعجة من الوصول إلى صندوق الوارد، ومع ذلك فإن هناك الكثير من هذه الرسائل الإلكترونية تمر من هذه الفلاتر مما يؤدي إلى فقدان الرسائل الواردة من الأصدقاء أو الزملاء في صندوق الوارد، ولحسن الحظ، فإن معظم برامج البريد الإلكتروني يمكنها تنقية الرسائل غير المرغوب فيها بمجرد وصولها، كما أنك تستطيع وضع بعض الإعدادات لإرسال هذه الرسائل إلى المجلد الخاص بها، وبالتالي حجب الرسائل الإلكترونية المستقبلية الواردة من نفس المرسل.

2-2-2-2تفعيل عامل تصفية الرسائل المزعجة في البريد الإلكتروني

تتنوع طرق تفعيل فلاتر الرسائل المزعجة بحسب برنامج البريد الإلكتروني، ففي برنامج Windows Mail، انقر بالزر الأيمن على الرسالة واختر Junk Mail (البريد غير المرغوب فيه)، وبعد ذلك يمكنك وضع علامة على الرسالة لتكون من الرسائل غير المرغوب فيها، ومن ثمّ حظر رسائل البريد الإلكتروني الأخرى الواردة من المرسل أو من أي شخص آخر له نفس عنوان البريد الإلكتروني،كما أن معظم أنظمة البريد الإلكتروني بها خيارات لتنقية الرسائل المزعجة والحد منها، فيعمل Gmail على خفض الرسائل غير المرغوبة من خلال فلاتر البريد الإلكتروني الخاصة به، انظر الشكل 9 أدناه :



الشكل 9: Gmail - عدد أقل من الرسائل المزعجة

3-2-2-2 ضبط إعدادات تصفية الرسائل المزعجة

فور ضبط الفلاتر على حساب البريد الإلكتروني الخاص بك، يمكنك تلقائيًا وضع علامة على جميع الرسائل الواردة من مرسل بعينه أو التي تحتوي على كلمة معينة في سطر الموضوع، فالرسائل الموضوع عليها علامة يمكن حذفها تلقائيًا أو جعلها كمقروءة أو نسخها إلى مجلد معين.

2-2-3 الشبكات اللاسلكية

2-2-3-1 فهم ماهية الشبكات اللاسلكية أو شبكات الواي فاي

تعد شبكة "الواي فاي" أحد أنواع شبكة المنطقة المحلية اللاسلكية (WLAN)، حيث تستخدم هذه الشبكة عادةً لتوفير الاتصال بالإنترنت، فأي جهاز يدعم خاصية "الواي فاي" يمكنه الاتصال بالإنترنت عبر نقطة وصول الشبكة اللاسلكية، إذ أن كل نقطة وصول للشبكة اللاسلكية لها نطاق لاسلكي يبلغ 20 مترًا وتُعرف بنقطة الاتصال، ويمكن أن يكون جهاز الاتصال كمبيوتر شخصي أو كمبيوتر محمول أو هاتف لوحي أو هاتف ذكي أو وحدة طرفية للتحكم في ألعاب الفيديو، وجديرُ بالذكر أن تقنية "الواي فاي" تنتشر بصورة كبيرة في المقاهي والمطارات والعديد من الأماكن العامة، وغالبًا ما يتم توفير هذه التقنية مجانًا،ويوضح الشكل 10 مثالاً للأحياءالمتوفر بها هذه التقنية في مدينة لندن، حيث تم سرد هذه الأحياءفي قائمة وتم عرضها على خريطة.

الشكل 10: نقاط اتصال "واي فاي" في دبي
(http://www.wificafespots.com/wifi/city/AE--Dubai)

يمكن أيضًا تنزيل تطبيق الهاتف المحمول من هذا الموقع والذي يخزن مواقع نقاط الاتصال بشبكة "واي فاي".

2-3-2-2 التعرف على المزايا والمخاطر المرتبطة باستخدام نقاط اتصال "الواي فاي" العامة

تم توفير نقاط اتصال "الواي فاي" العامة على نطاق واسع في المناطق الحضرية، والبعض منها يتم توفيره مجانًا،وإذا كانت نقطة الاتصال قد تم توفيرها لأرباب المكان التجاري ذاته مثل المقهى، أو المطار، فربما يتم فرض رسوم على هذه الخدمة.

المميزات

- يمكن استخدام الكمبيوتر المحمول والهاتف الذكي الخاص بك للدخول على الإنترنت، فاستخدام الجهاز الخاص بك عند نقطة اتصال يمنحك وصولا سهلا إلى الشبكة العنكبوتية وكافة الحسابات الخاصة بك على الإنترنت.
- تعد نقطة الاتصال من الأماكن المناسبة لفحص البريد الإلكتروني الخاص لمعرفة آخر الرسائل المهمة الواردة أثناء التنقل، فمعظم المقاهي والحانات والمطاعم توفر نقاط اتصال، لذا يمكنك تناول المأكولات والمشروبات وأنت تتصفح الإنترنت.
- وجود نقاط الاتصال في المطارات من الأمور المهمة نظرًا لاحتياج الأشخاص للدخول إلى الإنترنت قبل ركوب الطائرة لأنهم سيضطرون إلى إغلاق أجهزتهم طوال مدة الرحلة.
- إذا كنت تمكث في أحد الفنادق المتوافر بها نقطة اتصال، يمكنك إذن استخدام الإنترنت في غرفتك دون الحاجة إلى الذهاب إلى مقهى إنترنت.

المخاطر

- يمكن التجسس على أية بيانات تُرسل عبر نقاط اتصال "واي فاي" عامة من قِبل أي شخص يقوم بتسجيل الدخول إلى الشبكة، حيث يستطيع معتادو الإجرام إعداد نقاط اتصال "واي فاي" وهمية مجانية في الأماكن العامة، ومن ثمّ استخدامها في سرقة المعلومات الشخصية، مثل أسماء المستخدمين وكلمات المرور.
- عادةً ما تكون شبكات "الواي فاي" العامة بدون حماية ويسهل التجسس عليها.
- إذا استخدم كثير من الأشخاص نقطة اتصال بعينها ستنوء الشبكة بالحمل الزائد، الأمر الذي يؤثر سلبًا على كفاءة الأداء مع احتمالية فقدان الاتصال.

2-3-2-3 التعرف على ميزات الحماية الخاصة باستخدام أحدث البروتوكولات اللاسلكية WEP أو WPA

يتم تأمين نقاط اتصال "الواي فاي" المحلية أو الخاصة عمومًا باستخدام كلمة مرور، والمسماة أيضًا مفتاح تشفير حماية الشبكات اللاسلكية لضمان وصول المستخدمين المصرح لهم فقط،وعملية التشفير تعني تحويل البيانات إلى شكل يصعب فهمه على الأشخاص غير المصرح لهم مثل القراصنة، ومع ذلك فإن معظم نقاط اتصال "الواي فاي" لا تقوم بتشفير البيانات التي ترسلها عبر الإنترنت وليست آمنة، فإذا كنت تستخدم تلك النقاط بانتظام للدخول على حساباتك الخاصة، يفضل استخدام شبكة خاصة افتراضية لتشفير عملية المرور بين جهازك والإنترنت.

ويوجد معياران لتشفير شبكات "الواي فاي"، معيار التشفير اللاسلكي - القياسي، والخصوصية السلكية المكافئة (WEP)، التي يمكن الوصول إليها بكل سهولة والمستبدلة أيضًا بأحد خيارات التشفير (WPA وWPA2) الخاص بالوصول المحمي للواي فاي.

كما أن إجراءات الحماية تساعد في ضمان الوصول إلى الإنترنت بأمان، بجانب الحفاظ الآمن على المعلومات الشخصية والبيانات.

2-2 الأمان

4-2-2 الأمن المادي للأجهزة

1-4-2-2 التعرف على اعتبارات الأمن الماديعند استخدام الكمبيوترالمحمول والأجهزة اللوحية

لا يقتصر الأمان عند استخدام الكمبيوتر المحمول أو اللوحي على كلمات المرور وعمليات النسخ الاحتياطي والتشفير، فنظرًا لحجم أجهزة الكمبيوتر المحمول واللوحي نرى أنها عرضة للضياع أو السرقة، فإذا ما تُركت داخل السيارة أو في نقاط اتصال "واي فاي" عامة دون مراقبة، فإنها تجذب انتباه اللصوص فيحملونها بسرعة ويهربون.

2-4-2-2 معرفة كيفية تقليل المخاطر المرتبطة بسرقة الجهاز أو فقدانه: إبقاء الجهاز نصب العينين، واستخدام سلك الحماية (إذا كان ذلك مناسبًا)، والتأمين بكلمة مرور، وتدوين الرقم التسلسلي، واستخدام الرسم بالأقلام السرية

هناك بعض الاحتياطات الأساسية الممكن اتخاذها لتقليل خطر فقدان الكمبيوتر المحمول عن طريق السرقة أو الإهمال.

- ضع الجهاز نصب عينيك واتركه في مكان مرئي للحيلولة دون سرقته، واحتفظ بوضع الجهاز في حوزتك طوال الوقت إن أمكن ذلك.
- اربط سلك الحماية أو شاشة خصوصية أو إنذار حماية بحاسوبك المحمول - لأن معظم اللصوص يبحثون عن الأهداف السهلة،الشكل 11 يوضح مثالاً نموذجيًا سلك الحماية (الاقفال):

الشكل 11: قفل حماية نموذجي مثبت بالكمبيوتر المحمول

- أضف لافتات واضحة باسمك، فهذا من شأنه الحيلولة دون احتمالية السرقة والمساعدة في استعادة الجهاز إذا ما حدث الأسوأ.
- تأكد أن كافة حسابات المستخدمين تتطلب كلمة مرور، للحيلولة دون دخول اللصوص إلى الكمبيوتر.
- ضع ملاحظة على رمز المنتج والرقم التسلسلي، ثم احتفظ بهما في مكانٍ آمن بخلاف حقيبة الكمبيوتر المحمول.
- اكتب معلومات الاتصال بك على الجهاز مستخدمًا قلمًا سرياً، والذي سيظهر أثره فقط تحت ضوء الأشعة فوق البنفسجية.

3-4-2-2التعرف على قضايا الحماية فيما يتعلق بالتخلص من أجهزة الكمبيوتر، وأهمية إزالة البيانات منها قبل التخلص منها

على الرغم من أننا ندخل معلومات شخصية على الكمبيوتر ثم نحرص على حذفها على الفور، إلا أن هناك احتمالاً قائمًا بإمكانية استرجاع هذه البيانات من الكمبيوتر من قبل شخص آخر باستخدام برامج استعادة البيانات المحذوفة حتى بعد تفريغ سلة المهملات، بل إن إعادة تهيئة القرص الصلب ربما لا تزيل كافة البيانات منه،حيث تظل بعض المعلومات على الجهاز الإلكتروني بما في ذلك رسائل البريد الإلكتروني القديمة والمحتويات المخفية في المتصفح، ولأنك لا تعلم من سيقتني جهازك مستقبلاً فإنك لا تعلم كيف سيتعامل مع هذه المعلومات.

إن أفضل طريقة للتأكد من عدم بقاء أي من بيانات شخصية على الكمبيوتر هي إزالة القرص الصلب وتدميره فعليًا، ولكن ذلك سيؤدي إلى توقف الكمبيوتر، ثم يأتي خيار استخدام برامج تقطيع الملفات التي منها برنامج File Shredder الذي يمكنه الكتابة الفوقية على المساحة الخالية من القرص كما هو الحال في المعايير العسكرية، انظر الشكل 12 أدناه الذي يوضح شاشة تنزيل برنامج File Shredder من موقع http://www.fileshredder.org.

الشكل 12: شاشة تنزيل برنامج File Shredder

2-2 الأمان

2-2-5 الأجهزة الذكية

2-2-5-1 التعرف على البيانات التي يحويها جهازك ويشاركها على الإنترنت وكيف يمكن أن يساء استخدامها

في هذه الأيام نادرًا ما يترك جهازك الذكي يديك، وبالتأكيد لا يترك عينيك معظم اليوم، وهذا يعني أن معاملاتك على مدار اليوم لها نصيب مع جهازك الذكي، كما يعني أنك تحفظ على الجهاز كثيرا من المعلومات مثل: الرسائل، ورسائل البريد الإلكتروني، والصور، والفيديو، والاتصالات، وكلمات المرور، والتطبيقات.

كما يمكن تبادل هذه المعلومات بسهولة عبر الإنترنت من خلال تطبيقات المراسلة والدردشة ورسائل البريد الإلكتروني، وأحيانا في الخلفية من خلال التطبيقات المثبتة على الجهاز, ويتم عرض المزيد من المعلومات حول التطبيقات التي تم تنزيلها في القسم 2-2-5-4, كما يمكن أن يساء استخدام المعلومات في الأيدي الخاطئة للتنمر، والإحراج، وارتكاب جرائم مثل سرقة الهوية.

من أمثلة هذه الجرائم أيضًا سرقة جهازك مما يسمح للص بالحصول على التفاصيل الشخصية الخاصة بك من خلال المعلومات المحفوظة غير المحمية, أو سرقة عنوانك الفعلي، أو الوصول إلى البريد الإلكتروني الخاص بك ما يوفر وسيلة سهلة وسريعة لإعادة تعيين كلمات المرور على أي حساب على شبكة الإنترنت، أو استخدام المعلومات السرية أو المالية الأخرى.

2-2-5-2 **التعرف على مميزات الأمان الأساسية: حماية الجهاز بكلمة المرور، إعداد خدمة القفل التلقائي، تثبيت برنامج حماية، تثبيت تحديثات نظام التشغيل، تتبع الهاتف المحمول**

من المثال السابق يتضح تماما أن استخدام مميزات الأمان الأساسية المدمجة يعد وسيلة لحماية المعلومات الخاصة بك، وقد ذُكر عدد قليل من هذه المميزات في هذا القسم، وهناك تطبيقات على شبكة الإنترنت توفير مزيداً من الأمن أيضًا.

أولا وقبل كل شيء، يجب حماية الجهاز بكلمة سر في أقرب وقت ممكن، حيث تجرى هذه العملية عادة من خلال قوائم Settings / Options (إعدادات / خيارات) بالجهاز الذكي الخاص بك، وتأكد من أن كلمة المرور قوية بما يكفي لتجنب اختراق الجهاز.

إن إعداد خدمة القفل التلقائي من خلال قائمة (إعدادات / خيارات) على الجهاز الذكي الخاص بك سوف ينشئ قاعدة لقفل الجهاز بعد فترة معينة من الزمن، كما تتاح بعض تطبيقات الأمان للتثبيت لقفل الجهاز بعد مغادرة مكان آمن معين مثل منزلك أو مكتبك، حيث يعد ذلك أداة عظيمة إذا سُرق الجهاز الذكي.

كما أن تحديث نظام تشغيل الجهاز الذكي يعد أمرًا مهمًا للأغراض الأمنية, حيث يتم توفير هذه التحديثات عند اكتشاف عيوب في البرنامج, فتقوم التحديثات بإصلاح هذه العيوب.

ويعد تتبع الهاتف المحمول خدمة أخرى هامة تساعد في تحديد مكان الجهاز الذكي الخاص بك، حيث يتم توفير هذه الخدمة من قبل الشركة المصنعة للهاتف الخاص بك، ويمكن لمطوري التطبيقات الآخرين توفير نفس الخدمة، فهذه الخدمة تتعرف على الموقع الحالي للجهاز الذكي باستخدام أبراج الراديو على شبكة الجهاز الذكي الخاص بك أو من خلال إشارة نظام تحديد المواقع (GPS) بالجهاز، وبمجرد التعرف على الموقع يمكنك الذهاب إليه (إذا كنت قد نسيت الهاتف في مكتبك)،

وفي بعض الأحيان توجد خيارات لقفل الجهاز أو مسح بياناته تماما (حذف كامل) حال الشك في سرقته.

3-5-2-2 معرفة كيف أن استخدام التشفير على هاتفك الذكي يمكن أن يساعد على منع سرقة البيانات

إن معظم الأجهزة الذكية بها خيار لتشفير البيانات، وتخزينها في شكل بيانات غير مقروءة ومجمعة, ففي الهواتف التي تعمل بنظام Android يجب إدخال رمز PIN فور تشغيل الهاتف, وما لم يكن شخص ما لديه كلمة المرور الصحيحة أو رمز PIN, فإن البيانات تكون غير قابل للاستخدام، وهذا سوف يساعد في حماية المعلومات الحساسة المخزنة على الجهاز, وفي كل مرة يتم فيها قفل الهاتف تبقى البيانات مشفرة حتى يتم إدخال كلمة المرور الصحيحة.

لاحظ أن استخدام التشفير سوف يبطئ أداء الجهاز الخاص بك بسبب الحمل المضاف على المعالج لتشفير المعلومات المخزنة وفك تشفيرها، ومع ذلك ينصح بتشفير البيانات الموجودة على أجهزة الشركات لحمايتها من التعرض للتجسس.

4-5-2-2التعرف على المسائل الأمنية المتعلقة بالتطبيقات، تنزيل التطبيقات من المصادر المعتمدة فقط، والتحقق من صلاحيات التطبيقات

إن تطبيقات الأجهزة الذكية لهي من أعظم اختراعات هذا القرن, وذلك لأننا نرى أن هناك بعض هذه التطبيقات مثل "واتس آب" "سناب شات" و"إنستاجرام" للمراسلة و"فيس بوك" و"تويتر" وغيرها تستخدم لجعل حياتنا أكثر راحة ومتعة، ولكن لسوء الحظ عندما يتم تثبيت هذه التطبيقات على جهازك فأنها قد تفتح بابًا للوصول إلى الجهاز والمعلومات المخزنة داخله.

فتنزيل التطبيقات من مصادر موثوقة مثل "متجر آي تيونز" لمنتجات "أبل" أو "متجر جوجل بلاي" لأجهزة الأندرويد يقلل من خطر وصول الأشخاص إلى الجهاز.

ولتوفير حماية إضافية ضد إساءة الاستخدام يتعين على كل مستخدم أن يتريث لقراءة وفهم صلاحيات التطبيقات المعتمدة قبل التثبيت، وفيما يلي مثال يوضح أحد التطبيقات المرخصة لتحديد موقع جهازك باستخدام النظام العالمي لتحديد المواقع (GPS) في أي وقت.

5-5-2-2 التعرف على الفيروسات الموجودة على أنظمة تشغيل الهواتف المحمولة والبرامج الخبيثة للهواتف المحمولة

البرنامج الخبيث المتنقل هو برنامج يستهدف الأجهزة المحمولة بقصد الضرر أو تسريب المعلومات السرية، ومثل كافة الأجهزة المتصلة بالإنترنت، فإن الأجهزة الذكية المحمولة الخاصة بك عرضة لهجمات الفيروسات والبرامج الخبيثة المماثلة لتلك التي تهاجم جهاز الكمبيوتر الخاص بك.

(http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/)

ما تزال البرامج الخبيثة المتنقلة تتزايد ولا يبدوا انها ستتباطأ، ذكر مقال "فوربس" أن 200 تهديدًا جديدًا يتم إنشاؤهم في كل دقيقة، ولذلك يفضل تثبيت تطبيقات مكافحة الفيروسات لحماية جهازك من مثل هذه الهجمات.

6-5-2-2 التعرف على التهديدات الأمنية القادمة عبر البريد الإلكتروني أو الرسائل النصية غير المرغوب فيها، والتعرف على أعراض الإصابة بالبرامج الضارة: رسوم بيانات غير عادية على الفاتورة، تغييرات غير مفهومة في واجهة المستخدم

تسمى رسائل البريد الإلكتروني والرسائل النصية غير المرغوب فيها باسم "رسائل البريد المزعجة"، وغالبًا ما تأتي هذه الرسائل مع محتوى إعلاني قد يكون ضارًا، بل وقد تحتوي هذه الرسائل على رابط لموقع إنترنت يمكن أن يكون ذا قصد جنائي، أو قد تحتوي على مرفق مدرج يمكن أن يكون فيروساً.

ومن الممكن تقسيم غالبية البرامج الخبيثة المتنقلة إلى ثلاث مجموعات رئيسية: ‘مجموعة "SMS Trojans" التي تستهدف الاجهزة المحمولة عن طريق الرسائل النصية القصيرة SMS إلى الأرقام المميزة، ‘ومجموعة Backdoors التي تتيح الوصول غير المصرح به إلى الأجهزة الذكية مما قد يسمح بسرقة البيانات أو تغيير الإعدادات أو تثبيت برامج

خبيثة، ‘ومجموعة ywareSp التي تجمع من الجهاز المحمول بعض البيانات التي قد تشمل الاتصالات أو كلمات المرور أو الصور أو الفيديوهات.

7-5-2-2معرفة كيفية إيقاف وظائف "الواي فاي" و"البلوتوث" التلقائية لمنع الوصول غير المصرح به إلى بيانات الجهاز الخاص بك

تعتبر تقنية البلوتوث إحدى التقنيات اللاسلكية منخفضة الطاقة والتكلفة لربط الأجهزة عبر مسافات قصيرة، ويستخدم عادة لربط سماعات الأذن بالهواتف المحمولة، فعند تشغيل البلوتوث على أحد الهواتف المحمولة من خلال Settings – Wireless & Networks (الإعدادات - الشبكات السلكية واللاسلكية)، عليك إجراء المسح للوصول إلى الأجهزة التي تبحث بدورها عن أجهزة البلوتوث الأخرى في النطاق ذاته، حدد الجهاز المفضل واقترن به،وبمجرد الانتهاء، أوقف تشغيل البوتوث من خلال تحديد خيار (الإعدادات - الشبكات السلكية واللاسلكية - إيقاف تشغيل البلوتوث).

هناك خيار آخر متاح على الأجهزة الذكية يسمح للأجهزة الأخرى بالعثور على جهازك، ولكن تثبيت هذا الخيار يعرضك لمخاطر القرصنة باستخدام تقنية البلوتوث، لذا يستحسن إيقاف هذه الخاصية بعد الاقتران بجهاز.

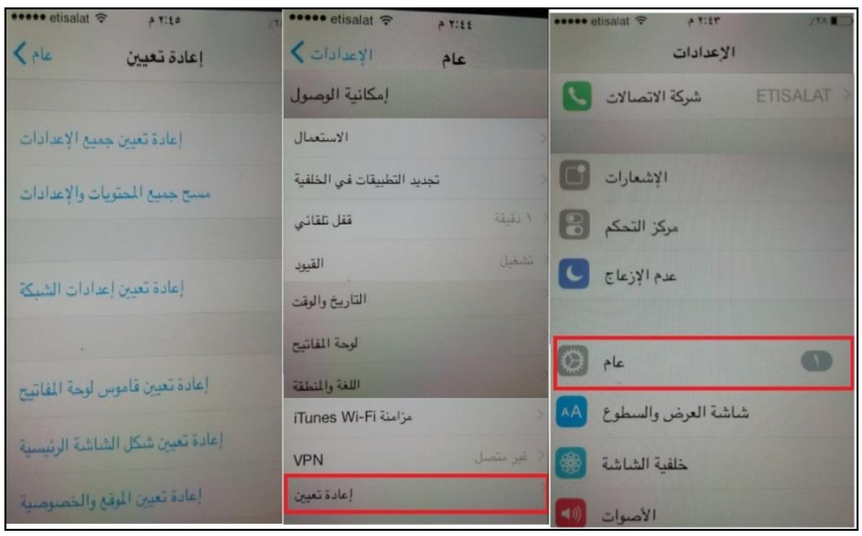
كما أن تقنية "الواي فاي" تشبه "البلوتوث" ولكنها أكثر قوة، وبالتالي فإنها ذات نطاق أوسع ومخاطر أكثر، ومع ذلك فإن معظم الأجهزة الذكية تقريبًا تستخدم الآن هذه التقنية للاتصال بالإنترنت، فالاتصال بتقنية "واي فاي" ‘مفتوحة’يعنيأنهاليسلهاكلمةمرور،الأمرالذييعدأكثر خطورة نظرًا لاحتمالية قيام العديد من الأجهزة غير المعروفة لك بتسجيل الدخول على الإنترنت، وباستخدام برنامج معين، يمكن لأحد الأشخاص الوصول إلى جهازك الذكي ومعرفة المعلومات المخزنة بداخله، ولذلك فإنه من الضروري أن تنسخ بيانات جهازك الذكي احتياطيًا بشكل منتظم لتجنب فقدانها عن طريق السرقة أو الهجمات.

8-5-2-2معرفة كيفية حذف جميع المعلومات الشخصية عند التخلص من الجهاز

إذا كنت تفكر في تحديث جهازك المحمول القديم أو استبداله، فإن هناك ثلاث خطوات مهمة يجب اتخاذها قبل بيع الجهاز أو إعادة تدويره، تتمثل الخطوة الأولى في نسخ معلوماتك الشخصية احتياطيًا أو نقلها إلى جهاز الكمبيوتر أو الجهاز المحمول الجديد الخاص بك، وتتمثل الثانية في مسح بيانات الجهاز أو إعادة ضبطه إلى إعدادات المصنع، وهذا ما يسمى في بعض الأحيان باسم "إعادة الضبط الصعب"، حيث يتم حذف الذاكرة والمعلومات بأكملها لإعادة الجهاز مرة أخرى إلى حالة المصنع الأصلية، وفي بعض الحالات تؤدي هذا الخطوة إلى إزالة التطبيقات الأخرى أيضًا في حالة عدم ضمان إلغاء تثبيت التطبيقات وفقًا لتعليمات الشركة المصنعة للجهاز المحمول الخاص بك، أما الخطوة الثالثة فتتمثل في إزالة بيانات بطاقة التخزين الخارجية أو حذفها. ‘

ولإجراء ما يسمى بـ "إعادة الضبط الصعب" استخدم الإنترنت لتحديد التعليمات المحددة لجهازك المحمول والتي من شأنها تفصيل العملية وشرح مدى المعلومات المحذوفة.

تعرض الصورة أدناه مثالا باستخدام هاتف ذكي محمول "آي فون".



9-5-2-2معرفة كيفية تمكين إعدادات تحديد المواقع وتعطيلها، وفهم مزايا وعيوب تمكين إعدادات تحديد المواقع

إن معظم الأجهزة الذكية النقالة الحديثة بها نظام GPS مضمن لتحديد موقع جهازك بدقة باستخدام خدمات الهاتف الخلوي والأقمار الصناعية على حد سواء, وهذه الميزة تسمح لتطبيقات الطرف الثالث والشركات المصنعة باستخدام تقنية تحديد المواقع لتقديم خدمات تعتمد على الموقع.

يتم تفعيل هذه الخدمة أو تعطيلها على جهازك الذكي من خلال قائمة Settings (الإعدادات).

مزايا تمكين خدمات تحديد المواقع:

- السماح للمستجيبين لخدمات الطوارئ مثل سيارات الإسعاف أو الشرطة بتحديد موقعك بسهولة أكثر.
- استرداد جهازك في حالة السرقة، حيث يمكن تحديد موقعه باستخدام تطبيقات طرف ثالث مدمجة.
- شبكات التواصل الاجتماعي المرتكزة على الموقع والتي تسمح للأصدقاء بالاتصال إذا كانوا على مقربة مثل زيارة نفس المقهى أو المركز التجاري.
- تلقي الإعلانات والعروض الترويجية الموجهة ذات الصلة بموقعك.

عيوب تمكين خدمات تحديد المواقع:

- استنزاف البطارية بشكل أسرع عند تشغيل نظام GPS على جهازك الذكي.
- احتمالية غمر تطبيقات الطرف الثالث هاتفك المحمول بالرسائل والإشعارات، ومع أن هذا قد يكون مجرد مصدر إزعاج، فإنه سوف يلتهم أيضًا بدل البيانات المخصص لك في الشهر.
- احتمالية توقف الخصوصية نظرًا لإمكانية تجسس أحد الأشخاص الذين لديهم حق الوصول إلى الموقع الخاص بك باستخدام شبكة الانترنت، وقد يحدث هذا بسبب فيروس مثبت على جهازك أو بسبب كثرة عدد التطبيقات المثبتة أيضًا.

10-5-2-2 تبادل رقم هاتفك المحمول مع من تعرفه وتثق به فقط، والاحتفاظ بسجل رقم IMEI الخاص بك في حالة فقدان الهاتف أو سرقته

يعد رقم هاتفك المحمول بابًا لحياتك الخاصة والمهنية، ففي بعض الحالات نجد أن بعض الأشخاص يمتلكون رقمين منفصلين، ولكن الكثير من الناس لديهم رقم واحد، وإذا ما حدث وأن وصل رقمك إلى أيدي مسوق عبر الهاتف سيتلقى الرقم سيلاً من المكالمات التسويقية والترويجية، ومثال ذلك المسابقات التي تحدث في مراكز التسوق ومحطات الوقود في جميع أنحاء المنطقة، حيث يطلب منك عادة الإفصاح عن اسمك والبريد الإلكتروني ورقم الهاتف في حال الفوز بجائزة مثل سيارة جديدة، ويستخدم هذا بدقة لتسويق المنتجات للبائع ولشركات الشراكة الأخرى، وفي المرة القادمة التي تقدم فيها معلومات خاصة بك في مثل هذه المسابقة، يرجى النظر إلى ما إذا كان الأمر يستحق العناء.

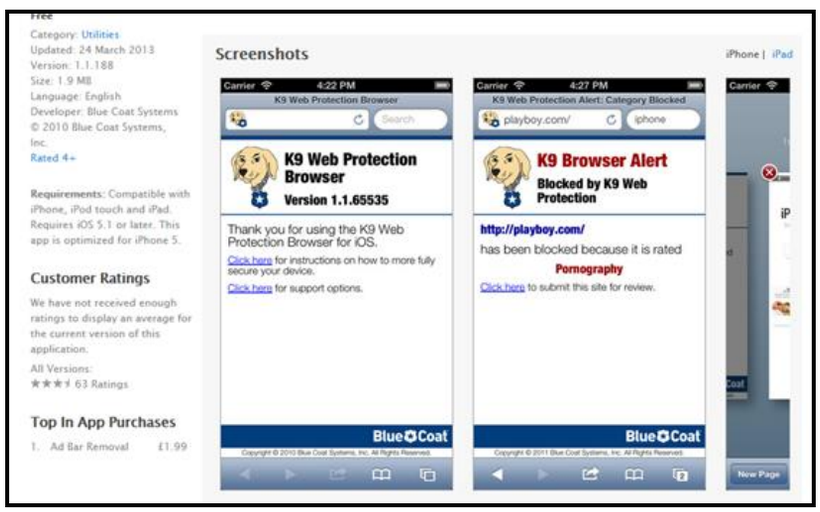
إن أي جهاز ذكي يحتوي على هاتف مدمج أو مودم GSM يجب أن يكون به رقم IMEI المكون من 15 رقمًا فريدًا لكل جهاز، لذا يجب حفظ هذا الرقم في السجلات الخاصة بك في المنزل أو المكتب لكي يستخدمه المزود المحلي حال فقد الجهاز أو سرقته لحجب الرقم حتى يتم تعطيل المكالمات إذا أراد شخص أن يستخدم الهاتف، أو حتى تستخدمه السلطات المحلية للتعرف على هاتفك حال العثور عليه.

يكتب رقم IMEI على العلبة الأصلية للجهاز الذكي ويمكن العثور عليه أيضا باستخدام نظام القائمة الموجود على الجهاز، وتعد قائمة "الإعدادات" أكثر الأماكن المرجح وجود الرقم بها. ‘

11-5-2-2 كيفية تطبيق التصفيه على الإنترنت لحجب المحتوى غير اللائق

يستطيع البالغون المسئولون التحكم فيما سيقوم به الأطفال من تنزيل للمحتويات متعددة الوسائط على هواتفهم، وعلى الرغم من أن فلاتر المحتوى بالغة الأهمية فيما يخص الهواتف الذكية التي تتمتع بوصولٍ كامل إلى الإنترنت والقدرة على تنزيل مقاطع الفيديو، إلا أن معظم الهواتف الخلوية الآن تدعم بعض الأنواع من المتصفحات، كما أن فلاتر المحتوى غير خطرة ومحتواها مناسب أيضًا؛ لذا يمكن تلقيها عبر الرسائل النصية/الرسائل القصيرة أو الرسائل الفورية أو رسائل البريد الإلكتروني.

هناك مثال متوفر على موقع Apple's iTunes (https://itunes.apple.com/gb/app/k9-web-protection-browser/id407657840?mt=8) يمكن تنزيل برنامج K9 Web Protection Browser لتدعيم برامج المراقبة الأبوية وتصفية الإنترنت، كما أنه متاح لأجهزة iPhones وiPads كمتصفح آمن لك ولجميع أفراد العائلة، انظر الشكل (13).



الشكل 13: متصفح تأمين الويب iTunes K9

اختبار

س1- ما المصطلح الحاسوبي المستخدم في عمل نسخ للملفات والمعلومات في حال فقدها أو سرقتها؟

أ- الانعكاس
ب- القفل
ج- النسخ الاحتياطي
د- النسخ

س2- أي من أنواع التخزين التالية الأقل سعة يمنحك القدرة على الوصول إلى البيانات على الإنترنت؟

أ- التخزين السحابي
ب- **القرص الصلب**
ج- مشغل USB
د- الأسطوانات المضغوطة

س3- ما المقصود برسائل البريدالإلكتروني المزعجة؟

أ- الرسائل الإلكترونية التي تم فرزها
ب- رسائل البريد الإلكتروني غير المرغوب فيها
ج- رسائل البريد الإلكتروني المنتهي فترتها
د- رسائل البريد الإلكتروني المتأخرة

س4-هل الجملة التالية صحيحة ام خاطئة؟

نقاط الاتصال اللاسلكي WiFi العامة هي مكان جيد لإجراء المعاملات المصرفية عبر الإنترنت

أ- صواب
ب- خطأ

الإجابات في الصفحة التالية

الإجابات

س1-ج- النسخ الاحتياطي
س2-د- التخزين السحابي
س3-ب- رسائل البريد الإلكتروني غير المرغوب فيها
س4-ب- خطأ

الفصل 2-3

توخ الحذر

2-3-1 مخاطر الإنترنت

2-3-2 التسوق عبر الإنترنت

2-3-3 الدفع عبر الإنترنت

3-2 توخ الحذر

1-3-2 مخاطر الإنترنت

1-1-3-2 التعرف على مخاطر الاستخدام اليومي للإنترنت: البريد الإلكتروني، تصفح الإنترنت، شبكات التواصل الاجتماعي وغيرها

أصبح الإنترنت جزء لا يتجزأ من حياتنا اليومية، لذا علينا أن نكون على دراية كبيرة بمخاطر استخدام شبكات التواصل الاجتماعي وتصفح الإنترنت واستخدام البريد الإلكتروني.

ونورد فيما يلي نماذج للمخاطر التي تواجهنا على الإنترنت عند:

- تسلم رسائل مزعجة والاستجابة لها.
- الاستجابة لرسائل البريد الإلكتروني التي تعتبر رسائل خادعة أو قد تؤدي إلى تسلل احدهم وتحكمه في جهاز الكمبيوتر خاصتك.
- الإفصاح عن المعلومات الشخصية.
- التعرض للتسلط عبر الإنترنت
- إصابة جهاز الكمبيوتر بالفيروسات.
- الإفصاح عن المعلومات الشخصية مما قد يؤدي إلى سرقة الهوية.
- التعرض لعمليات الاحتيال أو القرصنة.
- شراء بضائع لا وجود لها من الأساس.
- سرقة الهوية.
- التعرض لمحتوى غير لائق مثل المواد الإباحية أو العنصرية أو التطرف عبر الإنترنت.
- نشر معلومات شخصية تساعد على تحديد مكان الطفل عندما يكون غير متصل بالإنترنت.
- المشاركة غير المقصودة في نشر محتويات غير قانونية أو غير لائقة.

2-1-3-2 التعرف على مدى انتشار المواد غير اللائقة على الإنترنت

وفقًا لما قاله محققون بصحيفة"ديجيتال جورنال" فإن المواقع الإباحية تحظى بنسبة مرور تصل إلى 30% على الإنترنت (http://digitaljournal.com/article/322668#ixzz2RT1tY9cS) ووفقًا للإحصائيات فإن المواقع الوحيدة التي تتجاوز المواقع الإباحيةفيمايتعلق بنسبة المرور على الشبكة هي مواقع مثل جوجل وفيس بوك،وبجانب تلك المواد الإباحية هناك عدد من المواقع التي تحتوي على مواد عدائية وغير لائقة للكبار والصغار على حد سواء،ويشمل ذلك المواقع التي تحرض على التفرقة العنصرية وسلوكيات التمييز والمواقع التي تروج للمواد المخصصة للكبار،ويتلقىالعديد من الأفراد رسائل مزعجة تحتوي على روابط مخفية لمواقع تحتوي على مواد قد تسيء للمستخدمين - تم توضيح كيفية حظر رسائل البريد الإلكتروني المزعجة والرسائل غير المرغوب فيها بالقسم 2-2-2 "البريد الإلكتروني".

إن مجلس تقنية المعلومات والتجارة الإلكترونية بصدد إعداد مشروع قانون جديد لجرائم الإنترنت في 2004، فلم تعُد العقوبات الحالية المتضمنة في قسم 33 كافية أو ملائمة، وقد أصدر رئيس دولة الإمارات العربية المتحدة وأمير إمارة أبو ظبي سمو الشيخ خليفة بن زايد آل نهيان القانون الاتحادي رقم (5) في عام 2012، وهو قانون شامل للأحكام المكافحة للجرائم الإلكترونية الجديدة، والتي تشمل التشهير وازدراء الأديان وانتهاك الخصوصية، ويوضح الشكل 14 أدناه لقطة من الشاشة للصفحة الأولى، ويمكن الاطلاع على المواد بأكملها عبر الموقع الإلكتروني
http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf

الشكل 14 لقطة من الشاشة للقانون الاتحادي رقم (5) المُطبق في دولة الإمارات العربية المتحدة، قوانين جرائم الإنترنت (2012)

3-1-3-2 الحذر من المخاطر الشائعة: التعرف على مخاطر الطلبات الواردة عبر البريد الإلكتروني المشتبه بها ومواقع الويب المحتمل أن تكون ضارة

يعتبر البريد الإلكتروني من مصادر التهديدات الأكثر شيوعًا، فلا داعي لأن تجلب لنفسك المشاكل، فقد يتمكن مرسلو البريد المجهول من التحكم في عنوان بريدك الإلكتروني وبذلك تصبح هدفًا لهم.

ثمة أمور عدة يجب الاحتراس منها مثل:

- رسائل البريد الإلكتروني التي تطلب منك إدخال بيانات تتعلق ببطاقة الائتمان الخاصة بك أو بيانات مصرفية لأنك قد فزت بجائزة في مسابقة لم تشترك فيها أصلاً أو التي تمنحك فرصة ربح مبلغ كبير من المال.
- رسالة البريد الإلكتروني التي تحتوي على رابط وتطلب منك تنزيل النسخة الجديدة من لعبة على هاتفك المحمول أو جهاز الكمبيوتر.

- رسالة بريد إلكتروني من أحد البنوك أو الموردين على الإنترنت تطلب منك إعادة إدخال البيانات الخاصة باسم المستخدم وكلمة المرور خاصتك، فذلك من الطرق الاحتيالية الشائعة،لذا يرجى توخي الحذر والحيطة عندما يُطلب منك إدخال مثل هذه المعلومات.

يجب تثبيت برامج الحماية من الفيروسات ومكافحة التجسس كما ورد في القسمين 2-1-3 و2-1-4 على جهاز الكمبيوتر خاصتك لتوفر لك الحماية من التجسس والبرامج الضارة التي تسبب لك الدخول دون قصد على المواقع المحتمل أن تكون ضارة.

2-3-2 الخصوصية على الإنترنت

2-3-2-1 التعرف على كيفية توفير الحماية الكافية لنفسك قبل التسوق عبر الإنترنت: استخدام الإصدار الأحدث من المتصفحات, والتأكد من تحديث برنامج مكافحة الفيروسات, وما إلى ذلك.

يجب مراعاة الحيطة والحذر قبل التسوق عبر الإنترنت، فعادةً ما يبحث المتسلل عن مواطن الضعف في المتصفحات لاستغلالها، في حين أن المطورين يبذلون قصارى جهدهم للقضاء على نقاط الضعف هذه، لذا بات من الضروري استخدام المتصفحات الأحدث وتشغيل خاصية التحديث التلقائي لضمان تحديثها أولاً بأول.

إن متصفح "Internet Explorer" من "Microsoft" أحد متصفحات الويب التي تأتي مع نظام تشغيل MS Windows، ومن ثم يتم تحميل التحديثات الخاصة بها عند تثبيت تحديثات نظام تشغيل MS Windows, يوضح التمرين التالي كيف يمكن تثبيت التحديثات أو إعداد التحديثات التلقائية باستخدام نظام تشغيلMS Windows:

تمرين - تثبيت تحديثات نظام تشغيل Windows

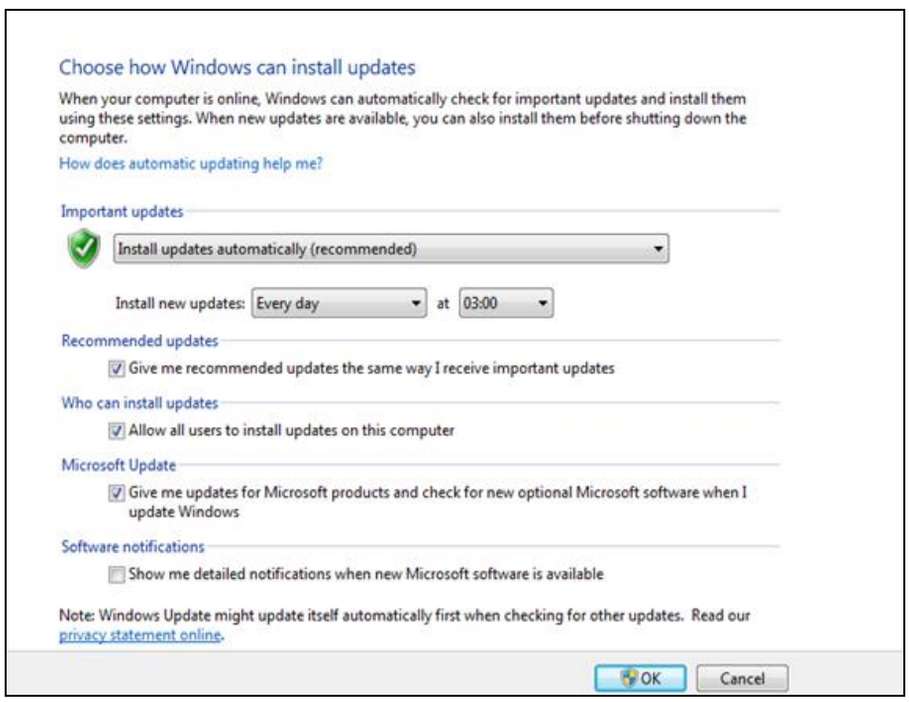
1- انقر بالزر الأيسر للماوس فوق Start (بدء)
2- انقر بالزر الأيسر للماوس فوق All Programs (كل البرامج)
3- انقر بالزر الأيسر للماوس فوق Windows Update (تحديث Windows)
4- انقر بالزر الأيسر للماوس فوق Install updates (تثبيت التحديثات)

تظهر الشاشة الموضحة في الشكل 15:

الشكل 15: شاشة تحديث نظام تشغيل Windows

يمكنك تغيير الإعدادات بحيث تجرى عملية التحديث تلقائيًا، للقيام بذلك اتبع الخطوات التالية:

1. اضغط بالزر الأيسر للماوس فوق Start (بدء)
2. اضغط بالزر الأيسر للماوس فوق All Programs (كل البرامج)
3. اضغط بالزر الأيسر للماوس فوق Windows Update (تحديث Windows)
4- اضغط بالزر الأيسر للماوس فوق Change Settings (تغيير الإعدادات) من الجانب الأيسر في الشاشة وستظهر الشاشة الموضحة في الشكل 16 أدناه:



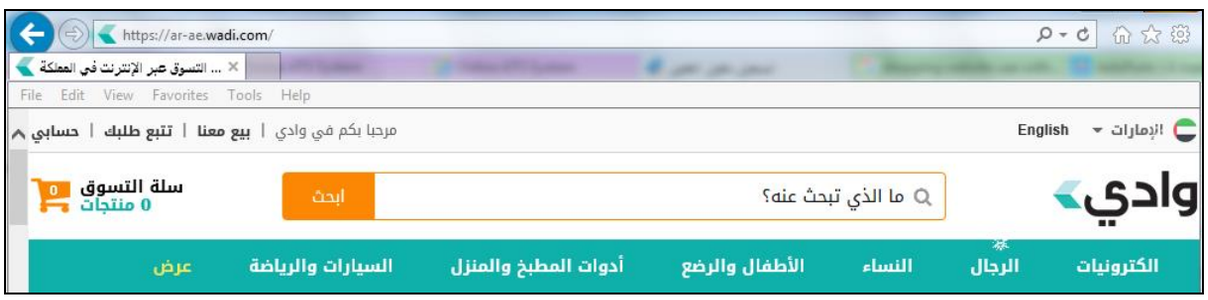
الشكل 16 شاشة تثبيت التحديث التلقائي لنظام Windows

5- حدد وقت تثبيت التحديثات، ثم اضغط فوق OK (موافق).

من الضروري أيضًا تحديث برامج مكافحة الفيروسات باستمرار لتوفير الحماية الكاملة، حيث يتم اكتشاف عدد كبير من الفيروسات الجديدة كل عام، إلى جانب التغييرات التي تطرأ على الفيروسات الحالية والجديدة, ولكل فيروس من هذه الفيروسات عدد من الخصائص أو التواقيع التي تمكن الشركات المصنعة لبرامج مكافحة الفيروسات من الكشف عنها وإيجاد حلول مناسبة من خلال التحديثات.

2-2-3-2 التعرف على كيفية تحديد المواقع الآمنة: ظهور أيقونة القفل على شريط حالة المتصفح، وظهور حرف "s" بعد http في عنوان URL

إذا كنت تتسوق عبر الإنترنت ستحتاج إلى إدخال البيانات المصرفية أو بطاقة الائتمان لإتمام عمليات البيع والشراء، لذا نوصيك بعدم إدخال مثل هذه البيانات إلا على مواقع آمنة، حيث يتم التعرف على المواقع الآمنة بطريقتين: الطريقة الأولى هي أن يبدأ عنوان URL في شريط عنوان المتصفح بهذه الحروف (https://), والمهم أن يأتي حرف"s" بعد (http)" لأن عناوينURL في المواقع غير الآمنة تبدأ بهذه الحروف (http://)، والطريقة الثانية هي أن يظهر رمز القفل في شريط المهام أو العنوان في المتصفح الذي تستخدمه، فاضغط على هذا القفل لعرض الشهادة الرقمية لطبقة المقابس الآمنة (SSL) التي تُعد نوعًا من أنواع بروتوكول التشفير عبر الإنترنت، ويوضح الشكل 17أدناه مثالاً على أحد مواقع التسوق (https://ar-ae.wadi.com)، حيث يمكنك رؤية (https://) في شريط العنوان مما يعني أن الموقع آمن.



الشكل 17: مثال علىhttps:// في بروتوكول عنوان URL (https://ar-ae.wadi.com/).

2-2-3-3 التعرف على سياسات الخصوصية

تضع المواقع الموثوق بها سياسة الخصوصية والتي تظهر عادة على رابط يوجد أسفل الشاشة، والهدف من هذه السياسة هو إعلامك بالمعلومات التي يتم تجميعها والأغراض المقصودة منها ومكان التقدم بشكواك إذ شعرت بأن هذه المعلومات يساء استخدامها، ويوضح الشكل 17 مثالاً لسياسة الخصوصية من موقع .https://ar-ae.wadi.com/privacy، وهو نفس الموقع المشار إليه في أعلى الصفحة التالية (الشكل 18).

الخصوصية والسريّة لوادي

وادي انترناشيونال للتجارة العامة ش ذ م م (" وادي ") هي شركة تأسست في دولة الإمارات العربية المتحدة رخصة تجارية رقم 722160 وعنوانها 3223 ،مجمع إعمارللذهب و الألماس، دبي ، الإمارات العربية المتحدة ، ص.ب 111169 .

نعمل على ادارة www.wadi.com "الموقع" بشكل كامل. وضمن سياسة الخصوصية هذه ، أي ذكر ل "أنت" تعني أي شخص قد يقوم بتقديم معلومات لنا أو لأحد عملائنا أو لموقعنا.

إذا كانت لديك أي تعليقات أو اقتراحات، فيسعدنا استقبالها على عنواننا المسجل بدبي أو على البريد service@wadi.com ، كما يمكنك الاتصال بنا هاتفيا على 800 2 449234

توضح سياسة الخصوصيّة كيفية جمع واستخدام بياناتك الشخصية (تحت ظروفٍ معينةٍ). كما تذكرُ أن الإجراءات المتبعة لضمان خصوصية معلوماتك. تُحدّد هذه السياسة الخيارات المتاحة لك فيما يتعلّق بجمع البيانات الشخصية واستخدامها والكشف عنها. ومن خلال زيارتك للموقع مباشرةً أو عن طريق موقع آخر، أنتَ توافق على التطبيقات المفصّلة في هذه السياسة. إن حماية بياناتك أمرٌ هامٌ جدًّا بالنسبة إلينا. بالتالي، يتم استخدام اسمك وغيره من المعلومات التي تتعلّق بك وفقًا للّنحو المبيّن في سياسة الخصوصيّة. وسنقوم بجمع المعلومات عند الضّرورة أو إذا كانت ذات صلةٍ ضرورية مباشرةٍ بمعاملاتنا معك.

وسنقوم بالاحتفاظ ببياناتك إذا طلب منا بموجب القانون أو لاستخدامها للأغراض التي جمعت لأجلها.

يمكنك تصفح الموقع دون الحاجة إلى تقديم أيّة بيانات شخصيّة. وتبقى هويّتك الشخصية مجهولة طيل زيارتك للموقع ولا يتم كشفها إلا إذا كنتَ تملك حسابا الكترونيا خاصًا على الموقع تُنفذُ إليه بواسطة اسم المستخدم وكلمة السر.

1. البيانات التي نجمعها

قد نحتاج لجمع المعلومات الخاصة بك خلال عملية الشراء عبر موقعنا.

نقوم بجمع البيانات اللازمة لتأمين أية مطالب محتملة قد تظهر لاحقا، ولتزويدك بالخدمات المتوفرة لدينا. مثال على ذلك ، الاسم والجنس وتاريخ الميلاد وعنوان البريد الإلكتروني والعنوان البريدي وعنوان التسليم (إذا كان مختلفًا) ورقم الهاتف ورقم الجوّال ورقم الفاكس وتفاصيل الدفع و تفاصيلٍ عن بطاقات الدفع.

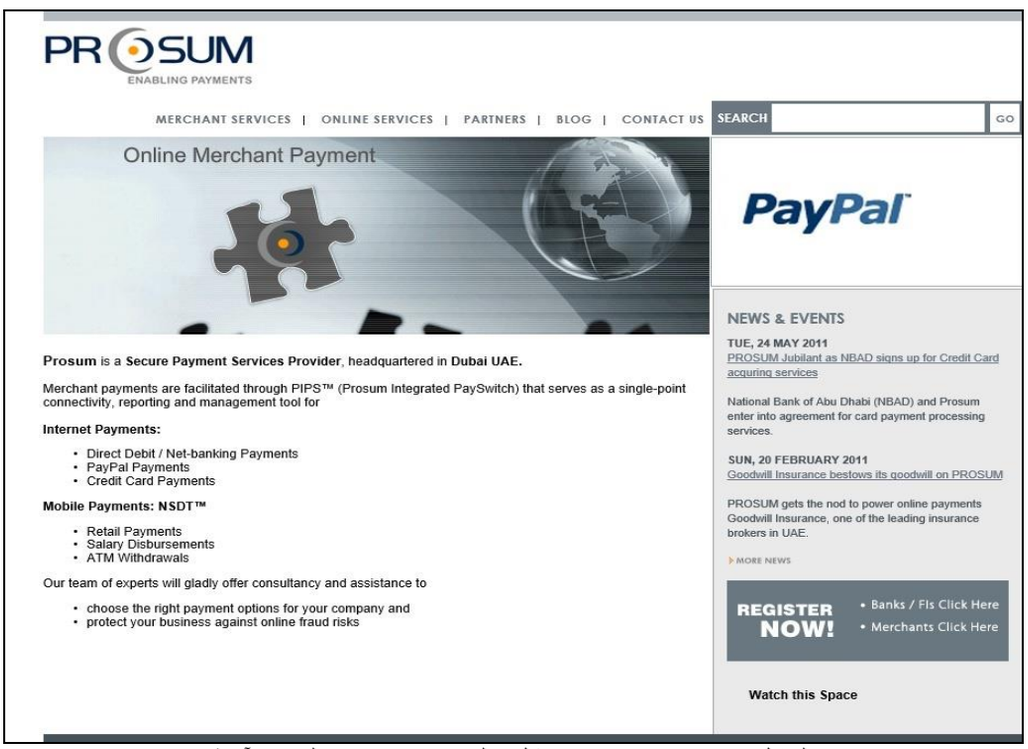
الشكل 18: مثال على سياسة الخصوصية (https://ar-ae.wadi.com/privacy)

4-2-3-2 توخ الحذر من أنه يتم تجميع المعلومات لتحديد ما إذا كانت ملائمة أم لا

يتعين على أي موقع ألا يطلب سوى المعلومات الضرورية له فقط، لذ يرجى استخدام الحس السليم عند إدخال المعلومات الشخصية على الإنترنت, فلا يُطلب منك، على سبيل المثال، عنوانك البريدي إلا عند شحن منتجات إليك، ولا ينبغي لك مطلقًا نشر معلومات كتاريخ ميلادك أو اسم والدتك على موقع إلكتروني أو إحدى شبكات التواصل الاجتماعي ما لم يوافق شخص بالغ مسئول كأحد والديك أو الوصي عليك على ذلك، ومن المهم مراعاة ذلك حيث قد يؤدي إهمال تلك التحذيرات إلى سرقة الهوية.

2-3-3-1 الانتباه إلى خيارات الدفع الآمنة: بطاقات الائتمان، وبطاقات السحب, وغيرها.

تضمن مواقع التسوق عادةً عدد من خيارات الدفع، ومن ثم يمكنك استخدام خدمة الدفع إذا كانت متاحة مثل Prosum (http://www.prosumfzc.com/) انظر الشكل 19أدناه أو WorldPay ((www.worldpay. com، للاستفادة من خدمة الدفع عبر الإنترنت، على البائع والمشتري إنشاء حسابات تمكنهم من دفع الرسوم، ويقدم المشتري معلومات الدفع مثل رقم الحساب المصرفي أو بطاقة الائتمان ويقدم البائع معلومات عن مكان إيداع المدفوعات، وهناك طريقة أخرى للدفع وهي عن طريق التحويل الإلكتروني أو تحويل الرصيد والتي تعد طريقة لنقل الأموال إلكترونيًا من شخصٍ لآخر أو من مؤسسة لأخرى ومن الأمثلة على ذلك نظام ويسترن يونيون (www.westernunion.com).



الشكل 19: Prosum - مثال على مقدم خدمات الدفع الآمنة

يجب ألا تقوم بدفع أية رسوم إلا لعمليات الشراء أو المعاملات الآمنة، ولا تدخل بيانات بطاقات الائتمان أو بطاقات السحب إلا على مواقع آمنة (https://)، ولا ترسل أية أموال إلى شخص لا تعرفه باستخدام خدمة نقل الأموال أو ترسل أموال لسداد الضرائب أو رسوم لمسابقات اليانصيب، فكيف يمكن الفوز بجائزة اليانصيب إذا لم تشارك فيها من الأصل!

2-3-3-2 التعرف على وسائل الأمان المختلفة الخاصة بعملية الدفع: استخدام مانع العناصر المنبثقة، إيقاف تشغيل أدوات الإكمال التلقائي, أمان المتصفح, إعدادات التنقية.

تضم معظم المتصفحات مجموعة من إعدادات الأمان المختلفة، لذا يجب عليك استخدام أكبر كم من هذه الإعدادات قدر المستطاع عند إدخال البيانات المصرفية أو بيانات بطاقات الائتمان الخاصة بوالديك على أي جهاز كمبيوتر حتى وإن كنت الوحيد الذي تستخدم الجهاز.

2-3-3-3 التعرف على الوقت المناسب لاستخدام أدوات الإكمال التلقائي وإيقاف تشغيلها

تحتوي بعض المتصفحات على أدوات الإكمال التلقائي التي تخزن معلومات مثل الاسم والعنوان عندما تقوم بملء استمارات على مواقع الإنترنت، وعند ملء استمارة في المرة التالية تتعرف هذه الأدوات على نفس الحقول وتستخدم نفس المعلومات،

وقد يعمل ذلك على توفير الوقت عند عمل استبيان أو إدخال قائمة تضم عدد من عناوين البريد الإلكتروني.

وعلى الجانب الآخر قد تنطوي عملية الإكمال التلقائي على بعض المخاطر لأنك لست الشخص الوحيد الذي يقوم باستخدام جهاز الكمبيوتر،فإذا ما سُرق جهاز الكمبيوتر الخاص بك، قد تكون أكثر عرضة لخطر سرق الهوية،لذا يجب عليك بشكل عام إيقاف تشغيل الإكمال التلقائي،خاصة إذا كنت تقوم بإتمام المعاملات باستخدام جهاز كمبيوتر يستخدمه آخرون أو كنت تستخدم جهاز كمبيوتر آخر لإدخال بيانات خاصة بالحساب المصرفي أو بطاقة الائتمان.

4-2-3-2 التعرف على مختلف وسائل الأمان الخاصة بالنماذج عبر الإنترنت: استخدام مانع العناصر المنبثقة، إيقاف تشغيل أدوات الإكمال التلقائي, أمان المتصفح, إعدادات التنقية.

تضم معظم المتصفحات مجموعة من إعدادات الأمان المختلفة، لذا يجب عليك استخدام أكبر كم من هذه الإعدادات قدر المستطاع عند إدخال البيانات المصرفية أو بيانات بطاقات الائتمان الخاصة بوالديك على أي جهاز كمبيوتر حتى وإن كنت الوحيد الذي تستخدم الجهاز.

- تشغيل مانع العناصر المنبثقة - على الرغم من أن هذا قد يسبب مشكلة مع المصادقة الثنائية.
- إيقاف تشغيل ملفات تعريف الارتباط والإكمال التلقائي - سيوفر هذا طبقة ثانية من الخصوصية والأمان.
- التأكد من استخدام موقع إلكتروني آمن كما مذكور في الجزء 2-2-3-2.

اختبار

س1-ترغب في التسوق عبر الإنترنت لشراء مقاطع فيديو موسيقية، فأي من حرف من الحروف الموجودة بعنوان الموقع الذي تريد الشراء منه سيمنحك مزيدًا من الحماية؟

أ- ‘s’
ب-‘d’ ‘‘
ج- ‘t’
د- ‘h’

س2- أي من خصائص متصفح الويب تترك بعض من بيانات الوصول الآمن في المتصفح ليستخدمها شخص آخر؟

أ- بحث شريط الأدوات
ب- الإكمال التلقائي
ج- المفضلات
د- مانع العناصر المنبثقة

س3- أي من الرموز التالية تظهر عادةً على شاشات عمليات الدفع الآمن؟

أ-القفل
ب- الدائرة
ج- النجمة
د- الشكل المتقاطع

س4- أي من الخطوات التالية تساعدك على تشغيل جهاز الكمبيوتر خاصتك على نحو أكثر آمانًا؟

أ- تشغيل مانع العناصر المنبثقة
ب- تشغيل فلتر الرسائل المزعجة
ج- إيقاف تشغيل مانع العناصر المنبثقة
د- تقليل الشاشات المنبثقة

الإجابات في الصفحة التالية

الإجابات

س1-أ-’s‘

س2-ب-الإكمال التلقائي

س3-أ- القفل

س4-أ-تشغيل مانع العناصر المنبثقة

الفصل 2-4

التفكير أولاً

2-4-1 الهوية الشخصية

2-4-2 أجهزة المشاركة

2-4-3 شبكات التواصل الاجتماعي

2-4-4 البريد الالكتروني غير المرغوب فيه والتصيد الاحتيالي على مواقع شبكة التواصل الاجتماعي

2-4-5 الهويات الزائفة على وسائل التواصل الاجتماعي

4-2 التفكير أولاً

1-4-2 الهوية الشخصية

1-1-4-2 استيعاب مفهوم الهوية عبر الإنترنت وما تعنيه شبكات التواصل الاجتماعي

تعد الهوية عبر الإنترنت هوية اجتماعية ينشئها مستخدمي شبكة الإنترنت في مجتمعات الإنترنت، كما يشار إليها بـ"اسم شاشة" أو "شخصية إنترنت"، فرغم تفضيل بعض مستخدمي الإنترنت استخدام أسمائهم الحقيقية عبر الإنترنت، يفضل البعض الآخر عدم الكشف عن هويتهم واستخدام أسماء مستعارة توحي باختلاف المعلومات الشخصية المحددة.

وشبكة التواصل الاجتماعي عبارة عن موقع إلكتروني يتيح لك التواصل مع أصدقائك والعائلة ومشاركة الصور والفيديوهات والموسيقى وغيرها من المعلومات الشخصية سواء مع مجموعة معينة من الأصدقاء أو مع مجموعة كبيرة من الأشخاص مثل موقع "فيس بوك" (www.facebook.com)، و"تويتر"(www.twitter.com)، و"لينكد إن" (www.linkedin.com)، و"يوتيوب" (www.youtube.com) وتعد هذه المواقع من الوسائل المناسبة تمامًا للتواصل مع أصدقائك والعائلة فضلاً عن تكوين صداقات جديدة مع أناس لهم نفس اهتماماتك أو وظيفتك.

2-1-4-2 معرفة الآثار المترتبة على وضع المعلومات الشخصية على الإنترنت

بمجرد نشر هذه المعلومات على الإنترنت، لا يمكنك التراجع عنها حتى لو حذفت هذا المنشور فستوجد نسخة منه في أي مكان آخر.

يمكن لأي شخص يمتلك وسيلة الدخول إلى الإنترنت الدخول على البيانات الشخصية بمجرد نشرها عبر الإنترنت، ومن بين هؤلاء الأشخاص، أصدقائك وأبويك وأصدقاء المدرسة أو الكلية وصاحب العمل المستقبلي ومن المحتمل أيضًا القراصنة والمحتالين والفضوليين، فنشر معلوماتك الشخصية يجعل من السهل التعرف عليك، وسيظل ما نشرته مثبتًا في الصفحة التي نشرت عليها وعادة ما تكون على علم بما يطرأ عليه من تغييرات.

3-1-4-2 فكر فيمن يمكنه الدخول إلى بياناتك الشخصية: الأصدقاء, الأصدقاء عبر الإنترنت "ممن لا تعرفهم شخصيًا"، المجرمون، المعتدون..

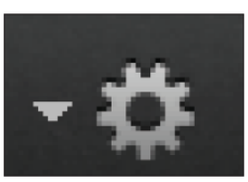
من الأهمية بمكان أن تعلم أن ملفك الشخصي يظهر لعامة الناس ومن السهل لأي شخص الاطلاع على المعلومات العامة، فما حجم المعلومات الشخصية التي قد تخبرها لشخص غريب لا تعرفه؟ هذا هو ما تفعله بملفك الشخصي العام، حتى لو قصرته على أصدقاء الأصدقاء فيمكن وجود الكثير من الأشخاص، فلو أن لديك 160 صديقا وكلاً منهم لديه 160 صديقا يكون مجموعهم 25.600 صديق، هل يمكنك أن تثق فيهم جميعًا؟

4-1-4-2 التعرف على خيارات الخصوصية بشبكات التواصل الاجتماعي وسبب أهميتها

من الضروري أن تتفحص خيارات الخصوصية على مواقع شبكة التواصل الإجتماعي المشترك فيها، حيث تختلف الإجراءات التي يمكن فعلها من موقع لآخر،وعلى وجه العموم، لا يمكنك منع الأشخاص من نشر تعليقاتهم عنك كما لا يمكنك منعهم من نشر صور لك، فكل ما يمكنك فعله هو منع الأشخاص من الإشارة إليك في الصور التي ينشرونها، كما يمكنك منع الأشخاص من رؤية تاريخ ميلادك أو مكان المدرسة التي ذهبت إليها أو محل العمل أو وضعك الحالي، ويمكنك أيضًا قصر معلومات معينة على الأصدقاء الحقيقيين فقط، وإذا رغب أي شخص آخر في معرفة المزيد عنك، يمكنهم إرسال طلب صداقة وأنت تقرر ما تود السماح لهم بمعرفته، الشكل 20 يوضح خيارات الخصوصية لموقع "فيس بوك"، حيث يمكنك رؤية المعلومات العامة والأشخاص الذين يمكنهم البحث عنك، وهذه الخيارات قابلة للتخصيص من خلال روابط Edit (تعديل) كما هو مبين.

الشكل 20: إعدادات وأدوات خصوصية فيس بوك (https://www.facebook.com/privacy)

للدخول على خيارات الخصوصية على أغلب مواقع التواصل الاجتماعي، انقر فوق رمز Tools (الأدوات) الموجود على الموقع، كما هو مبين في مثال الشكل 21 أدناه.



الشكل 21: مثال لرمز Tools (الأدوات)

للدخول على خيارات خصوصية موقع (تويتر):

1- اضغط على رمز Tools (الأدوات) الموجود على الجانب الايسر في اعلى الشاشة
2- اضغط على Settings (الإعدادات).
3- اضغط على خيار Security and Privacy (الامان والخصوصية) الموجود على الجانب الأيمن من الشاشة

خيارت الخصوصية تشمل ما هو موضح في الشكل 22 أدناه:

الشكل 22: خيارات الخصوصية في موقع تويتر

4-2 التفكير أولاً

2-4-2 أجهزة المشاركة

1-2-4-2 معرفة أنواع الأجهزة التي يمكن استخدامها في تبادل المعلومات: الهواتف المحمولة, الهواتف الذكية, مشغلات MP3, أجهزة الآي بود, الأجهزة اللوحية وغيرها.

يمكن لهذه الأجهزة تبادل المعلومات بطرق لا يمكن تصورها منذ عدة سنوات، حيث يمكنك للهواتف الذكية والأجهزة اللوحية تبادل المعلومات عبر الإنترنت والبلوتوث والشبكات اللاسلكية، كما يمكن لأي جهاز، مثل مشغلات MP3 وأجهزة الآي بود، أن يتصل بشبكة ويتبادل المعلومات مع أي جهاز آخر متصل بنفس الشبكة.

كما أتاحت مواقع التواصل الاجتماعى تبادل المعلومات والصور والفيديوهات عبر تلك الأجهزة.

2-2-4-2 الانتباه إلى إمكانية استخدام خصائص الصور والفيديو لتسجيل ونشر محتوى غير لائق على الإنترنت

من أمثلة نشر المحتوى غير اللائق قيام شخص بإرسال رسائل أو صور إباحية غير لائقة، أو بالتقاط صور غير مسموح بها لشخص آخر، وعادة ما تكون النساء هي الضحية فيشعرن بالإحراج أو الإهانة عند إدراك الأمر، ومما يزيد من حزنهن أن يتم بالفعل نشر تلك الصور على شبكة الإنترنت مع إمكانية التعرف عليهن.

ويمكن لأي جهاز يحتوي على كاميرا إرسال أي صورة على أنها رسالة، وبمجرد إرسالها، لا يمكن لصاحب المحتوى السيطرة على الأماكن التي ستنشر فيها هذه الصور فيما بعد، أما مواقع التواصل الاجتماعي فتتوافر بها اتفاقات لشروط الاستخدام لإرساء القواعد والمبادئ التوجيهية لضمان الاستخدام المناسب لجميع مستخدميها.

يحتوي موقع يوتيوب على إرشادات مجتمعية يوضحها الشكل 23 بالصفحة التالية وتنص هذه الإرشادات على منع نشر أي مواد غير لائقة، كما تنص على قواعد استخدام الموقع ويمكن الاطلاع عليها بالكامل على http://www.youtube.com/t/community_guidelines

الشكل 23: الإرشادات المجتمعية لموقع يوتيوب

لقد أصبحت شبكات التواصل الاجتماعي عبر الإنترنت إحدى أكثر الأنشطة شيوعًا بالنسبة للأطفال والشباب، حيث تشترط مواقع التواصل الاجتماعي مثل الفيسبوك وإنستغرام وسناب شات وتويتر عادة ألا يقل عمر مستخدميهم عن 13 عام عند إنشاء حساب, وللمساعدة في حماية الأطفال والشباب، يمكن للآباء وضع ضوابط وعوامل تصفية لما يشاهده أطفالهم.

3-2-4-2 توخي الحذر عند نشر الصور أو مقاطع الفيديو على الإنترنت من خلال هاتفك المحمول، وطلب إذن الآخرين قبل نشر الصور أو مقاطع الفيديو الخاصة بهم من خلال هاتفك المحمول

وفقًا لما ورد في الأقسام السابقة من هذا الكتاب فإن الخصوصية الفردية أصبحت أكثر وأكثر أهمية والمسؤولية الشخصية يبدو أنها تتزايد بعدد الفيديوهات والصور الفوتوغرافية التي التقطت ونشرت على الانترنت باستخدام الهواتف المحمولة، ومع ذلك فإن هذا ليس بتحذير بل تذكرة للتروي والحذر عند نشر الصور على الانترنت، وطلب الإذن هو دائما أفضل وأسلم طريقة لتقليل أو القضاء على هذه المسؤولية.

وهاك مثال للتأكيد على هذه الأهمية: بعض البلدان تفرض الآن قانونًا يسمح فقط للآباء بنشر صور عبر الإنترنت لأطفالهم، وأي شخص آخر يلتقط صورًا للقصّر وينشرها دون إذنهم قد يواجه اتهامات جنائية، وبالطبع فإن هذا لا يطبق دائمًا بل هو للأسبقية المستقبلية.

2-4-3 شبكات التواصل الاجتماعي

2-4-3-1 التعرّف على مختلف مواقع شبكات التواصل الاجتماعي التي يستخدمها الشباب مثل: فيسبوك، واتس آب, إنستغرام, سناب شات، تويتر، بيرسكوب.

غالبًا ما تستخدم مختلف مواقع شبكات التواصل الاجتماعي شرائح مختلفة من الشباب, ومن الأهمية بمكان استخدام برنامج التواصل المناسب لفئتك العمرية، فإذا أدخلت عمرًا عن طريق الكذب ودخلت إلى أحد المواقع التي تستهدف أشخاصًا كبار السن، يمكن للمستخدمين الآخرين تقديم افتراضات وإرسال تعليقات أو مواد لك قد تجد أنها غير ملائمة, إن أهم ما يميز مواقع التواصل الاجتماعي أن الشخص يستخدم الموقع المشهور بين أصدقائه.

يعد موقع "فيس بوك" الموقع الرائد في السوق حيث يستخدمه أكثر من مليار مستخدم (المصدر: tp://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/)فلقد كان يستهدف في البداية طلبة الكليات، ولا يشيع استخدامه بين المراهقين وشباب العشرينات فقط بل امتدت جاذبيته لجميع الفئات العمرية، ولكن لم يعد موقع فيس بوك المنصة الرئيسة التي يتفاعلون ويتواصل مع أصدقائهم من خلالها بعد الآن.

بمرور الوقت، أصبح المجتمع بأكمله يتفاعل الآن على الأجهزة المحمولة, حيث تساعد تطبيقات مثل تطبيق فيسبوك وفيسبوك ماسنجر مستخدميها على التواصل المستمر مع الأصدقاء في أي مكان.

كما يستخدم العديد من الأشخاص تطبيق واتس آب, حيث وصلت نسبة مستخدميه في عام 2016 إلى 1 مليار مستخدم (https://blog.whatsapp.com/616/One-billion), فلقد أصبح واحدًا من أكثر تطبيقات الرسائل النصية البديلة شعبية، حيث يمكن لأي شخص البقاء على اتصال مع العائلة والأصدقاء مجانًا.

يعد تطبيق إنستغرام أيضًا من أكثر وسائل التواصل استخدامًا, فعلى الرغم من أن معظم الأشخاص لديهم حسابات فيسبوك, إلا أن إنستغرام هو إحدى وسائل الإعلام الاجتماعي المستخدمة بشكل متكرر من قبل المراهقين, حيث يعد أكثر تفاعلية، كما يمكنك التنقل خلال التطبيقات دون الانزعاج من ظهور إعجاب أو تعليق لأحد الأصدقاء على ملف أخر الأخبار الخاص بك.

تستثمر العديد من وسائل التواصل الاجتماعية المحتوى المرتبط بالفيديو والذي يعد واحدًا من الاتجاهات الأكثر شعبية، فهم على دراية أن الحشود الشابة تنجذب إليها وتتواصل معها في معظم الأحيان, فعلى الرغم من قيام العديد من منصات وسائل التواصل الاجتماعي بذلك الآن، إلا أن تطبيق سناب شات يعد المنصة الوحيدة التي تبنت تأسيس ذلك, ونتيجة لذلك، أصبح هذا التطبيق متعارف عليه بشكل كبير بين جيل الشباب، حيث يتم مشاهدة ما يقرب من 7 مليار فيديو في اليوم الواحد، مما يجعله يواكب تطبيق فيسبوك بسرعة.
(http://www.bloomberg.com/news/articles/2016-01-11/snapchat-s-daily-mobile-video-views-said-to-rival-facebook-s)

لا يفضل المستخدمون أن يتم متابعتهم من قبل أفراد لا يعرفونهم, فبمجرد نشر قصة، يمكن لمتابعيك فقط مشاهدتها مرة واحدة.

يمتاز تويتر، أخر موقع تواصل تم إنشاؤه، بقاعدة كبيرة: حيث تصل نسبة مستخدميه إلى ما يقرب من 320 مليون مستخدم نشطًا شهريًا بمعدل إجمالي قدره 500 مليون تغريدة في اليوم الواحد. المصدر: (https://about.twitter.com/company

خلافًا للمنصات المذكورة سابقًا، يعتبر العديد من المراهقين تويتر مكانًا لمتابعة أشخاص لم يلتقوهم من قبل, حيث يمكنهم الآن القيام بذلك في تنسيق الفيديو باستخدام البيرسكوب, وبشكل أساسي، أصبح المراهقون الآن قادرون على مشاهدة أشرطة الفيديو الحية من جميع أنحاء العالم.

تشمل مواقع الشبكات الاجتماعي الأخرى تطبيق ڤاين وكيك (شبكات تبادل الفيديو القصير)، وساوند كلاود وماي سبيس (المعنيين بمشاركة الموسيقى)، وبنترست وفليكر (منصات مشاركة الصور عبر الإنترنت).

2-3-4-2 التعرّف على طريقة إنشاء ملف شخصي على شبكات التواصل الاجتماعي وكيفية ضبط ملفك الشخصي للعرض الشخصي أو العام

ليست هناك خصوصية تامة لمثل هذه الأمورعلى شبكة الإنترنت، فحينما يتعلق الأمر بالملفات الشخصية، تذكر أنه قد يطلع غير أصدقائك على ملفك والمعلمون وأفراد الشرطة ومن ثم لا تعرض الكثير من بياناتك الشخصية، فعند إنشاء الملف الشخصي، سل نفسك، "ما حجم المعلومات التي أرغب أن يعرفها عني شخص غريب؟"

يتألف ملفك الشخصي عادةً من اسمك ودولتك وتاريخ ميلادك واهتماماتك وحالتك وصورتك الشخصية، وتتيح لك الإعدادات تحديد الأشخاص الذين يمكنهم الاطلاع على ملفك الشخصي، فوضع 'عام' يتيح 'للجميع' رؤية ملفك الشخصي، وهذا بالنسبة لكل شخص يمكنه الدخول إلى شبكة الإنترنت، كما يمكن تخصيص العناصر الفردية، أي ان تقصر رؤية ملفك الشخصي على "الأصدقاء" أو "الأصدقاء المقربين" ويوضح الشكل 24 أدناه شاشة أدوات وإعدادات الخصوصية لموقع فيس بوك، حيث يمكنك التغيير وفقًا لما هو مذكور في إعداد "من يستطيع البحث عني" عن طريق تحديد رابط "تعديل" الموجود على اليمين، فإذا كان الإعداد مضبوطًا على "الجميع"؛ فهذا يعني أن معلوماتك الشخصية تكون ظاهرة للعامة، ولتغيير الإعداد لوضع "خاص"، إضغط فوق "تعديل".

الشكل 24: إعدادات وأدوات خصوصية فيس بوك.(https://www.facebook.com/settings/?tab=privacy)

3-3-4-2 استيعاب فكرة إمكانية رؤية أي شخص ملفك الشخصي على الإنترنت والبحث عنك باستخدام بعض المعايير والوصول إلى معلوماتك الشخصية

يمكن رؤية ملفك العام من قبل الأصدقاء والمعلمون وأفراد الشرطة والملاحقين والجناة المسجلين, وضع عام يعني للجميع، ولفحص حجم المعلومات التي تظهرها للجميع، يمكنك كتابة اسمك في محرك البحث والنقر فوق خيار "بحث".

يجب مراعاة مسألة ملائمة الملف الشخصي عند تمكين الجميع من رؤيته.

4-3-4-2 التعرّف على بعض مخاطر استخدام شبكات التواصل الإجتماعي: المحتوى غير اللائق، ومسائل التحقق من العمر، والدخول إلى الملفات الشخصية، واحتمالية وجود مستغلين

لا تتحقق أغلب مواقع شبكات التواصل الاجتماعي من هويتك الشخصية حينما تقوم بتسجيل الاشتراك، حيث يتحقق موقع تويتر من حسابات "المشاهير" فقط في حين يتحقق موقع فيس بوك فقط من امتلاكك لرقم الهاتف الذي قمت بتعيينه، مما يعني أنه بإمكان أي شخص إنشاء حساب على شبكات التواصل الاجتماعي باستخدام معلومات زائفة وهوية مفترضة، وتشير التقديرات إلى أن 7.5 مليون شخص في مرحلة ما قبل سن المراهقة يتواجدون على موقع فيس بوك في الولايات المتحدة الأمريكية فقط.

وقد يؤدي هذا إلى دخول الأطفال والشباب عن طريق الخطأ إلى صور غير لائقة ويصيرون ضحايا للمحتالين والمستغلين، وقد يشمل الاستغلال التعرض لمحتوى إباحي أو ضار وتشجيع الشباب على نشر محتوى غير لائق أو صور خاصة بهم، ومن ضمن المسائل التي يجب الحذر منها عند استخدام مواقع شبكة التواصل الاجتماعي ما يلي:

- السؤال عن البيانات الشخصية - كالعمر والعنوان ورقم الهاتف المحمول والصور الشخصية.
- اللقاءات الواعدة مع المشاهير أو نجوم الرياضة أو العروض أو الهدايا المجانية.
- الدفع لك مقابل التقاط صور فاضحة.
- اعتماد سلوك البلطجة الالكترونية أو الترهيب.
- طلب مقابلتك شخصيًا.
- انتحال صفة طفل أو مراهق بغية إجراء مقابلة معك.

4-4-2 البريد الالكتروني غير المرغوب فيه والتصيد الاحتيالي على مواقع شبكة التواصل الاجتماعي

1-4-4-2 إدراك أن البريد الالكتروني غير المرغوب والتصيد الاحتيالي منتشران أيضا على مواقع شبكة التواصل الاجتماعي

إن النمو السريع لمواقع شبكة التواصل الاجتماعي يعني أنها قد أصبحت هدفًا رئيسًا للبريد الإلكتروني غير المرغوب والتصيد الاحتيالي, ففي السنوات السابقة كان البريد الإلكتروني الوسيلة الرئيسية التي يستخدمها مرسلو الرسائل غير المرغوب فيها والمتصيدون للوصول إلى ضحاياهم، ولكن مع التطور المتزايد لعوامل التصفية المقدمة من قبل مزودي خدمة البريد الإلكتروني فإن تلك النافذة قد أغلقت بشكل كبير، وبدلاً من ذلك لجأ مرسلو الرسائل غير المرغوب فيها والمتصيدون إلى مواقع شبكة التواصل الاجتماعي التي تحمل الكثير من المعلومات العامة والشخصية والتي لديها قواعد أكثر من المستخدمين النشطاء.

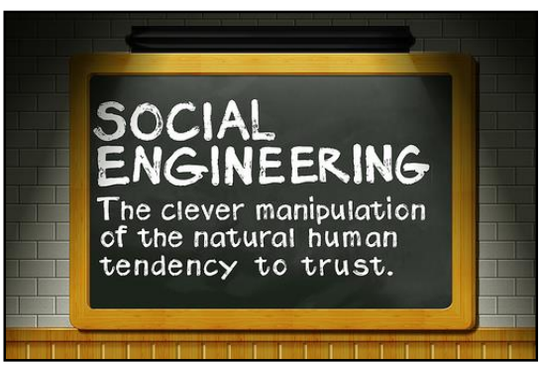
2-4-4-2 التعرف على الروابط المشبوهة لإعلانات الإنترنت، وتحديثات الحالة، والتغريدات، والمشاركات الأخرى

أثناء استخدام موقع التواصل الاجتماعي المفضل لديك ستلاحظ العديد من إعلانات الإنترنت، والتغريدات، والمشاركات، وتحديثات الحالة غير الصحيحة، والرابط الموجود في تحديث الحالة، أو التغريدة، أو المشاركة قد يكون مزيجا غريبًا من الحروف والأرقام أو قد يكون صيغة عامة لا يمكن أن تأتي من أصدقائك، فمن المستحسن أن تتجنب الضغط على هذه الروابط ما لم تتمكن من التحقق من أن هذا الرابط قانوني، وأدناه مثال على ذلك.

من الصعب كشف إعلانات الإنترنت، كما أن معظمها مجرد أشخاص مزعجون يريدون الحصول على المال من خلال الإعلانات ‘, فإذا قررت فتح إعلان من هذه الإعلانات من موقع تواصل اجتماعي, يرجى التأكد من عدم تحميل مرفقات إلا إذا كنت واثقا من الموقع والشركة.

3-4-4-2 فهم مصطلح "الهندسة الاجتماعية"، والاحتياط من التهديدات التي تشكلها هجمات الهندسة الاجتماعية.

الهندسة الاجتماعية، في سياق مواقع شبكات التواصل الاجتماعي، تشير إلى التلاعب النفسي بالناس (الشباب في الغالب) للكشف عن معلومات سرية يمكن استخدامها فيما بعد لغرض السرقة أو ارتكاب جرائم أخرى ضد الضحية، وتعد مواقع شبكات التواصل الاجتماعي منصة مثالية لمثل هذه الهجمات، لأن مستخدميها يضيفون مستخدمين آخرين على أساس منتظم ليصبحوا "أصدقاء" فإذا ما أراد شخص ارتكاب مثل هذا الهجوم فإنه يصبر ليبني علاقات ليستخدمها في نهاية المطاف لارتكاب جريمة.



4-4-4-2 ادراك سهولة إنشاء ملف شخصي على مواقع شبكات التواصل الاجتماعي، وامكانية استخدام المجرمين ذلك كفرصة لانتحال صفة شخص آخر

إن إنشاء ملف شخصي على مواقع شبكات التواصل الاجتماعي يستغرق مبتدئا أقل من خمس دقائق، ومن فعل ذلك من قبل فإن الأمر بالنسبة له قد يستغرق أقل من 60 ثانية! فهذه المواقع لا تطلب الكثير من المعلومات الشخصية بل إنها لا تتحقق منها نظرًا للكم الهائل من المستخدمين الجدد الذين يسجلون كل يوم, لذلك فإن معظم المواقع تطلب القليل جدا من المعلومات مثل الاسم وعنوان البريد الإلكتروني والعمر أو تاريخ الميلاد, ونادرًا ما يتم التحقق من هذه المعلومات، وبالتالي يتمكن الأشخاص بسهولة من إنشاء ملفات شخصية وهمية أو انتحال صفة شخص آخر, ومن ثم يمكن أن يؤدي ذلك إلى الجريمة من خلال هجمات الهندسة الاجتماعية المذكورة في القسم السابق.

5-4-2 الهويات الزائفة على وسائل التواصل الاجتماعي

1-5-4-2 التعرف على التهديدات التي يتعرض لها الأطفال عبر الانترنت عن طريق استخدام هويات زائفة: الاستمالة، واستغلال الأطفال

كما ذكر في القسم 2-4-4-4 فإنه من السهل إنشاء هوية زائفة على مواقع شبكات التواصل الاجتماعي, فتخيل شخص بالغ يقوم بإنشاء ملف شخصي لشاب صغير بغية التواصل معك عبر الإنترنت, فهذه "الاستمالة الطفولية" تهدف لاقامة علاقات صداقة مع القُصّر وإقامة روابط عاطفية بقصد الاعتداء عليهم جنسيًا، وهناك العديد من أشكال استغلال الأطفال ولكنه موضوع غير مناسب للمناقشة, ولكن المهم هو أن ندرك جميعًا التهديدات من أجل التصدي لها لضمان السلامة عبر الإنترنت.

2-5-4-2 التعرف على التهديدات التي يتعرض لها الكبار عبر الانترنت عن طريق استخدام هويات زائفة: الوصول إلى المعلومات الشخصية، وسرقة الهوية

الاستمالة هي كلمة تستخدم لوصف عمل يقوم به الكبار في محاولة للاستفادة من الأطفال من خلال استخدام هويات كاذبة عبر الإنترنت, فإضافة مستخدم على موقع تواصل اجتماعي يمكن الأفراد عديمي الأخلاق من رؤية صور أصدقائك وفهم نمط حياتك من خلال مشاركاتك دون الكشف عن هوياتهم الحقيقية, بل إن ذلك قد يُستخدم للوصول إلى المعلومات الشخصية، وربما يعرض سلامتك للخطر، سواء على الإنترنت أو في الحياة الحقيقية.

هناك عدد من التقنيات الخاصة التي يستخدمها مرتكبي الجرائم لإخفاء سلوكهم, حيث يتعمد الكثير منهم الظهور بصورة أشخاص طيبون حتى لا تشك بأنهم من مرتكبي الجرائم على الإنترنت فهم يصورون أنفسهم كأشخاص لطيفة وبريئة, ويشمل هذا التنكر، على سبيل المثال لا الحصر:

تستخدم جميع هذه الأساليب في نهاية المطاف لكسب ثقة المراهقين من أجل التلاعب بهم.

2-4-5-4 فهم ما هو المقصود بمصطلح التطرف عبر الإنترنت

يُعرّف مصطلح التطرف عبر الإنترنت على أنه العملية التي يصبح الأفراد من خلالها متطرفين، ويعد مصطلح التطرف، وتعريفه، في حد ذاته من المفردات الغامضة حيث يمكن استخدامه للإشارة إلى العديد من المفاهيم والتأثيرات المختلفة.

في هذا السياق، وعلى الرغم مما سبق، فإن التطرف عبر الإنترنت يُعرّف باعتباره العملية التي يتم من خلالها تعريف الفرد برسالة أيديولوجية وعقيدة أو اعتقاد ما والذي يشجعه على الانتقال بتفكيره من الإيمان بالمعتقدات السائدة إلى الإيمان بأفكار وآراء متطرفة وذلك من خلال استخدام وسائل الإعلام الإلكترونية في المقام الأول، ونتيجة لذلك يتأثر هذا الفرد ويبدأ في تبني تلك الأفكار المتطرفة.

2-4-5-5 معرفة دور المعلمين ومسؤولياتهم فيما يتعلق بحماية الأطفال والشباب

يتمثل السبب وراء ضرورة معرفة المعلمين بمصطلح التطرف عبر الإنترنت وفهمه وتدريسه هو أن المدارس تلعب دورًا حيويًا في العملية التعليمية، ولذلك ينبغي للمدارس أن تلعب دورًا في حماية الأطفال من أية إساءة أو تعدي عبر الإنترنت، كما ينبغي أن تتوخى اليقظة بشأن أية علامات أو دلائل لاحتمال تعرضهم للاعتداء الجسدي أو العاطفي من قبل المتطرفين عبر الإنترنت والذين يريدون استقطاب الشباب والعقول البريئة.

حال ساورتك شكوك أو مخاوف بشأن سلامة أحد الطلاب الشباب المعرضين لخطر التطرف، ينبغي لك مناقشة الأمر مع مسؤول حماية الطلاب المُعيّن في مدرستك أو مدير المدرسة أو والدي الطالب.

2-4-5-6 معرفة عوامل الدفع والجذب المرتبطة بالتطرف عبر الإنترنت

يؤمن كثير من الأشخاص بأن التأثير المتزايد للتطرف عبر الإنترنت قائم ببساطة على فكرة أن الأفراد الذين لديهم المعتقدات والقيم نفسها يستطيعون في الوقت الحاضر الوصول بشكل أفضل إلى شبكة الإنترنت، كما لا يزالون يؤمنون بأن عدم المساواة الاجتماعية وضعف مستوى التعليم، بالرغم من ضرورة أخذ هاذين العاملين بعين الاعتبار، ليست هي الأسباب الوحيدة وراء انتشار قضايا التطرف حول العالم وزيادة التغطية الإخبارية العالمية لها.

أوضحت الأبحاث التي تم إجراؤها أنه لا توجد صلة بين التطرف وعدم المساواة الاجتماعية وضعف مستوى التعليم، لكن في الواقع أشار خبراء ومحللو مكافحة الإرهاب أنهم رصدوا تزايد أعداد الشباب من الطبقة المتوسطة الذين يتم استقطابهم وتجنيدهم، وفيما يتعلق بالمتطرفين دينيًا، فإن عددًا كبيرًا من الشباب المراهقين، الذين يتعرضون لهذا المحتوى ويتم استقطابهم وتجنيدهم نتيجة لذلك، لا يمارسون شعائر دينهم بشكل منتظم.

(http://www.theguardian.com/commentisfree/2015/mar/01/what-draws-jihadis-to-isis-identity-alienation)

ينبغي للمعلمين والتربويين أن يدركوا وجود عامل دفع وعامل جذب فيما يتعلق بالتطرف عبر الإنترنت تحديدًا في دول مجلس التعاون الخليجي:

- يشير عامل "الدفع" إلى التدخل الغربي في غالبية الدول المسلمة (على سبيل المثال، التصورات والمفاهيم المتعلقة بقرارات السياسة الخارجية والتي تؤثر بشكل مباشر على المنطقة)

- يشير عامل "الجذب" إلى الفرصة التي تسنح للجماعات المتطرفة (على سبيل المثال، الجماعات الأصولية الدينية) لتشجيع الشباب على تبني أفكارهم ومعتقداتهم الأيديولوجية والتكيف معها والموافقة عليها والمساهمة في قضيتهم.

يقومان معًا بتشكيل هوية عرقية وثقافية ضيقة للغاية، مما قد يؤدي إلى شعور الأفراد بالرغبة في السعي إليها والانضمام لها، على سبيل المثال، مراهق يقضي معظم وقته على الإنترنت وغالبًا ما يشعر بالغربة والانسلاخ عن المجتمعات التي تتّبع المعتقدات والشعائر السائدة للدين الإسلامي، كما أنه قد يشعر بعدم الترحاب أو الألفة فيما يتعلق بالأفكار الغربية، ومع عدم وجود انْدِماج في المجتمع ونقص التوجيه من المعلمين والآباء، فإنهم قد يكتشفون عن طريق الإنترنت والتطرف عبر الإنترنت إيمانهم ومعتقداتهم ومجتمع افتراضي شاسع يمكنهم الاعتماد عليه للحصول على النصيحة.

2-4-5-7 التمكن من التعرف على العلامات والدلائل التي تشير إلى الأفراد المعرضين لخطر التطرف عبر الإنترنت

قد تجعل القضايا التالية الأطفال والشباب عرضة للتطرف عبر الإنترنت:

- أزمة الهوية: البعد عن التراث الثقافي والديني والشعور بعدم الراحة فيما يتعلق بمكانتهم في المجتمع من حولهم.
- أزمة الشخصية: التوترات العائلية، الشعور بالعزلة، تدني احترام الذات وتقديرها، الانفصال عن مجموعة الأصدقاء الحاليين وتكوين علاقات صداقة مع مجموعة جديدة من الأصدقاء ذوي الاهتمامات المختلفة.
- الظروف الشخصية: التوترات المجتمعية المحلية، الإنسلاخ عن قيم المجتمع والنفور منها، الأحداث التي تؤثر على الوطن الأم أو الهوية، وجود شعور بالظلم ناتج عن تجربة شخصية تتعلق بالتعرض للتعصب أو التمييز.
- التطلعات غير الملباة: الشعور بالظلم والفشل ورفض القيم المجتمعية.
- الإجرام: تجارب احتجاز الأحداث، التورط السابق في سلوك إجرامي.

بالرغم من ارتباط القضايا المذكورة أعلاه باحتمال تعرض الفرد للتطرف عبر الإنترنت، إلا أنه توجد تغييرات معينة في السلوك والتي قد تجدها عند أي طفل وينبغي أن يضعها البالغون في اعتبارهم كذلك، ومن بينها الآتي:

- تغييرات عامة في الحالة المزاجية أو أنماط السلوك، السرية
- تغيير الأصدقاء وطريقة ارتداء الملابس
- استخدام لغة غير لائقة أو غير مقبولة
- حيازة كتابات أدبية عنيفة ومتطرفة
- التعبير عن آراء متطرفة
- الدفاع عن أعمال عنف وتأييد الوسائل العنيفة
- التواصل مع متطرفين معروفين (على الإنترنت أو في العالم الواقعي)
- السعي إلى تجنيد الآخرين في أيديولوجيات متطرفة

تشير الأبحاث أيضًا إلى أن الأساليب والوسائل والأدوات المتاحة لمنع مختلف أشكال السلوك المحفوف بالمخاطر تعد هي أيضًا فعالة في منع التطرف عبر الإنترنت والتجنيد في جماعات متطرفة، ونتيجة لذلك، فإن صانعو السياسات يتعاونون مع المدارس (ولا سيما المستشارين والمرشدين والمعلمين) لتقديم مجموعة واسعة من على الأساليب و الموارد للطلاب للحفاظ على الحوار مع المعلمين في بيئة آمنة.

بالإضافة إلى ما سبق، تتوفر أفضل الممارسات في مجال وسائل التواصل الاجتماعي للمساعدة في الحد من خطر أن يجد شخص ما طالب شاب ويحاول التواصل معه، على سبيل المثال، تأكد من تعيين إعدادات الخصوصية لدى طلابك على وضع الخاص في جميع مناصتهم الإلكترونية.

تتوفر أيضًا خيارات على منصات وسائل التواصل الاجتماعي التي تمنع الطلاب الشباب من رؤية محتوى مماثل، على سبيل المثال، يحتوي موقع يوتيوب على زر يُمكنك الضغط عليه لمنع الطلاب من رؤية محتوى ذي صلة بهذا الفيديو، ومن الضروري مراعاة ذلك عند إخبار طلابك الذين قد يتعرضوا لمحتوى غير لائق على صفحاتهم في مواقع التواصل الاجتماعي.

لا تزال هناك حاجة لتحسين وتطوير وسائل وأساليب مكافحة التطرف عبر الإنترنت ومنعه لكن لا يقل ذلك أهمية عن مشاركة محتوى يتعلق بمكافحة التطرف عبر الإنترنت مع المعلمين الآخرين وطلابك وآبائهم وأصدقائك (على سبيل المثال، السلطات المحلية).

اختبار

س1- في حالة نشرك لشيء ما على أحد مواقع شبكات التواصل الاجتماعي، هل سيكون من السهل حذفه فيما بعد؟

أ- نعم
ب- أحيانًا
ج- عادةً
د- لا

س2- أي خاصية في مواقع شبكة التواصل الاجتماعي تحدّد من يمكنه رؤية ملفك الشخصي على الإنترنت؟

أ- إعدادات الوصول
ب- إعدادات الإنترنت
ج- إعدادات الخصوصية
د- إعدادات الاستخدام

س3- أي من المواقع التالية يشتهر بمشاركة مقاطع الموسيقى؟

أ- سكايب
ب- انستغرام
ج- تويتر
د- ماي سبيس

س4- أي من برامج التواصل الاجتماعي التالية يضم أكبر عدد من المستخدمين الفعالين؟

أ- فيس بوك
ب- فليكر
ج- تويتر
د- جوجل +

الإجابات في الصفحة التالية

الإجابات

س 1- د- لا
س 2- ج- إعدادات الخصوصية
س 3- د- ماي سبيس
س 4- أ- فيس بوك

الفصل 2-5

العالم الافتراضي

2-5-1 المراسلة الفورية / غرف الدردشة

2-5-2 الفيديوها، المدونات

2-5-3 ألعاب الإنترنت

2-5-4 تولي المسؤولية

5-2 العالم الافتراضي

1-5-2 المراسلة الفورية / غرف الدردشة

1-1-5-2 التعرف على خاصية المراسلة الفورية وغرف الدردشة

المراسلة الفورية (IM) عبارة عن إرسال رسائل فورية بين مستخدمي الإنترنت وهي شبيه إلى حد كبير بنظام الرسائل النصية في الهواتف المحمولة، وتحظى هذه الخدمات بشهرة واسعة بين الأجيال الشابة، وتستخدم كثيرًا في أماكن العمل لسرعة التواصل بين الموظفين.

وغرف الدردشة هي غرف على الانترنت أو غرف افتراضية يجتمع فيها الأشخاص ذوي الاهتمامات المشتركة للتواصل مع بعضهم البعض في نفس الوقت، على عكس المنتديات حيث تكون وتيرة التواصل والمناقشات فيها بين الأشخاص أكثر بطأ وتكون من خلال نشر الرسائل.

ومن أمثلة المراسلة الفورية "جوجل هانج آوتس" https://hangouts.google.com/ و"سكايب" (انظر الشكل 25أدناه) (www.skype.com)،و"فيس بوك شات" للدردشة مع أصدقائك على موقع فيس بوك المتصلين حاليًا بالإنترنت، كما يمكنك استخدام تطبيقات الإنترنت بما في ذلك تطبيق "فيس بوك" و"فيس بوك ماسنجر".

الشكل 25:مميزات "سكايب" متضمنة المراسلة الفورية، حيث يمكنك أيضًا إجراء مكالمات الفيديو والدردشة عبر الفيديو ومشاركة الصور والفيديو وغير ذلك مجانًا.

أمثلة لغرف الدردشة:

- آي أر سي تو غو (irc2go)(http://en.irc2go.com/online.php).
- شات آورChathour (http://www.chathour.com/).
- غرفة الدردشة المباشرة من فيس بوك (www.facebook.com/LiveChatRoom).
- بالتوك Paltalk (http://www.paltalk.com/g2/webapp/groups/GroupsPage.wmt)

مزايا استخدام غرف الدردشة:

- تمكنك هذه الغرف من التواصل مع أشخاص من مختلف دول العالم لمشاركة الاهتمامات المتشابهة فيما يتعلق بالموسيقى، الترفيه، السياسة والدين في بيئة آمنة ومريحة.
- تمكنك من التواصل مع الناس بطريقة مباشرة وتوفر الكثير من الوقت.
- تمكنك من المشاركة في المجتمعات الموجودة على الإنترنت حيث لا أحكام على المظهر.
- تمكنك من إخفاء شخصيتك، وبالتالي إزالة لحظات الإحراج الأولى عند الدردشة مع شخص غريب.

استخدم غرف الدردشة بأمان والاحتراس من مخاطرها، مثل:

- تتطرق المناقشات في غرف الدردشة إلى العنف أو الأمور غير الأخلاقية، أو إثارة مشاعر الكراهية ضد الآخرين.
- التحرش أو المضايقة التي قد تتعرض لها نتيجة تصرف بعض الناس كيفما شاءوا.
- غرف الدردشة عبارة عن بيئة مناسبة للمصابين بالهوس للأطفال وغيرهم من المتحرشين الذين يسعون إلى التواصل مع الصغار.
- إنشاء العلاقات مع غرباء عبر الإنترنت ضمن غرف الدردشة قد يؤدي إلى التعرض للملاحقة عبر الإنترنت أو إرسال مواد إباحية أو ممارسة الضغوطات لترتيب لقاءات فعلية.
- يعتبر "التقريع" سلوك شائع في غرف الدردشة - حيث قد تتعرض للإهانة الشخصية أو قد تزدري شخصًا آخرًا.

يمكنك التواصل مع الآخرين والدخول إلى برامج المراسلة الفورية وغرف الدردشة في أي وقت من خلال أجهزة الكمبيوتر، الكمبيوتر المحمول، الهواتف اللوحية أو الهواتف الذكية.

2-1-5-2 تعلم كيفية إنشاء ملف شخصي لبرامج المراسلة الفورية

لا بد من تسجيل بياناتك قبل استخدام برامج المراسلة الفورية مثل غرف الدردشة، حيث يتضمن التسجيل في مثل هذه البرامج إدخال بعض التفاصيل الحقيقية مثل العمر والجنس والعنوان، إلا أن الملف الشخصي يسجل عليه المعلومات التي ترغب في اطلاع الغير، ويمكن من خلال هذا الملف الشخصي تسجيل الدخول إلى غرف الدردشة بدون ذكر اسمك،ويمكنك افتراض شخصية وهمية أثناء التواصل عبر الإنترنت غير شخصيتك الحقيقية،اختر اسم مستخدم مميز مع مراعاة تجنب الإساءة للغير، مع العلم أن كثير من غرف الدردشة وخدمات المراسلة الفورية تركز على عدم استعمال المستخدمين على إيحاءات أو لغة غير ملائمة.

وإذا طلب منك، اختر أحد الرموز المصورة (صورة شخصية أو صورة عامة) تناسب شخصية الإنترنت التي تتقمصها، وستظهر هذه الصورة عندما تتصل بالإنترنت،يجب أيضًا عند اختيار الصورة تجنب الصور العدائية أو المحرجة.

2-1-5-3ضبط الخيارات للسماح لقائمة الأصدقاء فقط بالتحدث إليك، وحجب الأشخاص الذين لا ترغب في التحدث إليهم

في غرف الدردشة يمكن أن تختار من تتحدث معه، فإذا شعرت بعدم ارتياح لطريقة الحوار يمكن حظر ذلك الشخص، ولا يمكن لمن قمت بحظره ضمن القائمة السوداء أن يراك عندما تكون متصلاً،وإذا كنت صغيرًا يمكنك أن تضع ضوابط لتحديد من تريد أن يرى بياناتك من المستخدمين ضمن قائمة بيضاء أو قائمة أصدقاء.

القائمة البيضاء هي قائمة بعناوين البريد الإلكتروني أو أسماء المجال التي يسمح برنامج حظر البريد الإلكتروني باستقبال الرسائل منها،أما قائمة الأصدقاء فهي قائمة بمن تود أن تتواصل معهم من المستخدمين.

2-1-5-4 معرفة آليات تعطيل كاميرا الويب

تستخدم بعض غرف الدردشة كاميرا الويب تلقائيًا إذا كانت متوفرة، فإذا لم تكن حذرًا من هذه الكاميرا قد تنتشر مقاطع فيديو محرجة عبر الإنترنت، ولكن يمكن تعطيل هذه الكاميرات بسهولة إذا لم ترغب في استخدام الفيديو، وإليك بعض الإجراءات التي توضح الخطوات:

تمرين - تعطيل كاميرا الويب الموجودة في نظام الويندوز

لتعطيل كاميرا الويب الموجودة في نظام الويندوز،قم بالخطوات التالية :
1- إذهب إلى Control Panel (لوحة التحكم).
2-اختر Device Manager (مدير الجهاز).
3-اضغط بالزر الأيمن للماوس على Integrated Webcam (كاميرا ويب مضمنة)
4-اختر Disable (تعطيل).

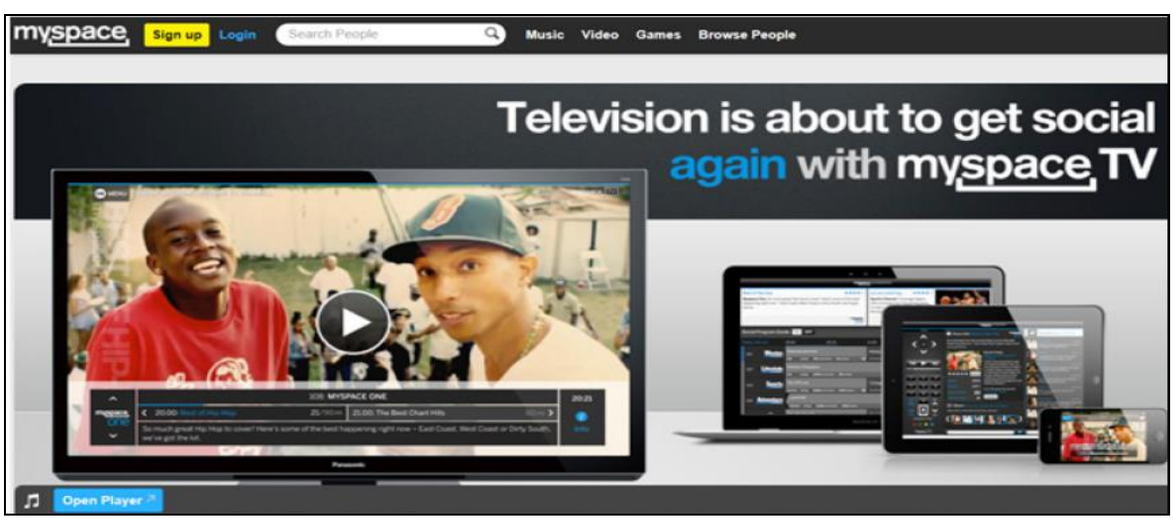
2-5-2 مقاطع الفيديو، المدونات

1-2-5-2 التعرف على إمكانية مشاركة مقاطع الفيديو على الإنترنت من خلال: يوتيوب،ماي سبيس تي في،الخ

تسمح خدمات إضافة مقاطع الفيديو للمستخدمين برفع ومشاركة الصور ومقاطع الفيديو،وقد سهلت الكاميرات وكاميرات الويب وكاميرات الهواتف المحمولة من التقاط الصور التي يمكن رفعها ومشاركتها مع الأصدقاء والعائلة،وفيما يلي بعض مواقع التواصل الاجتماعي التي يمكن من خلالها مشاركة مقاطع الفيديو:

- يوتيوب موقع لمشاركة الفيديوهات (www.youtube.com)
- بريسكوب تطبيق لبث مقاطع الفيديو مباشرة على شبكة الإنترنت (/http://www.periscope.com)
- فليكر موقع لمشاركة الصور ومقاطع الفيديو (www.flickr.com)

انظر الشكل26 أدناه الذي يوضح سهولة المشاركة عن طريق أجهزة التلفزيون أو أجهزة الكمبيوتر أو الكمبيوتر المحمول أو الأجهزة اللوحية أو الهواتف الذكية.



الشكل 26 موقع "بريسكوب" لبث مقاطع الفيديو مباشرة على شبكة الإنترنت (/http://www.periscope.com).

عند استخدام مواقع مشاركة الصور ومقاطع الفيديو ينبغي إتباع الإرشادات وسياسات الأمان وإرشادات الخصوصية الخاصة بها.

يوضح الشكل 27 الموجود في الصفحة التالية المساعدة التي يقدمها موقع "يوتيوب" للمستخدمين والمعلمين والطلاب وغيرهم لكيفية استخدام الموقع بطريقة آمنة، يجب مراعاة القسم الذي يُعنَى تحديدا بالمستخدمين في سن المراهقة.

الشكل 27نصائح الاستخدام الآمن لموقع يويتوب(http://www.youtube.com/yt/policyandsafety/safety.html)

2-2-5-2 استيعاب مفهوم المدونات والمدونات المصغرة وكيفية دمجها مع شبكات التواصل الاجتماعي

كلمة مدونة هي اختصارٌ لمصطلح سجل الويب وهو عبارة عن موقع يحتوي على سلسلة من المشاركات المرتبة زمنيًا من الأحدث للأقدم،وتعتبر المدونة تجسيدًا لك على الإنترنت، فهي مكان لجمع ومشاركة الأشياء التي تراها شيقة - سواء تعليق سياسي أو مذكرات شخصية أو روابط لمواقع تريد أن تتذكرها،وكثير من الناس يستخدمها لتنظيم أفكارهم الشخصية، في حين يستخدمها آخرون للتواصل مع ملايين المتابعين عبر العالم، ويستخدمها الصحفيون المحترفون والهواة لنشر الأخبار العاجلة، بينما يستخدمها الصحفيون المستقلون للإفصاح عن أفكارهم الشخصية.

يمكن ربط المدونة بصفحات التواصل الاجتماعي،لذا يمكن ضبط عملية إدخال المنشورات و البيانات الشخصية ليتم تحديث صفحات التواصل الاجتماعي تلقائيًا.

وخدمة التدوين المصغر هي خدمة شبكية تتيح للمستخدمين معرفة نبذة عن آخر المستجدات من خلال الهواتف الذكية أو أجهزة المحمول،وتكون المدونات عبارة عن جمل صغيرة أو صورة فردية أو روابط لمقاطع فيديو وفي بعض الأحيان يشار إليها على أنها منشورات مصغرة.

3-2-5-2 التعرف على المخاطر المصاحبة لتسريب المعلومات الشخصية أو القذف أو النميمة من خلال المدونات

تستخدم المدونات لتسجل أشياء حدثت من قبل في صورة مذكرات شخصية، وتكون هذه المدونات عبارة عن سجلات عامة - حيث يمكن لأي متصل بالإنترنت أن يقرأها وعلى هذا أي معلومات شخصية ترد فيها تكون متاحة للعامة، وتعامل المعلومات المنشورة في المدونة كما لو كانت معلومات منشورة في جريدة، وإذا ورد في المدونة ما يدل على القذف أو النميمة يمكن مساءلتك على التشهير بالناس.

ممارسات النشر السليمة:

لا تنشر:

- التعليقات التعسفية أو المسيئة للآخرين.
- التعليقات التي قد تسبب إحراجا لك أو للآخرين في أي وقت، فما ينشر على الإنترنت لا يمكن حذفه.
- المعلومات الشخصية لأنها قد تصل بسهولة إلى المجرمين أو المتحرشين أو الجماعات المتطرفة على الإنترنت.
- النميمة على الأصدقاء أو الزملاء أو المعلمين أو غيرهم من الناس.

انشر:

- التعليقات الصحيحة والتي لا تنطوي على افتراء.
- التعليقات الصادقة التي تعبر عن أفكارك دون تجريح في الآخرين.
- التعليقات ذات الصلة بالموضوع.

4-2-5-2 استيعاب آليات عمل مواقع مشاركة الملفات واحتمالية الإصابة بالفيروسات والبرامج الضارة أثناء استخدام مواقع مشاركة الملفات

تسمح مواقع مشاركة الملفات للمستخدمين بمشاركة محتويات مثل الموسيقى والأفلام ونقلها إلى أجهزتهم، وهذا عن طريق مستخدمين متصلين بشبكة مباشرة متصلة بالإنترنت وإتاحة الملفات لمستخدمين آخرين متصلين بنفس الشبكة، والشبكة المباشرة تعني أن الملفات تنقل من جهازك الخاص إلى جهاز الطرف الآخر بشكل مباشر أو العكس بالعكس, على سبيل المثال، يتصل المستخدم بإحدى الشبكات المباشرة ثم يبحث عن أغنية معينة، فتقوم الشبكة بالبحث في كافة الأجهزة والمشغلات المتصلة والتي لديها الأغنية المطلوبة، فيبدأ المستخدم في نقل نسخة من الأغنية إلى جهازه، وهذه هي عملية مشاركة الملفات، حيث تتيح الشبكة ملفات كافة المستخدمين للمشاركة مع بعضهم بعضًا.

وتعد مخاوف الإصابة بالفيروسات وغيرها من البرامج الضارة هو محور اهتمام المستخدمين الذين ينقلون ملفات من أجهزة كمبيوتر مجهولة لأن بعض الفيروسات تتخفى في صورة ملفات لأغاني أو أفلام، ومع تنزيل نسخة من أي ملف تكون هناك فرصة سانحة لانتشار الفيروس خلال الشبكة، في حين يستخدم بعض قراصنة الإنترنت عملية مشاركة الملفات كطريقة لإطلاق البرامج الضارة.

أمثلة لمواقع مشاركة الملفات:

- **فورشيرد** موقع المشاركة المجانية للملفات والفيديو والموسيقى والكتب والألعاب وغيرها (http://www.4shared.com/)،انظر الشكل 28أدناه.
- **هايتيل** موقع المشاركة المجانية للملفات الكبيرة (https://www.hightail.com).
- **فيل كونفوي** موقع لخدمات تبادل الملفات كبيرة الحجم مجانًا (www.fileconvoy.com).
- **شير فيل** موقع لمشاركة الملفات المهنية (www.sharefile.com).

الشكل 28: موقع فورشيد - مثال لمواقع مشاركة الملفات - (http://www.4shared.com/)

5-2 العالم الافتراضي

3-5-2 ألعاب الإنترنت

1-3-5-2 الاحتراس من ألعاب تقمص الأدوار (RPG) الموجودة على الإنترنت وما يتعلق بها من مخاطر مثل: اللاعبون المجهولون والوصول لمستوى الإدمان.

تتيح الألعاب التفاعلية فرصة التنافس مع لاعبين آخرين على الإنترنت، ولكنها محفوفة بالمخاطر، فلا يرى اللاعبون إلا رموزًا مصورة لبعضهم دون معرفة شخصياتهم الحقيقية.

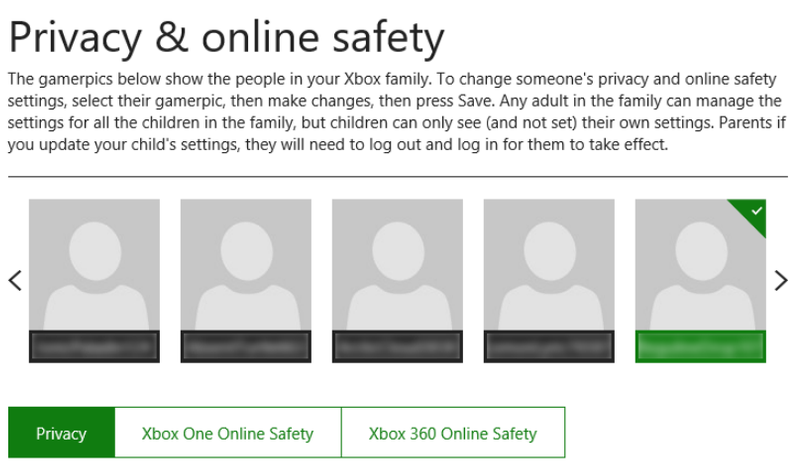
قد يدمن بعض اللاعبين هذه الألعاب ويقضوا معظم وقت فراغهم في هذا العالم الافتراضي، وتعد ألعاب الإنترنت من الأنشطة الثانوية الداخلية؛ لذا فإن قضاء الكثير من الوقت في ممارستها قد يؤدي إلى مشاكل صحية واضطرابات في العمل بالإضافة إلى مشاكل جسدية وانهيار العلاقات الشخصية.

2-3-5-2 الحرص على معرفة كيفية تعيين إعدادات الخصوصية لمنع الغرباء من التواصل مع الشباب في الألعاب.

يعد تغيير إعدادات الخصوصية وإعدادات الأمان عبر الإنترنت الخاصة بالألعاب من الوسائل التي تُمكنك من حماية نفسك من التعرض للهجمات عبر ألعاب الإنترنت، وينبغي لك استشارة شخص بالغ لمساعدتك في تعيين إعدادات الخصوصية للعبة، إذا دخل طلابك إلى وحدة تحكم الألعاب فمن المهم أن يكونوا على دراية بإعدادات الخصوصية والأمان الخاصة بها.

إذا كان لديك على سبيل المثال, لعبة PlayStation 4 أو XBox أو وحدات ألعاب أخرى، يمكنك تغيير إعداداتك من خلال اتباع الخطوات الثلاثة التالية:

- قم بتسجيل الدخول إلى حسابك (مثال XBox Live) حيث يجب أن تكون متصلاً بالإنترنت لإجراء هذه التغييرات.
- حدِّد علامة تبويب الخصوصية (أو الأمان على الإنترنت) وفقًا للإعداد المطلوب تغييره لحساب الطفل.
- راجع الإعدادات بشكل مناسب, ثم حدِّد Save (حفظ).



إخلاء المسؤولية: قد يتم تقييد الأطفال والمراهقين فيما يتعلق بتغيير إعدادات الخصوصية والأمان عبر الإنترنت لحسابهم الخاص (منها Xbox One، على سبيل المثال).

سواء كان يمكنهم فعل ذلك بشكل مستقل أم لا، فمن المهم مناقشة قضايا الألعاب عبر الإنترنت مع الآباء لتوعية الأطفال حول سلامة هذه الخيارات وكيف يمكن منعهم من التواصل مع الغرباء لمنع خطر التعرض للاستغلال.

4-5-2 تحمّل المسؤولية

1-4-5-2 لا يجب تعميم كيف تكون مواطنًا مسؤولاً في العالم الرقمي من خلال عدم تعميم الرسائل أو الصور أو غيرها من المواد التي يمكن أن تكون مؤذية، ومشاركة الصور مع الأشخاص الذين تعرفهم وتثق بهم فقط.

أولا وقبل كل شيء، يجب أن تشارك الصور فقط مع من تعرفهم وتثق بهم, لأن مشاركة الصور مع الغرباء قد يؤدي إلى مشاكل لا حاجة لها ويعرضك لجذب الانتباه غير المرغوب فيه والإساءة المحتملة, فالطبيعة اللحظية والوصول الواسع لمواقع شبكة التواصل الاجتماعي يعني أن الهجمات الشخصية يمكن أن تحدث وتتصاعد بسرعة كبيرة سواء بين الأفراد أو الجماعات، وبذلك فإن الضرر الناتج قد يكون غير قابل للإصلاح. هذه المعلومات تتعلق بضمان عدم تعرض كل من المعلمين والطلاب للتحرش.

ثانيًا وبنفس الأهمية لا تتداول الرسائل أو الصور المؤذية لمن هو مذكور بها أو لمن يتلقاها، وضع نفسك في نفس الموقف.

2-4-5-2 معرفة كيفية رفض أو منع الغرباء والاتصالات غير المرغوب فيها، والحذر من التخطيط لمقابلة أشخاص لا تعرفهم،حتى لو كانوا أصدقاء لك على الإنترنت.

عندما يحاول الغرباء بلا كلل إضافتك على موقع تواصل اجتماعي أو إرسال دعوات لك،يمكنك حجب هذه الطلبات باستخدام خيارات هذا الموقع،فكل اتصال جديد يمر عبر عملية موافقة يمكنك من خلالها أن تقبل هذا الاتصال أو تتجاهله أو تحظره.

وأما الاتصالات الموجودة بالفعل على الموقع فإنها قد تسيء التصرف،ومن ثم يمكنك حظرها يدويا عن طريق الذهاب إلى إعدادات الموقع،فموقع "فيس بوك" على سبيل المثال يتطلب منك تحديد الصفحة الخاصة بهذه الاتصالات،حيث يوجد أعلى الصفحة بجوار صورة الملف الشخصي مجموعة خيارات بها خيار "حظر" ، فبمجرد تحديد هذا الخيار لن يتمكن هذا الصديق من رؤيتك أو مراسلتك.

وتذكر أن أصدقاء الإنترنت الذين لم تقابلهم من قبل ليسوا بالضرورة أصدقاء حقيقيين ويجب عليك التفكير في مقابلتهم بالفعل،كما يجب عليك اصطحاب بعض أصدقائك لتأمين المقابلة،وتجنب تبادل معلومات عن حياتك حتى تقام علاقة قوية مع الوقت.

2-5-4-3 استخدام كاميرا ويب مع من تعرفهم فقط،وفصلها أو تعطيلها عند عدم الاستخدام

كاميرا الويب، وفقا لمعايير الإنترنت، تعني أنك تدعو شخصًا ما لمنزلك،فهل تود ذلك؟ ربما لا،ولذا يفضل عدم استخدام الكاميرا مع الغرباء،فإذا أردت ذلك في ظل ظروف معينة،يستحسن أن تأخذ جهازك،إذا كان محمولا مثل الكمبيوتر اللوحي أو الكمبيوتر المحمول،وتذهب إلى مكان آخر مثل المقهى،المكان المناسب لمقابلة شخص جديد.

وعند عدم استخدام الكاميرا تأكد من فصلها أو تعطيلها،حيث يمكنك تعطيلها من خلال خيارات الإعدادات الموجودة في التطبيقات التي تستخدم الكاميرا،وإذا كنت تستخدم كاميرا مزودة بسلك USB، افصل السلك لتعطيلها.

2-5-4-4 معاملة الآخرين على الإنترنت بما تحب أن يعاملوك به

على الرغم من أن العالم الافتراضي يبدو وكأنه عالم غير حقيقي أحيانًا،إلا أنه يجب عليك أن تدرك أن مستخدمي الإنترنت هم أشخاص حقيقيون ولديهم مشاعر حقيقية ولكل منهم لحظات من الفرح والحزن،ومن ثم ينبغي عليك معاملة الناس على الإنترنت بما تحب أن يعاملوك به،فهذه القاعدة ستحميك ومن تتواصل معهم في العالم الافتراضي.

2-5-4-5 إدراك أن تنزيل الموسيقى والأفلام والصور وبرامج الكمبيوتر والألعاب من على الإنترنت قد يكون مخالفًا للقانون ما لم ينص على ذلك صراحة على الموقع المستخدم

كمعلم، تتجاوز كيفية تفاعل الطلاب في الفصول الدراسية ما هو أبعد مما يقولون، من المهم أن تتعامل بلطف وبصورة ودودة مع الأشخاص على الإنترنت ولكن إذا رأيت شخصًا ما يتم التعدي عليه عبر الإنترنت، فمن واجبك مساعدته لتكون مواطنًا صالحًا في العالم الرقمي.

وإذا ما أردت بعد ذلك تنزيل ملفات بشكل غير قانوني،يرجى التفكير في البيان التالي: إننا جميعًا نعمل من أجل كسب الرزق ولا يمكننا العيش بدون ما نحصل عليه من أموال، فلدينا فواتيرَ مستحقة الدفع وأطفالا يريدون الأكل وعقارات تستوجب مبالغ الإيجار،كما أن صناع هذه المواد يعيشون على ما يربحونه من مال منها،فإذا ما أخذ مستخدمو الإنترنت هذه المواد دون مقابل،فإنهم يؤذون كل من شارك في صنع ما نستمتع به من هذه المواد.

6-4-5-2 تعلم استراتيجيات مختلفة للتعامل مع البلطجة الانترنت وماذا تفعل إذا كان ناشئا

- إذا كنت مستهدفًا من قبل المتعدين عبر الإنترنت، فمن الضروري عدم الرد على أية رسائل يتم إرسالها لك، بغض النظر عن مدى الإساءة التي تحملها أو عدم صحتها أو كونها مؤلمة أو مؤذية، ومع ذلك، فمن الضروري عدم التفكير في الانتقام أو مشاركة منشور عن الحادث على الإنترنت لأن هذا الامر سيزيد الوضع سوءًا، وبدلاً من ذلك، ينبغي لك مواجهة التعدي عبر الإنترنت عن طريق: الاحتفاظ بدليل على تعرضك للتعدي عبر الإنترنت من خلال حفظ الرسائل النصية أو لقطات الشاشة أو تسجيل فيديو على هاتفك المحمول.
- إبلاغ شخص بالغ عن الحادث على الفور سواء كان والديك أو إدارة مدرستك.
- احرص على وقف كافة سبل الاتصال مع المتعدي عبر الإنترنت، بعد حفظ الدليل، عن طريق حظر رقم هاتفه وعنوان بريده الإلكتروني وحذفه من قائمة جهات الاتصال على وسائل التواصل الاجتماعي.

سوف يكون تناول موضوع التسلط عبر الإنترنت أمرًا في غاية الصعوبة بشكل مؤكد ما لم يتم تضمينه في البنية الهيكلية التعليمية من قِبَل المدارس والمُعلمين, ويمكن أن يلعب المعلمون دورًا مباشرًا في التعامل مع التسلط عبر الإنترنت من خلال إنشاء خطط الدروس التي تدور حول القضايا والأساليب المستخدمة لتجنب التعدي الإلكتروني، ولكن الأهم من ذلك يكمن في توعية الطلاب بتداعيات نشر أشياء مؤلمة ومؤسفة على الإنترنت، يقدم موقع Digizen ومؤسسة كومن سنس ميديا خطوط رائعة لدروس حول هذا الموضوع، (ارجع إلى الروابط أدناه.)

http://www.digizen.org/downloads/cyberbullying_lesson.pdf
https://www.commonsensemedia.org/educators/lesson/cyberbullying-crossing-line-6-8

يمكنك أيضًا خلق فرص للطلاب للبحث في الموضوع بأنفسهم والتفكير في طرق مبتكرة لزيادة وعيهم بالتسلط على الإنترنت، ويمكن تخصيص المشاريع على أساس مواضيع محددة في نطاق التسلط على الإنترنت ومناقشة الكيفية التي تؤثر عليهم وعلى غيرهم داخل المجتمع المحلي، كما أنه يساعدهم على الانخراط في محادثات في محاولة لإيجاد حلول خاصة بهم حول كيفية الحد من التسلط على الإنترنت.

وأخيرا وليس آخرا، ينبغي الإقرار بأنه قد يكون هناك بعض الطلاب الذين قد لا يشعرون بالراحة في الحديث إلى شخص يشاركهم حياتهم على أساس يومي مثل المعلم أو أحد الوالدين بسبب الوصمة السلبية التي قد تلحق بهم، لذلك، يمكن للشخص الرجوع أيضًا إلى طرف آخر - مثل مستشار التوجيه - الذي يمتلك المهارات الفنية والخبرة المهنية للتواصل مع الطلاب بشكل مريح بدرجة أكبر.

اختبار

س1- ما هي التقنية التي تمكنك من إرسال رسالة فورية إلى مستخدم آخر عبر الإنترنت؟

أ- الرسائل الفورية
ب- الرسائل النصية الفورية
ج- التعرف الفوري على الأصوات
د- البريد الفوري

س2- ما هي الخاصية التي تمكنك من تحديد من تريد التواصل معهم داخل غرف الدردشة؟

أ- قائمة الأصدقاء
ب- قائمة الأصدقاء المفضلين
ج- القائمة السوداء
د- القائمة الخضراء

س3- ما هي الخدمة التي تمكنك من مشاركة الصورة بطريقة آمنة من خلال الإنترنت؟

أ- فليكر
ب- يوتيوب
ج- المراسلات الفورية
د- آي تيونز

س4- أي من الأشياء الآتي ذكرها يمثل خطرًا على مواقع مشاركة الملفات؟

أ- تعطل أجهزة الكمبيوتر
ب- فقدان المساحة التخزينية
ج- هجمات فيروسات الكمبيوتر
د- عدم قدرة جهاز الكمبيوتر على النسخ الاحتياطي بطريقة جيدة

الإجابات في الصفحة التالية

الإجابات

س1- أ- الرسائل الفورية
س2- ب- قائمة الأصدقاء المفضلين
س3- أ- آداب التعامل على الإنترنت
س4-ج- هجمات فيروسات الكمبيوتر

الفصل 6-2

التعلم سويًا

6-2-1 المناقشة

6-2-2 المراقبة الأبوية

6-2-3 إدمان الإنترنت

6-2 التعلم سويًا

1-6-2 المناقشة

1-1-6-2 التعلم سويًا ومناقشة موضوع استخدام الكمبيوتر مع أصدقائك وأسرتك

يستخدم الطلاب الإنترنت بانتظام، وقد يمارس هؤلاء نشاطات عبر الإنترنت أكثر من آبائهم، ورغم أن معظم استخدامات الإنترنت إيجابية إلا أنهم قد يحيدون عنها ويتجهون لاستخدام طرق تجعلهم عرضة للخطر مثل المضايقات على الإنترنت أو استمالة الأطفال واستغلالهم، ولضمان سلامتك عبر الإنترنت، ناقش مع أسرتك وأصدقائك أسباب استخدامك للإنترنت واطرح على والديك ومعلميك بعض الأسئلة خاصة إذا لم تكن على دراية بذلك.

2-1-6-2 قبول حقيقة أن ترك أجهزة الكمبيوتر المنزلية في مواقع مركزية مفتوحة هو الإجراء الأفضل

يعد أفضل مكان لوضع جهاز الكمبيوتر فيه هو المكان الذي يستطيع أفراد الأسرة جميعهم استخدامه بدلاً من أن يكون داخل غرفة النوم، مما يساعد على خلق شعور بالشفافية مع الوالدين فيما يتعلق بالمحتويات التي يتم الدخول إليها على الإنترنت، ويمكن إعداد ملفات تعريف المستخدم لكل فرد من أفراد الأسرة، بجانب وضع قواعد محددة لاستخدام الإنترنت لضمان استمتاعك وجميع أفراد أسرتك بالاستخدام الآمن للإنترنت.

يجب أن يكون معلومًا أن ليس من الخطأ التحدث إلى الوالدين، وأن ما تقوم به من أنشطة عبر الإنترنت بشكل منتظم لا يُعد أمرًا خاطئًا، ولا يعزو الأمر في ذلك إلى الفضول ولكن لحرصهم على توجيهك والحد من المخاطر كالتعرض لمحتوى غير لائق أو سرقة المعلومات الشخصية.

3-1-6-2 الإلمام ببرامج التصفية والمراقبة من أجل تصفية الصور الإباحية وأنشطة التسجيل عبر الإنترنت وضبط مؤقتات الإنترنت وحظر إرسال المعلومات الشخصية عبر البريد الإلكتروني أو نشرها

باستخدام برامج التصفية على الإنترنت، يصبح الدخول إلى المحتوى الذي قد يكون إباحيًا أو غير قانوني أو مضر محجوب عن أي شخص يستخدم الكمبيوتر، تجدر الإشارة إلى أن هناك نوعين من برامج التصفية: أحدهما مثبت في برامج نظام التشغيل بحيث يمكن إدارته من سطح المكتب وآخر يقدمه مزودو خدمات الإنترنت (ISP)، وتشبه برامج التصفية قوائم حجب المحتويات الضارة أو غير اللائقة في جودتها وهي معدة خصيصًا لهذه المحتويات، ومن خلال فحص هذه البرامج مع مزودي خدمات الإنترنت، تأكد أن خيارات الرقابة الأبوية أو التصفية متوفرة كجزء من خيارات الخدمة.

هذا ويقوم برنامج المراقبة بتسجيل كل الأنشطة التي يمارسها الأبناء على جهاز الكمبيوتر، بالإضافة إلى ما يقدمه هذا البرنامج من معلومات عن مختلف المواقع الإلكترونية التي تمت زيارتها مثل "فيس بوك" أو أية أنشطة تواصل اجتماعي أخرى مثل الدردشة وخدمة الرسائل الفورية فضلاً عن أنشطة البحث، كما أن هذه البرامج تضيف وسائل مراقبة أخرى مثل التنبيه بأي رسائل إلكترونية تم إرسالها لإضافة مستوى آخر ضمن برامج المراقبة، ولبرنامج المراقبة الأبوية الذي يأتي في بعض الأحيان مثبتًا على الكمبيوتر مجموعة من الميزات الإضافية.

ثمة أمثلة لبعض البرامج التي يمكن تنزيلها مجانًا للمساعدة في مراقبة استخدام الأطفال للإنترنت وحجب المواقع الإلكترونية:

- برنامج كاي 9 ويب بروتكشن (K9 Web Protection) (انظر الشكل 1 أدناه) - http://www1.k9webprotection.com/
- Hidetools HT Parental Controls (برنامج هايد تولز اتش تي للمراقبة الأبوية) - http://www.hidetools.com/parentalcontrol.html
- NCH Software (برنامج إن سي اتش سوفت وير) - http://www.nchsoftware.com/childmonitoring/index.html

باستخدام برامج المراقبة الأبوية يمكنك التحكم في:

- الفترات الزمنية للحيلولة دون دخول المستخدم خلال ساعات محددة.
- الألعاب التي تناسب فئة عمرية محددة وحجب الألعاب التي لم يتم تصنيفها أو ألعاب أخرى معينة.

الشكل 29 برنامج K9 Web Protection

تدريب - استخدام Windows 7 لإعداد أنظمة لتصنيف اللعبة باستخدام برامج المراقبة الأبوية

1- انقر فوق الزر Start (ابدأ)
2- انقر فوق Control Panel (لوحة التحكم).
3- انقر فوق User Accounts and Family Safety (حسابات المستخدم وسلامة العائلة) ثم انقر فوق خيار Set up Parental Controls (إعداد برامج المراقبة الأبوية) الموجود تحت Parental Controls (برامج المراقبة الأبوية)، (قد يطلب منك كلمة مرور مسؤول، اكتب كلمة المرور وفقا للتعليمات الموجودة على الشاشة)
4- انقر فوق Game Rating System (نظام تصنيف اللعبة)، وسيُطلب منك تحديد نظام تصنيف لعبة، حيث إن هذا النظام يفحص محتوى الألعاب ويعين التصنيفات العمرية لها، على غرار نظام تصنيف السن المطبق على الأفلام، وكل خيار له رابط للموقع المطابق له للحصول على معلومات إضافية.

ينطبق التصنيف العمري على كافة المستخدمين.

2-6-2 المراقبة الأبوية

1-2-6-2 إدراك أن برامج المراقبة الأبوية متوفرة في مجموعة من أجهزة الوسائط مثل: التلفزيون الرقمي، ألعاب الفيديو والكمبيوتر والهواتف المحمولة وأجهزة iPods والأجهزة اللوحية وبرامج الكمبيوتر

يستطيع والداك كشف ما يمكنك رؤيته على الإنترنت ومراقبته والتحكم فيه وذلك بهدف عدم تعرضك لمحتوى غير لائق، ففي أجهزة التلفزيون الرقمية، يمكن إغلاق قنوات معينة؛ لذا يتعين على المستخدم إدخال رمز PIN لمشاهدة هذه القنوات، كما يوفر مزودو خدمات الهواتف المحمولة وسائل مراقبة أبوية وأنظمة تصفية محتوى مجانية تسمح لأبويك بوضع ضوابط تتحكم فى المحتوى الذي تقوم بتنزيله على هاتفك، إن استخدام برامج المراقبة يجعل والديك يضطلعون بمسؤولية استخدام هاتفك المحمول، حيث يمكنهم حجب أرقام معينة أو تقييد المكالمات الصادرة لقائمة مسموح بدخولها مسبقًا وتعطيل الهاتف خلال ساعات الدراسة الرسمية على سبيل المثال، كما يتيح الاستخدام المزدوج لهاتفك المحمول ولوالديك حق الوصول إلى السجلات فيما يتعلق بحسابك، بما في ذلك كل الأرقام المتصلة.

كما يمكن تنزيل تطبيقات المراقبة الأبوية مباشرةً على الهواتف الذكية ومن أمثلة ذلك:

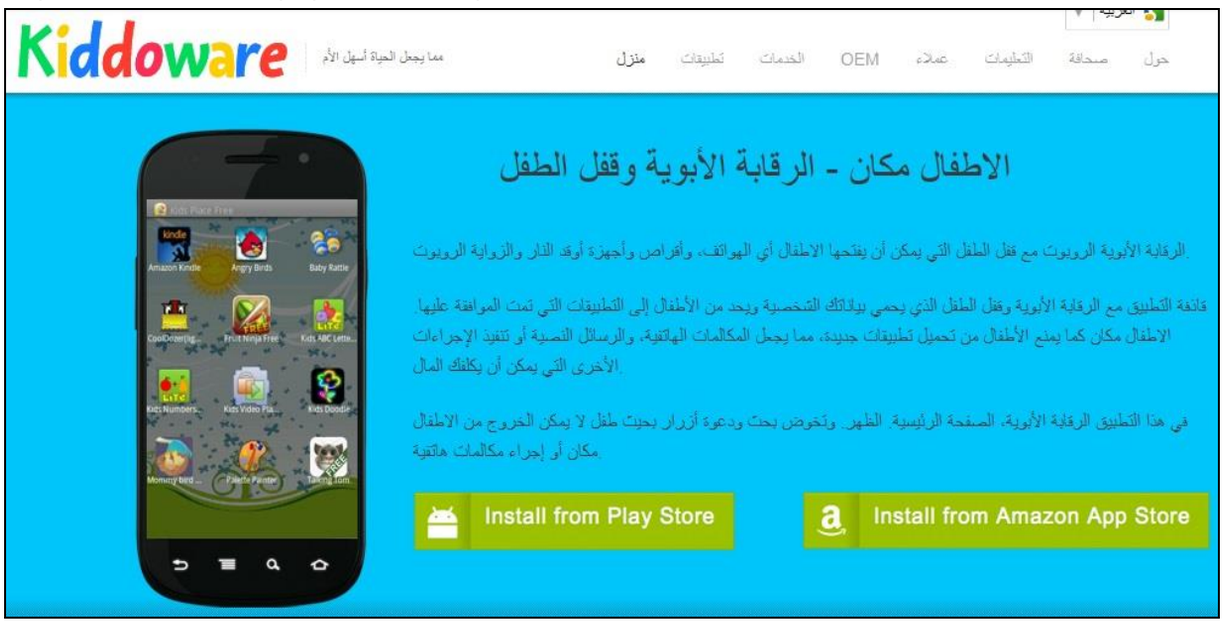
تطبيق Mobile Minder - على موقع http://www.mobileminder.com/ ووسائل الرقابة الأبوية لأجهزة الهاتف. تطبيق Myfone.mobi - على موقع
https://play.google.com/store/apps/developer?id=Myfone.mobi

يمكن إعداد برامج المراقبة الأبوية على مجموعة من الأجهزة الذكية بما في ذلك الأجهزة اللوحية وأجهزة الآي باد وبرامج الكمبيوتر، هذا وتشتمل أنظمة التشغيل مثل Windows على برامج المراقبة الأبوية وتتخذها مقياسًا، كما يتشجع الآباء للتعامل بجانب الأطفال لتوفير بيئة أكثر أمانًا في مجال الكمبيوتر.

يعد جهاز الآي باد مثالاً شهيرًا على الأجهزة اللوحية حيث يمكنك وضع الضوابط المعروفة أيضا ببرامج الرقابة الأبوية بهدف منع الوصول إلى محتويات أو خصائص معينة مثل متصفح سفاري ويوتيوب والموسيقى والألعاب الخ

لتفعيل خاصية الضوابط على جهاز الآي باد، انقر فوق خيارnsRestrictio (الضوابط) الموجود تحت General Settings (الإعدادات العامة) ثم انقر فوق Enable Restrictions (تمكين الضوابط) وأدخل كلمة مرور، حيث إن كلمة المرور ضرورية لتغيير الإعدادات أو تعطيل الضوابط، كما يمكن تهيئة كلمة مرور لجهاز الآي بإتباع الخطوات التالية: General > Pass code Lock < Settings (الإعدادات> عام > قفل كلمة المرور)

يوجد العديد من التطبيقات قابلة للتنزيل مجانًا للهواتف المحمولة والأجهزة اللوحية للحفاظ على سلامة الصغار والبالغين خلال استخدامهم للإنترنت، ومن هذه التطبيقات تطبيق كيدز بلاس (Kids Place) (انظر الشكل 30 أدناه):



الشكل 30: مثال لبرامج المراقبة الأبوية – KidsPlace
(http://www.kiddoware.com)

2-2-6-2 ضبط برامج المراقبة الأبوية على برامج التشغيل.

لإعداد برامج المراقبة الأبوية على جهاز كمبيوتر يعمل ببرنامج تشغيل Windows 7، اتبع الخطوات التالية:

- اضغط على الزر Start (بدء) واختر Control Panel (لوحة التحكم).
- اضغط User Accounts (حسابات المستخدم) وFamily Safety (سلامة العائلة).
- أضف حساب مستخدم لكل شخص يستخدم هذا الكمبيوتر ثم حدد كلمة مرور لكل حساب.
- اضغط Parental Controls (برامج المراقبة الأبوية)، ثم قم بما يلي لكل مستخدم:
  - حدد عدد الساعات وعدد الأيام التي يمكن فيها لهذا الشخص استخدام الكمبيوتر.
  - الألعاب مصنفة حسب الفئة العمرية، قم بإعداد مجموعة عمرية مناسبة لهذا المستخدم، واسمح ببعض الألعاب واحجب بعضها.
  - اسمح للمستخدم تشغيل أي برنامج على الكمبيوتر أو حدد البرامج التي يمكن للمستخدم أن يشغلها.

3-2-6-2 كيفية تثبيت بعض برامج المراقبة الأبوية أو تنزيلها: www.parentalcontrolbar.org

هناك العديد من برامج المراقبة الإلكترونية التي تسمح لك بحجب المحتوى غير اللائق من الكمبيوتر كما تتيح تسجيل المواقع التي تمت زيارتها للتأكد من إذا ما كانت هذه المواقع مناسبة أم لا، كما أن بعضًا من هذه البرامج تجارية لكن أكثرها يمكن تنزيله مجانًا، وتتضمن الخيارات برنامج Net Nanny، وK9 Web Protection، و Parental Control Bar لمتصفح **Internet Explorer** وSafari وProCon Latte وتطبيق FoxFilter لمتصفح Firefox.

لتثبيت خدمة Parental Control Bar:

1- اذهب إلى موقع www.parentalcontrolbar.org (انظر الشكل 31 أدناه)

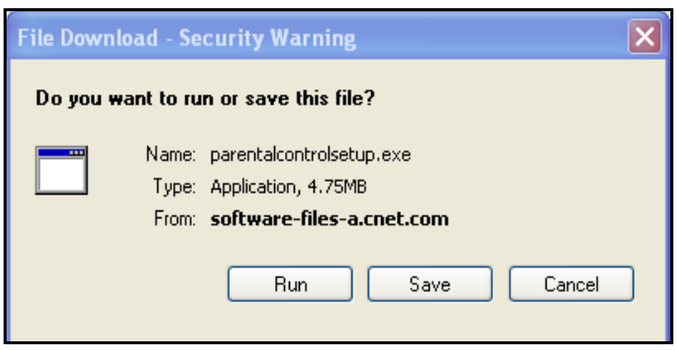
شكل 31 http://www.parentalcontrolbar.org/

2- انقر فوق رابط Download Now (تنزيل الآن) الموجود أعلى الناحية اليمنى.

3- سوف يأخذك هذا الرابط إلى موقع (download.cnet.com)، حيث ستنقر فوق زر Download Now (تنزيل الآن) الموجود على الجانب الأيسر للصفحة. (انظر الشكل 32 أدناه)

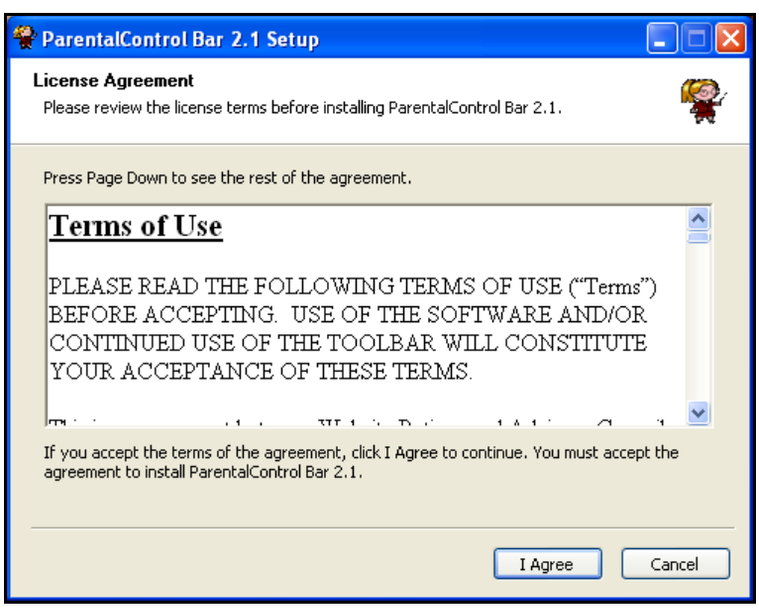
شكل. 32 رابط التنزيل

4- تظهر شاشة File Download – Security Warning (تنزيل الملف - تحذير أمني) حدِّد زر Run (تشغيل) كما هو موضح في الشكل 33 أدناه.



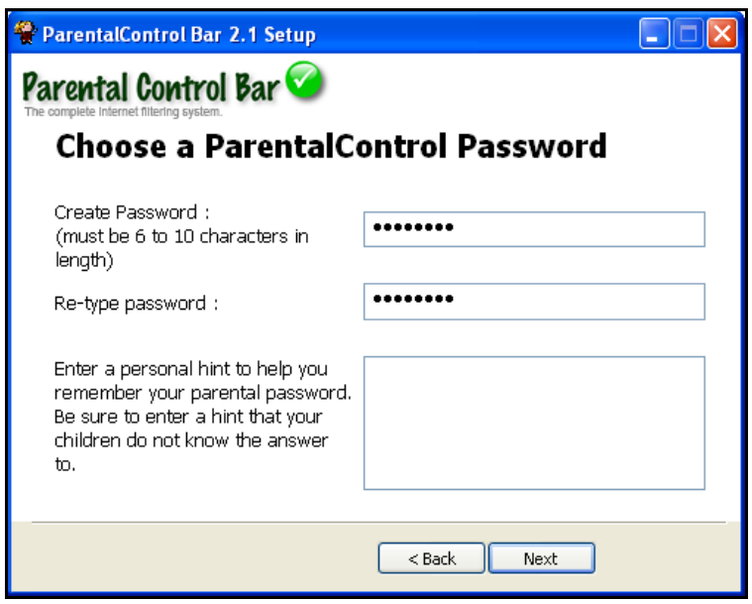
الشكل 33 - نافذة Run or Save (تشغيل أو حفظ)

5- بمجرد تنزيل التطبيق وتشغيله، تنبثق نافذة Terms of Use (شروط الاستخدام) فحدد رز I Agree (أوافق). (كما هو موضح بالشكل 34 أدناه).



شكل 34 اتفاقية ترخيص مستخدم إنترنت بين الآباء والأطفال.

6- من خلال النافذة Parental Control Bar يمكنك إنشاء كلمة مرور وتأكيدها وذكر تلميح يساعدك على تذكرها حال نسيانها، وبمجرد إدخال المعلومات المطلوبة، حدد زر Next (التالي) (كما في الشكل 35 أدناه).

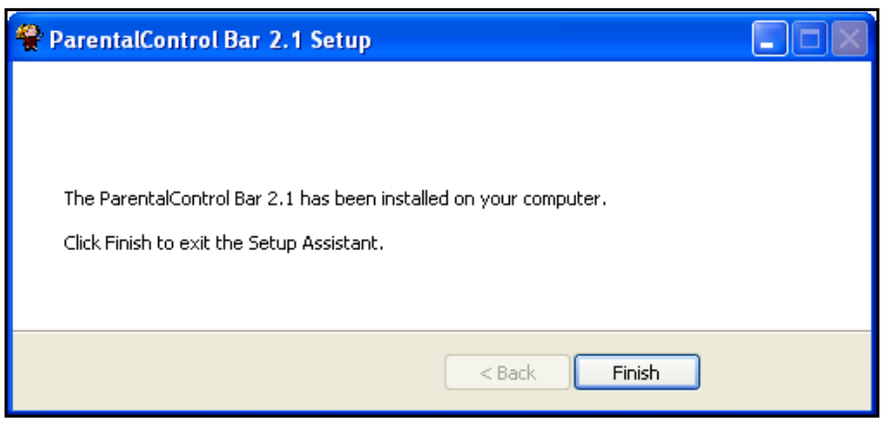


الشكل 35 اختيار كلمة مرور

7- أسفل العنوان Forgotten Password Assistance (المساعدة عند نسيان كلمة المرور) الموجود في النافذة التي تراها على الشاشة، أدخل البريد الإلكتروني مرتين وفقًا لذلك، ثم اضغط على الزر Next (التالي)، (انظر الشكل 36 أدناه). فهذا سوف يحدد حساب البريد الإلكتروني الذي يمكنه إعادة تعيين كلمة المرور حال نسيانها.

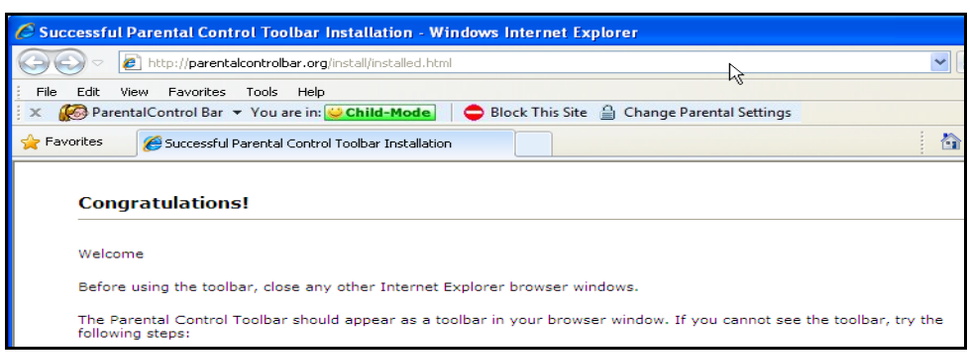
الشكل 36 - المساعدة عند نسيان كلمة المرور

انقر فوق زر Finish (إنهاء) للخروج، انظر الشكل 37 أدناه.



الشكل 37 - نافذة اتمام الإعداد

انتهت عملية التثبيت، ويمكنك الآن رؤية صفحة Congratulations! (تهانينا!) على متصفح الإنترنت كما هو موضح بالشكل 38 أدناه.



الشكل 38: صفحة التهنئات

للحصول على مساعدة لميزات المنتج اتبع التوجيهات الواردة أدناه:

1- أدخل هذا الرابط http://www.parentalcontrolbar.org في شريط العنوان لكي يتم تحويلك إلى صفحة موقع الويب الرئيسية.
2- انقر فوق علامة التبويب Product Features (ميزات المنتج) الموجودة أمامك.
3- كما ترى في الشكل 11 أدناه، فإن Control Bar Help Menu (قائمة مساعدة شريط التحكم)، و The Child Mode (وضع الطفل)، وEasily Block Adult Sites (حظر مواقع البالغين بسهولة)، وChange Parental Settings (تغيير الإعدادات الأبوية) تحتوي على تعليمات مفصلة تساعدك على التعرف على طرق حماية أطفالك على الإنترنت.

الشكل 39 - المساعدة عند نسيان كلمة المرور

4-2-6-2 التعرف على أهمية إنشاء حسابات مستخدم مختلفة بامتيازات وصول لكل حساب.

هناك العديد من الأسباب الهامة وراء ضرورة إنشاء حسابات مستخدم مختلفة.

- حسابات المستخدمين تفصل حسابات البريد الإلكتروني وتوفر المزيد من الخصوصية.
- يتم حفظ تفضيلات المواضيع وخيارات العرض والإعدادات الأخرى القابلة للتخصيص لكل مستخدم.
- هناك تحسن أمني لأن الوصول يمكن أن يكون مختلف لكل مستخدم مما يحد من وصول الأطفال لبعض المواقع ويطلب موافقة حساب مسؤول قبل تثبيت التطبيق للحد من هجمات الفيروسات المحتملة.

تقليل مشاكل تبادل الملفات لأن كل مستخدم يحصل على مجلد خاص به.

5-2-6-2 التعرف على أسباب إنشاء حساب إلكتروني للطفل وتوجيه الرسائل الواردة بصندوق الوارد ببرنامج المراقبة الأبوية لاستعراضها.

للسبب ذاته، يقوم الآباء بإنشاء حسابات مختلفة للمستخدم؛ لذا يحق لكل فرد أيضًا أن ينشئ حساب البريد الإلكتروني الخاص به.

ومن بين برامج المراقبة التي يمكن وضعها على حساب البريد الإلكتروني:

- تقييد رسائل البريد الإلكتروني الواردة إلى قائمة بيضاء من جهات الاتصال المعتمدة.
- إرسال نسخة من كل الرسائل الواردة إلى حساب أحد الوالدين.
- إرسال نسخة من كل الرسائل الصادرة إلى حساب أحد الوالدين.

توفر هذه الميزات طبقة إضافية من الأمان والتنقية التي تحد من خطر تلقي أطفالك محتوى غير لائق، كما تقدم رؤى إضافية في حياتهم الشخصية لضمان استمرارية سلامتهم.

6-2-6-2 التعرف على المعايير التي يجب مراعاتها عند اختيار برنامج لتصفية المحتوى خاص بالآباء، كيف يطبق البرنامج على الأنواع المختلفة من الأجهزة، مثل الهواتف الذكية أو أنظمة الألعاب؟

بغض النظر عن فوائد برامج تصفية المحتوى الخاصة بالآباء، هناك عدة معايير يجب مراعاتها قبل الاستثمار في تطبيق البرنامج.

- الخفاء - يمكن أن تكون المراقبة فعالة فقط إذا كان طفلك لا يعلم ولا يشعر بوجود البرنامج، فلا يُسمح للطفل بتعطيل أو إزالة البرنامج.
- تصفية البيانات - من السهل جدا أن تشعر بالارتباك فيما يتعلق بالبيانات التي يتم جمعها من استخدام طفلك للإنترنت، لذا يتعين عليك إيجاد برنامج تصفية جيد يوفر معلومات مفيدة تظهر عند استخدام بعض الكلمات أو فتح مواقع معينة.
- الوصول إلى البيانات - بمجرد جمع هذه البيانات يمكن الوصول إليها إما عن بعد أو محليا من خلال الكمبيوتر، فإذا كان طفلك يستخدم الجهاز منفردًا، يفضل تلقي البيانات عن بعد عن طريق بريد إلكتروني أو رابط لأن المراقبة المستمرة للجهاز تدفع الطفل للبحث عن غيره من الأجهزة لأنشطته غير اللائقة.
- القدرة على الرصد - تطبيق البرنامج ينبغي أن يوفر المراقبة لتطبيقات متعددة بما في ذلك برامج تصفح الإنترنت والدردشة والمراسلة والفيديوهات المشاهدة والموسيقى المسموعة وغيرها من بوابات الشبكات الاجتماعية، كما ينبغي أن يوفر المراقبة لأجهزة متعددة، إن أمكن، بما في ذلك الكمبيوتر والأجهزة الذكية مثل الأجهزة اللوحية أو الهاتف المحمول.

7-2-6-2 الاطلاع على الطريقة التي يمكن للشباب من خلالها إخفاء الأنشطة التي يمارسونها عبر الإنترنت عن الآباء.

يحاول بعض الشباب إخفاء ما يمارسونه من أنشطة على الإنترنت عن الوالدين بإزالة محفوظات متصفح الإنترنت أو حجب المتصفح حينما يشعرون بمجيء أحد الوالدين أو اقترابه من الكمبيوتر الذي يستخدمه، وقد يتجهون إلى إنشاء حسابات خاصة أو صفحات تواصل اجتماعي ليس للآباء دراية تامة بها، إضافة إلى ذلك، يمكن استخدام الهواتف المحمولة في الوصول إلى المواقع الإلكترونية غير المسموح بها أو الاحتفاظ بالرسائل الموجودة على صفحات التواصل الاجتماعي.

يمكن استخدام الهواتف الذكية للاستمرار في إرسال الرسائل الفورية أو لتنزيل مقاطع الفيديو، وفي أسوأ الأحوال يمكن للشباب تنزيل محتوى غير قانوني أو مسروق، الأمر الذي يعد في حد ذاته سلوكًا إجراميًا، وينبغي للآباء الانخراط مع أبنائهم في حديث إيجابي مفتوح وتشجيعهم على التمييز بين الوسائل الآمنة والمقبولة وغيرها من الوسائل غير المقبولة للحد من التعرض للمخاطر.

2-6-2-8 التعرف على الطرق التي تمنع الشباب من حجب أنشطتهم عبر الإنترنت.

يتعين على الآباء مشاركة أبنائهم الصغار في تعلم الإنترنت وطريقة استخدامه، وبالإشارة إلى ما يقوم به الآباء من تقدير للميزات التي يقدمها عالم الإنترنت ووسائل الإعلام الاجتماعية والتكنولوجيا، يظهر الآباء إدراكهم واستيعابهم للأشياء، ومن ناحية أخرى، يتعين على الآباء تحديد مجموعة كبيرة من المخاطر ووضع ضوابط واضحة حول ما هو آمن ومقبول وما هو غير ذلك، كما يتعين على الآباء تشجيع أبنائهم على التحدث إليهم وفتح حوار معهم حول السلوكيات التي تحدث على الإنترنت، بالإضافة إلى تطبيق برامج المراقبة الأبوية أو غيرها من سبل الحماية لتصفية المحتوى أو مراقبة هذه السلوكيات.

ينبغي للآباء التحدث مباشرة مع أبنائهم عن المشكلات التي يتعرضون لها على الإنترنت وتتسبب في مضايقتهم وإزعاجهم، وإذا ما حدث ذلك عليهم التوجه بالحديث معهم أو مع معلمهم، يمكن استخدام برامج المراقبة الأبوية للحد من المخاطر المحتملة التي يتعرض لها الأطفال والشباب نتيجة للتفاعل مع شبكات وسائل الإعلام الاجتماعية وغيرها من المحتويات التفاعلية، ومن ضمن هذه المخاطر:

- التعرض للمضايقات التي يتعرضون لها من أشخاص يقيمون معهم صداقات عبر الإنترنت.
- نشر معلومات شخصية تساعد على تحديد مكانهم عندما يكونون غير متصلين بالإنترنت.
- الصداقات غير اللائقة والاستغلال وسوء المعاملة والتواصل مع الغرباء.
- التعرض لمشاهدة محتويات غير لائقة.
- التورط في نشر محتويات غير قانونية وإباحية للكبار.
- التعرض لرسائل تفرقة عنصرية.
- مدح ممارسة أنشطة بذيئة مثل تعاطي المخدرات أو الكحوليات.
- مغادرة المنزل نتيجة للاتصالات التي تتم عبر الإنترنت.

يتعين على الآباء إرساء القواعد والضوابط الواضحة والتواصل مع أبنائهم بشكل مستمر، فمن الأفضل أن يكون طفلك صديق لك وليس عدو.

2-6-2-9 إدراك أن برامج التصفية ليست بديلا عن إشراف الوالدين الصحيح والنقاش المفتوح مع الأطفال والمراهقين.

على الرغم من أن برامج التصفية يمكن أن توفر الكثير من المراقبة والأمن فإنها لا يمكن أبدا أن تكون بديلا عن إشراف الوالدين، فالأطفال فضوليون وهذا الفضول يمكن أن يعرضهم دون قصد منهم لمخاطر الإنترنت التي يتم معالجتها بشكل فعال من قبل برنامج التصفية، ولكن في نهاية المطاف نحن بشر يعيش على هذا الكوكب ومعظم القضايا التي يتم اكتشافها على الإنترنت تتعلق بحياتنا الشخصية والحقيقية، يجب على الآباء الحفاظ على حوار مفتوح مع أطفالهم لكشف المشاكل الحقيقية ومعالجتها قبل إطلاقها على شبكة الإنترنت.

10-2-6-2 التعرف على كيفية إنشاء اتفاقية مستخدم إنترنت للآباء والأطفال.

الأمان على الشبكة:
عقد الشباب

1- سأحرص دائما على إبلاغ والدي أو شخص كبير إن صادفني شيء محير أو مخيف أو شيء هددني.

2- لن أفصح أبدا عن اسمي بالكامل وعنواني الحقيقي ورقم هاتفي واسم مدرستي أو مكاني أو جدولي أو كلمة المرور الخاصة بي أو معلومات تعريفية تخصني عندما أكون على الانترنت، وسأرجع إلى شخص كبيرة إن لاحظت أية استثناءات.

3- لن أقابل أبدًا شخصًا تعرفت إليه عن طريق الإنترنت، وفي حالات نادرة قد يوافق الوالدين على ذلك، ولكن في حالة قررت أن أقابل صديق الإنترنت، فسوف أقابله في مكان عام وأن أحد الوالدين أو الوصي يرافقني.

4- لن أرد أبدًا على أية رسائل على الإنترنت، والتي تتضمن كلمات بذيئة أو مخيفة أو تهديدية أو غريبة، وإذا استلمت هذا النوع من الرسائل، سوف أطبعها وأخبر أحد البالغين على الفور، حيث يمكن له الاتصال بخدمة الإنترنت أو وكالة مناسبة معنية بذلك، وحال شعرت بعدم الراحة في إحدى غرف الدردشة، سوف أستخدم زر ignore (تجاهل).

5- لن أدخل على منطقة جديدة عبر الإنترنت، والتي سوف تكلف مالاً إضافيًا دون الحصول على إذن مسبق من أحد الوالدين أو المعلم.

6- لن أرسل أبدًا صورة عبر الإنترنت أو عبر البريد الإلكتروني العادي إلى أي شخص دون الحصول على إذن من أحد الوالدين.

7- لن أعطي رقم بطاقة ائتمان عبر الإنترنت من دون حضور أحد الوالدين.

الشاب_____التاريخ:_____

ولي الأمر/الوصي_____التاريخ:_____

6-2 التعلم سويًا

3-6-2 إدمان الإنترنت

1-3-6-2 إدراك كيف أن استخدام الإنترنت يمكن أن يتداخل مع الحياة اليومية والعمل والعلاقات

على الرغم من الوقت الذي تقضيه على الانترنت يمكن أن يكون مثمرًا، إلا أن استخدام الإنترنت القهري يمكن أن يكون مدمرًا لحياتك اليومية وعملك وعلاقاتك، فالاستخدام الطاهر في البداية للإنترنت من أجل العمل أو الحياة الشخصية يمكن أن يتحول بسرعة إلى الإدمان والضرر النفسي المحتملين.

2-3-6-2التعرف على مفهوم اضطرابات إدمان الإنترنت (IAD) والأنواع المختلفة لمشاكل الإدمان: المحتوى غير اللائق، وغرف الدردشة، وألعاب الإنترنت، وتصفح الإنترنت القهري

يعرف مصطلح اضطرابات إدمان الإنترنت أيضًا بالاستخدام المشكل للإنترنت (PIU) أو اضطرابات الإنترنت القهرية (CIU)، وفي الأساس فإن أي سلوك قهري ذو صلة بالانترنت ويتعارض مع الحياة الطبيعية يمكن أن يصنف على أنه اضطراب بسبب إدمان الإنترنت.
ومن المشاكل الشائعة لاضطرابات الاستخدام المفرط (إدمان) الإنترنت:

- إدمان الكمبيوتر - الاستخدام المفرط والوقت المستغرق على جهاز كمبيوتر
- الحمل الزائد للمعلومات - تصفح الإنترنت للحصول على المعلومات مما يؤدي إلى انخفاض إنتاجية العمل.
- دوافع الإنترنت - الألعاب، والتسوق، والمواقع الإلكترونية، والقمار وغيرها من الخدمات المعروضة على الانترنت
- علاقات الإنترنت - الشبكات الاجتماعية، وغرف الدردشة، والمراسلة والوصول إلى نقطة تكون فيها العلاقات الافتراضية أكثر أهمية من العالم الحقيقي.
- مضايقات المحتوى غير اللائق - الاستخدام القهري للمواقع ذات المحتوى الخاص بالكبار والتي تؤثر سلبا على العلاقات الاجتماعية والزوجية.

من الممكن تصنيف اضطرابات إدمان الإنترنت في المستقبل على أنها اضطرابات نفسية نظرا لانتشارها الكبير في مجتمعنا اليوم.

3-3-6-2 التعرف على بعض أعراض اضطرابات إدمان الإنترنت: فقدان مسار الوقت على الإنترنت، الانعزال عن الأسرة والأصدقاء، الدفاع عن استخدام الإنترنت، صعوبة استكمال المهام الأخرى، اضطرابات أثناء النوم

تختلف العلامات والأعراض ولكن يجب الانتباه إلى العلامات التحذيرية التالية:

- فقدان مسار الوقت على الانترنت - تجد نفسك تقضي وقتًا على الانترنت أطول مما كنت تقصد، فالدقائق تتحول إلى ساعات، أو أن تصبح غريب الأطوار إذا انقطع الوقت على الانترنت.
- الانعزال عن الأسرة والأصدقاء - قد تعاني حياتك الاجتماعية من إهمال الأسرة والأصدقاء، ولا أحد يفهم ذلك سوى أصدقائك عبر الإنترنت ‘
- الدفاع عن استخدام الإنترنت - وصف من يشكون من استخدامك للكمبيوتر بالمرضى، وإخفاء استخدامك للإنترنت من المقربين إليك.
- صعوبة استكمال المهام الأخرى - يمكن أن تتراكم الأعمال المنزلية، كما يمكن أن تتسلل مهام العمل من بين يديك، بل ربما تعمل لوقت متأخر للحاق بالركب أو تظل مستيقظًا لوقت متأخر لاستخدام الانترنت بحرية.
- اضطرابات أثناء النوم - وجود أفكار ليلية توحي لك بالبحث على الانترنت على الفور، فتجد نفسك مستيقظًا لوقت متأخر أكثر من المعتاد على أساس منتظم.

4-3-6-2 فهم ما الذي يمكنك فعله إذا شعرت بأن الطفل يعاني من إدمان الإنترنت: تشجيع الاهتمامات والأنشطة الاجتماعية الأخرى، مراقبة استخدام الحاسوب ووضع حدود واضحة، استخدام تطبيقات للحد من استخدام الطفل للهاتف الذكي، مناقشة القضايا الأساسية مع الطفل، الحصول على مساعدة مهنية.

هناك ثلاث خطوات يجب أن يتخذها كل الآباء لمعالجة اضطرابات إدمان الإنترنت بشكل صحيح مع أطفالهم، تتمثل الخطوة الأولى في إتمام اختبار إدمان الانترنت على النحو المنصوص عليه في القسم التالي أو من أي مصدر آخر موثوق به عبر الإنترنت، فإذا أشارت النتائج إلى وجود اضطرابات بسبب إدمان الإنترنت، يرجى الانتقال إلى الخطوة التالية المتمثلة في السعي للحصول على مساعدة شخصية كما هو موضح في هذا القسم، وأخيرا، إذا حققت توجيهات الوالدين نتائج قليلة جدا أو لم تثمر عن تحسن في سلوك الطفل، يتعين عليهم طلب المساعدة المتخصصة لمعالجة المشاكل النفسية المحتملة.

ينبغي أن يعمل التوجيه الشخصي من الآباء، إلى جانب المساعدة المقدمة من المعلمين، على تحقيق العديد من الأمور لك.

1- وضع حدود لاستخدام الإنترنت مثل أي نشاط آخر لك، وينبغي أن تتضمن تلك الحدود الوقت ونوع المحتوى المسموح به، تذكر أنه ينبغي القيام بأي أمر باعتدال.
2- مراقبة استخدام الأطفال للإنترنت مع الاستفادة من التوصيات الواردة في الفصل 2-6، بما في ذلك استخدام البرمجيات والتطبيقات.
3- المناقشة المفتوحة لاكتساب المزيد من التبصر في مصدر الإدمان الذي قد يكون أكثر خطورة من سلوك الإدمان والذي قد يشمل التسلط والاكتئاب.

5-3-6-2 إدراك وجود اختبارات للإدمان متاحة عبر الإنترنت لتحديد مستوى الإدمان.

اختبار الإدمان المقدم هنا هو اختبار للآباء والأطفال من موقع www.healthyplace.com، ولكن هناك العديد من الاختبارات المتاحة على الانترنت للبالغين والأطفال، وأدناه رابط لمصدر موثوق على الإنترنت:
http://www.globaladdiction.org/dldocs/GLOBALADDICTION-ScalesInternetAddictionTest.pdf

اختبار إدمان الإنترنت

يجب الإجابة على جميع الأسئلة باستخدام مفاتيح الإجابة المذكورة أدناه، فالرقم الموجود يسار كل إجابة هو القيمة المعطاة، على سبيل المثال، إذا أجبت بـ "كثيرا" على السؤال 1، يجب إدخال الرقم 3 كإجابة على هذا السؤال، وبمجرد الانتهاء من جميع الأسئلة وإدخال الأرقام، احسب المجموع الإجمالي لجميع الأسئلة،وبناء على المجموع يوجد جدول أسفل الاستبيان يوضح درجة الاختبار.

مفاتيح الإجابة:

1- لا يوجد أو نادرًا
2- أحيانًا
3- كثيرًا
4- غالبًا
5- دائمًا

1- كم مرة تقوم بكسر المهل الزمنية التي حددتها لاستخدام الإنترنت؟
2- كم مرة تُهمل أداء الأعمال المنزلية لقضاء المزيد من الوقت على الإنترنت؟
3- كم مرة تُفضل قضاء الوقت على الإنترنت وليس مع بقية العائلة؟
4- كم مرة تكوّن علاقات جديدة مع مستخدمين على الإنترنت؟
5- كم مرة تشعر بالضيق من مقدار الوقت الذي تقضيه على الإنترنت؟
6- كم مرة تقل درجاتك بسبب مقدار الوقت الذي تقضيه على الإنترنت؟
7- كم مرة تتحقق من البريد الإلكتروني قبل القيام بشيء آخر؟
8- كم مرة تبتعد عن الآخرين منذ اكتشاف شبكة الإنترنت؟
9- كم مرة تُصبح دفاعيًا أو متكتمًا عندما تُسأل عما تفعل على الإنترنت؟
10-كم مرة لاحظت تسللك إلى الإنترنت رغمًا عنك؟
11-كم مرة تقضي بعض الوقت وحدك في غرفتك لتلعب على الكمبيوتر؟
12-كم مرة تتلقى مكالمات هاتفية غريبة من أصدقاء جدد "على الإنترنت"؟
13-كم مرة تصرخ أو تصيح أو تضيق ذرعًا إذا أُزعجت أثناء الوجود على الإنترنت؟
14-كم مرة تبدو متعبًا ومرهقًا بشكل أكبر مما كان عليه الأمر قبل معرفتك بالإنترنت؟
15-كم مرة تبدو مشغولاً بعودتك مرة أخرى إلى الإنترنت عند تركك إياها؟
16-كم مرة تشعر بالغضب بسبب التدخل في طول المدة التي تقضيها على الإنترنت؟
17-كم مرة تختار قضاء بعض الوقت على الإنترنت بدلاً من القيام بهواياتك القديمة أو اهتماماتك الخارجية؟

18-كم مرة تُصبح غاضبًا أو عدوانيًا عند وضع حدود زمنية للوقت الذي تقضيه على الإنترنت؟
19-كم مرة تختار قضاء المزيد من الوقت على الإنترنت بدلاً من الخروج مع الأصدقاء؟
20-كم مرة تشعر بالاكتئاب أو تقلب المزاج أو العصبية عندما لا تكون على الإنترنت وتود أن تعود إليه مرة أخرى؟

الدرجة:

20-49: (أنت مستخدم متوسط للإنترنت، وقد تتصفح الإنترنت لوقت طويل إلى حد ما في بعض الأحيان، ولكنك تسيطر على استخدامه)
50-79: (أنت تعاني من مشاكل عارضة أو متكررة بسبب الإنترنت، يجب عليك النظر في التأثير الكامل للإنترنت على حياتك وأثر ذلك على بقية أفراد أسرتك).
80-100: (استخدام الإنترنت يسبب لك مشاكل كبيرة في حياتك وعائلتك على الأرجح، لذلك لابد من معالجة هذه المشاكل الآن).

اختبار

س1- أي الروابط(URL) التي يحظر من خلالها استخدام بعض المواقع الإلكترونية المحددة؟

أ-www.computercontrolbar.com
ب- www.controlbar.com
ج- www.datachecker.com
د- www.parentalcontrolbar.org

س2- ما أفضل مكان يوضع فيه جهاز الكمبيوتر في المنزل؟

أ-مكان مركزي مفتوح
ب-مكان منعزل
ج-مكان مزدحم جدًا
د-مكان خاص

س3-أي من مميزات نظام MicrosoftWindows من شأنها مساعدة الآباء في تأمين استخدام الأطفال للكمبيوتر؟

أ-ضوابط الوصول
ب- ضوابط التحكم في الأبناء
ج- الرقابة الأبوية
د- أدوات التحكم في الكمبيوتر

س4- حدد ما إذا كانت الجملة التالية صواباً أم خطأ، "لا ينبغي للوالدين على الإطلاق قراءة رسائل البريد الإلكتروني الخاص بأولادهم".

أ- صواب
ب- خطأ

الإجابات في الصفحة التالية

الإجابات

س1- د- www.parentalcontrolbar.org
س2- أ- مكان مركزي مفتوح
س3- ج- الرقابة الأبوية
س4- ب- خطأ

الفصل 2-7

السلوكيات الافتراضية

2-7-1 التواصل

2-7-2 التسلط عبر الإنترنت

7-2 السلوكيات الافتراضية

1-7-2 التسلط عبر الإنترنت

1-1-7-2 استيعاب معنى مصطلح "آداب التعامل على الإنترنت"

إن مصطلح "آداب التعامل على الإنترنت" مؤلف من شقين "آداب التعامل" و"الإنترنت" (أي مرتبط بالإنترنت) وهو يصف القواعد العامة للسلوك الواجب مراعاتها عند استخدام الإنترنت،فبينما تمتلك مواقع التواصل الاجتماعي قواعد استخدام رسمية خاصة بها، انتشرت ممارسات غير رسمية لاستخدام للإنترنت على مر السنين ومن بينها:

- وضوح الكتابة وخلوها من الأخطاء الإملائية واستخدام الكلمات المناسبة؛ حيث إن مستخدمي المواقع ليسوا جميعًا من متحدثي اللغة الأم التي تتحدثها.
- تجنب كتابة العبارات بحروف كبيرة.
- التحلي بكريم الأخلاق والأدب على الإنترنت.
- تجنب إرسال الرسائل أو المحتويات البذيئة.
- تذكر أن منشوراتك علنية - حيث يمكن قراءتها من قبل أي شخص بما في ذلك شريك حياتك أو أطفالك أو والديك أو إخوتك أو صاحب العمل أو المعلم الخاص بك.
- تجنب إرسال رسائل غير مرغوبة، وتجنب تكرار الإعلانات التي تنشرها لمنتجات أو خدمات معينة.
- تجنب نشر المواد المحمية بحقوق طبع ونشر ما دمت لا تمتلك هذه الحقوق.

إن السلوكيات التي تنتهجها على الإنترنت تعبر عنك وتمثلك فإن التزمت الأدب والإيجابية، فستلقى الاحترام من الغير.

2-1-7-2 إدراك مفهوم "لا تراجع" فور نشر معلومات

تظل المعلومات على الإنترنت ما إن يتم نشرها، ولن تحذف نهائيًا من الإنترنت حتى وإن تم حذفها أو تعديلها، لذا تجنب نشر أية صور أو منشورات قد تسبب لك أو لأي شخص إزعاجًا فيما بعد،وقد يصل صديق لك لصفحتك على شبكة التواصل وينسخ أية معلومات خاصة أو صور محرجة وينشرها على صفحات أخرى.

فكر قبل أن تنشر أي محتوى، وإذا ما ساورتك أية شكوك حول ما يمكنك نشره، فلا تنشر أية مواد ومن الأفضل الاحتفاظ بها لنفسك، فعلى سبيل المثال، عند نشر محتويات على صفحة فيس بوك (انظر الشكل 40 أدناه)، فكر جيدًا في "بمَ تفكّر؟".

الشكل 40:فيس بوك - شاشة نشر " بم تفكر؟"

3-1-7-2الهدف من اختيار اسم مستخدم "ذكي" على الإنترنت لا يفصح إلا عن جزء قليل جدًا من المعلومات الشخصية

إن الاسم الجيد للمستخدم يسهل تذكره ولكن لا يوحي بأية معلومات حساسة عنك مثل الاسم بالكامل أو العنوان أو رقم الهاتف، إذ أن اسم المستخدم الذي يشتمل على جزء كبير من اسمك الحقيقي يسهل عملية البحث عن شخصك ومعرفة معلومات شخصية عنك، ويمكنك كذلك تمييز اسمك بأي شيء لتتذكره ولا يمكن للآخرين التعرف عليه.

هذا ويمكن استخدام اسم المستخدم في أغراضٍ عدة بدايةً من الأغراض المباشرة مثل التسويق وحتى تلك الأغراض التي قد تضر بك مثل سرقة الهوية،فقد يستخدم المتحرشون على الإنترنت معلوماتك الشخصية لتعريض المستخدمين لمحتويات غير ملائمة.

ولن تكون عرضة للإفصاح عن معلوماتك الشخصية إذا ما استخدمت أسماء "ذكية" على الإنترنت.

4-1-7-2 التعرف على سبب أهمية حماية المعلومات الشخصية والحفاظ على الخصوصية

قد تتسبب مشاركة كم كبير من المعلومات الشخصية في سرقة الهوية مما يسهل على المجرمين الحصول على أموال وبضائع وخدمات باسمك، فإذا تمكن أحد المعتدين عبر الإنترنت من تجميع ما يكفي من معلومات عنك، فإنه قد يتعرف على عنوان منزلك أو مدرستك مما قد يعرضك لأن تقع ضحية للتسلط عبر الإنترنت والملاحقة والإيذاء البدني وربما قد يصل الأمر إلى الخطف.

فاحرص دومًا على حماية معلوماتك الشخصية (ومعلومات عائلتك عند الاقتضاء).

5-1-7-2 اتخاذ الحيطة من إضافة أشخاص لا تعرفهم إلى قائمة الأصدقاء/الزملاء لتجنب المخاطر

أصدقاء الإنترنت ليسوا بأصدقاء حقيقيين، فكلمة "صديق" تستخدم على الإنترنت لمجرد الإشارة إلى جهة اتصال، فالصديق الحقيقي على أرض الواقع هو من تقابله في حياتك اليومية ويمكن وضع ثقتك الكاملة فيه، وتذكر دومًا أن كل صديق من الأصدقاء الجدد بإمكانه الوصول إلى ملفك الشخصي وإضافة "أصدقاء الأصدقاء" مما يتيح الفرصة أمام أشخاص لا تعرفهم من الاطلاع على معلوماتك الشخصية.

7-2 السلوكيات الافتراضية

2-7-2 التسلط عبر الإنترنت

2-7-2-1 التعرف على مصطلح "التسلط عبر الإنترنت"

إن مصطلح "التسلط عبر الإنترنت" يعني استخدام التقنيات المتعلقة بالإنترنت، مثل الوسائط الاجتماعية، لإلحاق الضرر بالأفراد على نحو متعمد ومتكرر وعدواني،ومن أمثلة التسلط عبر الإنترنت الاتصالات التي تسعى لترهيب المتلقي أو السيطرة عليه أو التلاعب به أو تحقيره أو تشويه سمعته كذبا أو إذلاله،وقد يشمل ذلك:

- رسائل البريد الإلكتروني غير المرغوب بها المرسلة إلى شخص ما.
- الرسائل النصية غير الملائمة أو الرسائل القصيرة (SMS).
- الإساءة إلى فرد في أحد المنتديات.
- الإفصاح عن البيانات الشخصية الخاصة بأحد الأفراد.
- انتحال شخصية شخص آخر.

كما أن برامج التواصل الاجتماعي تعمل على رفع مستوى الوعي لدى الأفراد وتعريفهم بخطورة التسلط عبر الإنترنت لحماية المستخدمين، فعلى سبيل المثال قام مستخدمو (جوجل+) بإنشاء مجتمع "وقف التسلط عبر الإنترنت" (انظر الشكل 41 أدناه) لتمكين المستخدمين من مشاركة أفكارهم حول كيفية إيقاف هذه الظاهرة.

الشكل 41: الفريق المجتمعي لـ (جوجل+) - وقف التسلط عبر الإنترنت
https://plus.google.com/114933068076498476678/posts

2-7-2-2 التعرف على الوسائل التي يتم من خلالها التسلط عبر الإنترنت

يستخدم المتسلطون عبر الإنترنت الوسائل التقنية على الإنترنت للتربص بالضحايا ويشمل ذلك مواقع التواصل الاجتماعي والرسائل النصية والبريد الإلكتروني والرسائل الفورية وغرف الدردشة واستطلاعات الرأي عبر الإنترنت والمواقع ورسائل الصور ولوحات تبادل الرسائل المستخدمة على أجهزة الكمبيوتر أو أجهزة الحاسب المحمول أو اللوحية أو الهواتف الذكية أو أي أجهزة أخرى يتم توصيلها بالإنترنت.

3-2-7-2 التعرف على مدى سرعة انتشار المعلومات/الصور وما هي التأثيرات المترتبة على التسلط عبر الإنترنت

يمكن إرسال رسالة نصية أو صورة من هاتف ذكي لكل جهات الاتصال مرة واحدة، فإذا ما تم إرسال رسالة إلى 16 شخصًا، ثم قام كل واحد من هؤلاء بإرسالها إلى 16 شخصًا آخر، فقام كل منهم بإرسالها إلى 16 شخصًا آخرين (x16x1616)، فسيرى الرسالة ما يزيد عن 4000 شخص.

وقد يتسبب التسلط عبر الإنترنت في إصابة الضحايا بمشاعر قلق وإحباط وهناك عدد من الحالات الموثقة نتج عنها انتحار الضحايا.

تُعد حالة ريان هاليغان والبالغ من العمر 13 عامًا فقط هي أحد الأمثلة على ذلك والذي دفع حياته ثمنًا لتعرضه للمضايقات على الإنترنت، فهو مثال من بين العديد من الأمثلة التي لم يستطع فيها الفرد تحمل المشاعر التي انتابته على أثر وقوعه ضحية للمضايقات، (http://www.ryanpatrickhalligan.org/index.htm).

4-2-7-2 التعرف على عواقب التسلط عبر الإنترنت ودوافعه التي منها: إخفاء الهوية، حيث يشعر المتسلط بأنه قادر على "الهروب بفعلته"، والتعرف على أن التسلط عبر الإنترنت يمكن أن يكون عملية ذات اتجاهين

إن التسلط عبر الإنترنت له عواقب على مرتكب الجريمة، وبالطبع الضحية، ومن العواقب ما قد يكون قانونيًا وعاطفيًا وربما جسديًا إذا كان الطرفان يعرفان بعضهما شخصيا، ويجب أن تتذكر أيضا أن التسلط عبر الإنترنت إنما هو عملية ذات اتجاهين مما يعني أن الضحية الأولى قد ينتهي بها إلى التسلط على نحو أسوأ من المحرض الأول.

وقد يكون من السهل على المتسلطين أن يقوموا بالتسلط عبر الإنترنت بسبب عامل "إخفاء الهوية" مما يتيح لهم إنشاء هويات مزيفة والشعور بالقدرة على الهروب بأفعالهم دون عواقب. ‘

هذا وتختلف دوافع التسلط عبر الإنترنت، كما تختلف الاستجابات لكل سبب من الأسباب التي تدفع الطفل للتسلط، ومن دوافع التسلط ما يلي:

- الغضب
- الإحباط
- الثأر
- الملل
- التسلية
- الطاقة

5-2-7-2 التعرف على العلامات التحذيرية للتسلط عبر الإنترنت

إن تجنبك لأفعال التسلط عبر الإنترنت ليس بالأمر الهين، ومن ثم فإنه من الضروري أن تراقب سلوكك واستخدامك العادي للتكنولوجيا.

قد تتعرض إلى التسلط عبر الإنترنت إذا كنت:

- تواجه تقلبات مزاجية أو تشعر بالقلق بعد استخدام الإنترنت أو الهاتف المحمول.
- تشكو بشكل متزايد من أعراض مرضية.
- لا يوجد لديك الرغبة في الذهاب إلى المدرسة أو الخروج بشكل عام.
- تنسحب بشكل غير طبيعي من الأنشطة الاجتماعية.
- لديك انخفاض تدريجي في الدرجات أو الأداء الأكاديمي.
- تشعر بالغضب والاستياء بعد استخدام الكمبيوتر أو الدخول على الإنترنت باستخدام هاتف محمول أو جهاز نقال.

6-2-7-2تعلم كيف يمكن مواجهة التسلط عبر الإنترنت وتسجيله وإبلاغ السلطات المختصة عما به من مخاوف

ما الاحتياطات الإضافية التي يمكن اتخاذها لحماية نفسك وأصدقائك من التسلط عبر الإنترنت؟

- عدم فتح رسائل البريد الإلكتروني والرسائل النصية إلا تلك التي تصلك من أشخاص تعرفهم جيدًا.
- تجنب إعادة إرسال رسائل البريد الإلكتروني المتسلسلة أو الخدع.
- تجنب نشر أية مواد تمثل لك أي نوع من الخصوصية.
- تجنب الرد على رسائل البريد الإلكتروني أو النصوص التي تسبب لك مضايقات، فلن يعمل ذلك إلا على تشجيع التسلط عبر الإنترنت.
- حظر المتسلطين - تتضمن العديد من التطبيقات إعدادات حظر وصول رسائل البريد الإلكتروني أو الرسائل الفورية أو النصية المرسلة من أشخاص معينة.
- الاحتفاظ بالرسائل - ليس ثمة داعي لقراءة هذه الرسائل فهناك دلائل عليها.
- إبلاغ مشغلي المواقع الإلكترونية أو الهواتف المحمولة بأية انتهاكات تحدث أو إبلاغ الشرطة بالقضايا الخطيرة أو إعلام شخصٍ له سلطة عن نوع الاتصالات التي تتلقاها ودعه يقرر الخطوة التالية التي يجب اتخاذها.
- الحد من المعلومات التي يتم نشرها على الإنترنت.
- ضبط إعدادات الخصوصية بحرص شديد.

عندما تستهدف المضايقات الإلكترونية أو الهاتف المحمول الأفراد لا سيما الشباب والأطفال، قد تشعر بالوحدة خاصةً وإن كان من حولك من البالغين ليس لديهم أدنى فكرة عن المضايقات الإلكترونية وأثرها، ومن خلال تشجيع زملائك على الإبلاغ عن عمليات التسلط عبر الإنترنت لأحد الأشخاص البالغين أو إحدى السلطات المحلية أو سلطة على الإنترنت فضلاً عن تشجيعهم على عدم الرد مطلقًا على هذه العمليات مباشرةً، فأنت تسيطر على الوضع تمامًا.

7-2-7-2 فهم كيفية التعامل مع الأطفال المتسلطين على الآخرين عبر الإنترنت.

إذا كان طفلك متسلطًا فهذا لا يعني بالضرورة أنك والد سيء، بل يجب عليك فقط أن تأخذ في الاعتبار أن عقاب الطفل عقابًا تقليديًا كأن تحبسه في حجرته لن يُجدي.

هناك العديد من الأمور التي يمكن للوالد القيام بها في البداية لمحاولة إيقاف هذا السلوك.

- تأكد من فهم الطفل أن سلوك التسلط عبر الإنترنت سلوك غير مقبول، مع توجيه هذا السؤال له: كيف ستشعر لو فعل شخص ما بك نفس الشيء؟
- حاول فهم سبب حدوث التسلط، فقد يكون طفلك قد قام بالتسلط كرد فعل دفاعي نتيجة تعرضه لعملية تسلط مسبقة.
- اشرح خطورة ما يقوم به الطفل من أفعال مع الإشارة إلى أن سلطات إنفاذ القانون أو سلطات المدرسة قد تتدخل.
- أن تأمر الطفل بوقف هذا السلوك فورًا.
- أن تراقب أنشطة الطفل على الإنترنت بما في ذلك الأجهزة المحمولة الخاصة به مثل الهاتف الذكي.

أشياء يجب عليك القيام بها للرجوع إليها في المستقبل ومنها:

- إثراء معرفتك بالتكنولوجيا، فإن لم تكن على دراية بالأدوات التي يستخدمها طفلك لن تتمكن من حمايته من التهديدات المحتملة التي يتعرض لها بشكل يومي.
- التعرف على المسائل القانونية ذات الصلة عن طريق البحث على الإنترنت من خلال المواقع الحكومية ومواقع الأطراف الأخرى.
- الإفصاح عن مخاوفك إلى مدرس ومستشار ومدير المدرسة التابع لها طفلك عند الضرورة.
- الحرص على معرفة أن المشكلة يمكن أن تكون أكثر خطورة وقد تنطوي على مشاكل عاطفية أو تنموية تحتاج إلى معالجة من قبل الطبيب.

8-2-7-2 إدراك أن البالغين قد يتعرضون أيضًا للتسلط عبر الإنترنت.

إن قيام البالغين بالتسلط عبر الإنترنت أكثر انتشارا مما هو معترف به، فقد حدث وأن شعرت إحدى الوالدات بضرورة وضع بعض أسرارها (الحسنة والسيئة) على الإنترنت، ولكن سرعان ما ظهرت هذه الأسرار على الإنترنت وتعرف عليها أطفالها! كما تقوم أُخريات بالدخول على موقع فيس بوك لانتقاد صور الأطفال التي يشعرن بأنها غير لائقة، فهذه هي كل أشكال التسلط عبر الإنترنت ويمكن أن تؤثر تأثيرًا ضارًا على الضحايا، كما لا يختلف التسلط عبر الإنترنت بالنسبة لجميع الفئات العمرية ويمكن أن يتم من خلال مواقع التواصل الاجتماعي أو رسائل البريد الإلكتروني أو الرسائل أو أي منتديات أخرى على الإنترنت.

تُعد الملاحقة عبر الإنترنت معضلة أخرى تواجه الناس، فالملاحقة بشكل عام تعني تتبع شخص معين ومراقبته ومضايقته باستمرار بطريقة مخيفة أو خطرة، ويتم ذلك عبر الإنترنت من خلال الرسائل المتكررة والمراقبة المستمرة والتفاعل غير المرغوب فيه، وعادة ما تكون الملاحقة عبر الإنترنت مصحوبة بالملاحقة الفعلية، وفي كلتا الحالتين فإن الملاحقة جريمة جنائية يمكنك الاستعانة بالسلطات المحلية لحمايتك منها

والهندسة الاجتماعية، كما هو موضح في القسم 2-4-4-3، تختلف عن الملاحقة عبر الإنترنت في نقطة رئيسية وهامة: فالهندسة الاجتماعية هي أسلوب لجذب ثقة الأشخاص وخلق علاقة مبنية على هذه الثقة، أما الملاحقة عبر الإنترنت فهي فعل وقح وسرعان ما يصبح مصدر إزعاج ثم خطر محتمل.

اختبار

س1-أي من المصطلحات التالية يشير إلى أن الصورة لا يمكن حذفها فور نشرها على الإنترنت؟

أ- تعذر إعادة الاتصال
ب-لا تراجع
ج- عدم استعادة المنشور
د- عدم استعادة الحذف

س2- إذا كنت تستخدم اسمك الأول فقط على المنتديات،
ماذا يطلق على ذلك؟

أ- اسم مستخدم ذكي
ب- اسم مستخدم غير كامل
ج- اسم مستخدم مجهول
د- اسم مستخدم مختصر

س3-تلقيت بعض الرسائل النصية المسيئة على هاتفك،ماذا يطلق على ذلك؟

أ- التسلط عبر الإنترنت
ب- الإساءات
ج- الإزعاج
د-تزوير العناوين

س4- ما الذي يجب عليك القيام به إذا تعرضت للتسلط عبر الإنترنت؟

أ- تجاهل الأمر
ب-الإبلاغ عنه
ج-الرد عليه
د- عدم الانتباه إليه

الإجابات في الصفحة التالية

الإجابات

س1-ب-لا تراجع
س2-أ- اسم مستخدم ذكي
س3-أ- التسلط عبر الإنترنت
س4-ب-الإبلاغ عنه

الفصل 2-8

السياسة المتبعة

2-8-1 الاستخدام

2-8-2 حقوق الطبع والنشر

8-2 السياسة المتبعة

1-8-2 الاستخدام

1-1-8-2 معرفة سياسة الاستخدام المقبول (AUP) وأهميتها في المدارس

سياسة الاستخدام المقبول (AUP) هي مجموعة من القواعد يجب أن يوافق عليها المستخدم ليتصل بإحدى الشبكات أو الإنترنت، وهي شائعة الاستخدام في المدارس وتتطلب موافقة الطلاب قبل منحهم بطاقة الدخول على الشبكة، وقد صُممت سياسة الاستخدام المقبول لحماية المستخدمين وتحديد ما هو مقبول الاستخدام وعقوبات خرق هذه القواعد.

تواجه الكثير من المدارس مسؤولية كبيرة فيما يخص إدخال التقنية الحديثة والتعليم عبر الإنترنت، وتنص سياسة الاستخدام المقبول المدرسية على استخدام الإنترنت داخل نطاق المدرسة والتي تحتوي عادةً على أمور السلامة الشخصية والأنشطة غير القانونية وحماية النظام والخصوصية والسرقة الأدبية وانتهاك حقوق الطبع والنشر والدخول على المواد غير اللائقة، كما تنص على عدم جواز استخدام وسائل التقنية المملوكة للمدرسة إلا في الأغراض التعليمية، وينبغي توضيح حقوق الطلبة مثل حرية التعبير والحصول على المعلومات والعمليات اللازمة بالإضافة إلى عواقب انتهاك هذه السياسات.

وتحتوي مواقع شبكات التواصل الاجتماعي على سياسات الاستخدام المقبول، ويقوم تويتر بنشرها ضمن القواعد والسياسات الخاصة بها، انظر الشكل 42 أدناه:

قوانين وسياسات تويتر

الإرشادات

الإبلاغ عن انتهاك

قوانين توييتر

هدف ما ارائه سرويسی است که به شما اجازه می دهد محتوای منابع مورد علاقه تان را شناسایی کرده و دریافت کنید، همچنین بتوانید محتوایتان را با دیگران به اشتراک بگذارید. ما به مالکیت محتوای اشتراک گذاری شده توسط کاربران احترام می گذاریم، و هر کاربر مسئول محتوایی است که خودش ارائه می کند. به دلیل وجود چنین اصولی، ما مرتباً موارد را کنترل نمی کنیم و محتوای کاربر را سانسور نخواهیم کرد، مگر اینکه شرایط محدودی در زیر توصیف شده باشد.

محدودیت محتواها و استفاده از توییتر

به منظور ارائه سرویس توییتر و امکان برقراری ارتباط با دیگران و حفظ چنین ارتباطی، چند محدودیت در مورد نوع محتوایی که در توییتر قابل انتشار است در نظر گرفته شده است. این محدودیت ها با تبعیت از شرایط قانونی در نظر گرفته شده اند و سبب می شوند توییتر به تجربه ای بهتر برای همه ما تبدیل شود. ممکن است لازم باشد در مواقع مختلفی این قوانین را تغییر دهیم و از چنین حقی برخوردار هستیم. برای مشاهده جدیدترین قوانین، باز هم به اینجا سری بزنید.

- **جعل هویت**: شما نباید از طریق سرویس توییتر به صورت عدمی یا با هدف گمراه سازی، سردرگم کردن دیگران یا فریب دادن آنها، جعل هویت کنید.
- **مارک تجاری**: ما از این حق برخوردار هستیم تا از طرف شرکت یا فردی که حقوق قانونی با مارک تجاری مرتبط با نام های کاربری خاصی به آنها تعلق دارد، نسبت به لغو آن نام های کاربری اقدام کنیم. حساب هایی که از نام وایا آرم هایی برای گمراه کردن دیگران استفاده می کنند، به صورت دائمی غیرفعال می شوند.
- **اطلاعات خصوصی**: شما نمی توانید اطلاعات خصوصی و محرمانه سایر افراد را بدون اجازه صریح آنها منتشر کرده یا پست کنید، از جمله شماره های کارت اعتباری، آدرس خیابان یا شماره امنیت اجتماعی/شماره کارت ملی. شما نباید عکس ها یا ویدیوهای خصوصی که بدون رضایت سوژه موجود در آنها ضبط و توزیع شده است را پست کنید.
- **خشونت و تهدید**: نباید تهدید خشونت آمیز مستقیم و خاصی را نسبت به سایر افراد منتشر کرده یا پست کنید.
- **حق نسخه برداری**: ما به اعلامیه های کامل و شفاف نسبت به موارد نقض حق نسخه برداری پاسخ می دهیم. عملکرد ما نسبت به موارد حق نسخه برداری در شرایط سرویس عنوان شده است.
- **استفاده غیرقانونی**: نباید از سرویس های ما برای هرگونه هدف یا فعالیت غیرقانونی استفاده کنید. کاربران بین المللی موافقت می کنند که از همه قوانین محلی در ارتباط با فعالیت آنلاین و محتوای قابل قبول پیروی کنند.
- **سوء استفاده از نشان های توییتر**: شما نباید از نشان های توییتر، از جمله و نه محدود به نشان تبلیغ شده یا تأیید شده توییتر استفاده کنید، مگر اینکه از طرف توییتر در اختیار شما قرار گرفته باشد. حساب هایی که از این نشان ها به عنوان بخشی از عکس های نمایه، عکس های سرصفحه، پس زمینه استفاده می کنند یا به روشی از آن استفاده می کنند که به صورت غیرواقعی نشانگر ارتباط با توییتر است، ممکن است غیرفعال شوند.

سوء استفاده و هرزنامه

توییتر تلاش می کند از کاربرانش نسبت به موارد سوء استفاده و عملکرد هرزنامه محافظت کند. سوء استفاده از کاربر و موارد سوء استفاده فنی در Twitter.com به هیچ عنوان قابل قبول نیست و ممکن است باعث غیرفعال شدن دائمی حسابتان شود. هر حسابی که در فعالیت های توصیف شده در زیر شرکت داشته باشد ممکن است به صورت دائمی غیرفعال شود.

- **حساب های سری**: نمی توانید چند حساب مختلف برای انجام سوء استفاده ایجاد کرده یا همزمان از همگی آنها استفاده کنید. ایجاد تعداد زیادی حساب ممکن است سبب غیرفعال شدن همه حساب های مربوطه شود. لطفاً توجه داشته باشید که هرگونه نقض قوانین توییتر سبب غیرفعال شدن دائمی همه حساب ها خواهد شد.
- **سوء استفاده هدفمند**: نباید در فعالیت های سوء استفاده و اذیت و آزار هدفمند شرکت کنید. بعضی از عواملی که سبب می شوند فعالیتی به عنوان فعالیت با هدف سوء استفاده یا اذیت و آزار هدف مند شناخته شود عبارتند از:

الشكل 42: مثال لسياسة الاستخدام المقبول - قواعد موقع تويتر.
(https://support.twitter.com/articles/18311-the-twitter-rules)

2-1-8-2 معرفة محتويات سياسة الاستخدام المقبول السليمة: توعية الآباء والتلاميذ والحد من المخاطر ودعم آداب استخدام الإنترنت والسلوكيات الاجتماعية والأخلاقية الملائمة وحماية الأطفال قليلي الخبرة وحماية الهوية الشخصية وكلمة المرور.

يجب أن تتضمن سياسة الاستخدام المقبول السليمة ما يلي:

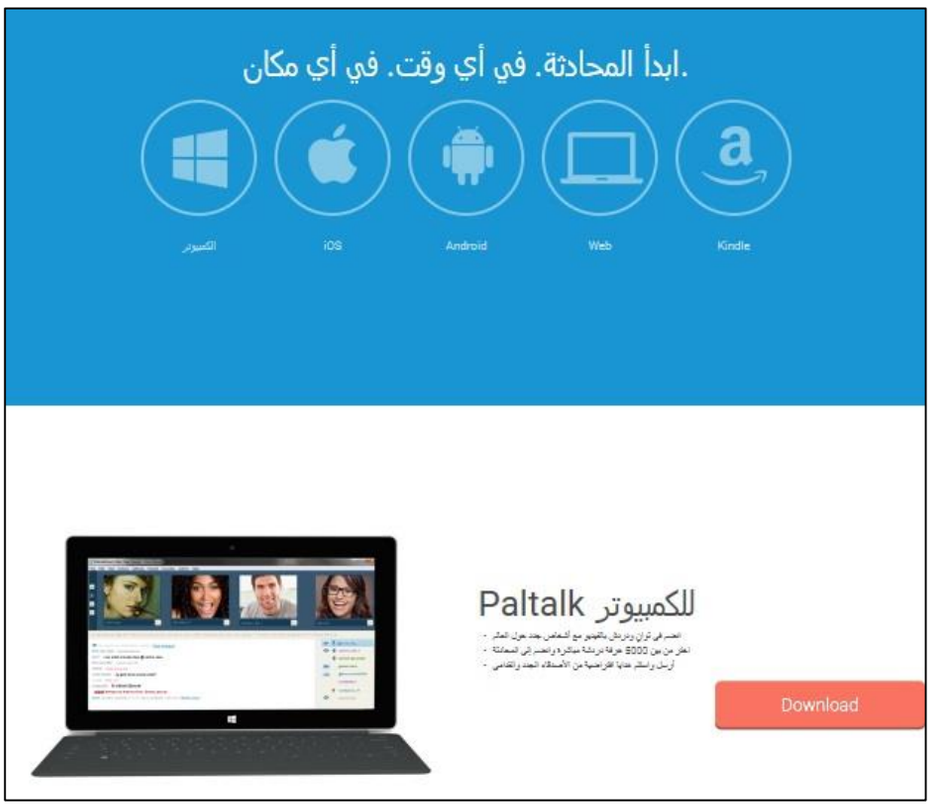
- استخدام أجهزة الكمبيوتر والأجهزة الشخصية، بما في ذلك استخدام برامج مكافحة الفيروسات.
- الوصول إلى الإنترنت واستخدامه.
- القواعد غير الرسمية لاستخدام الإنترنت أو ما يسمى (آداب استخدام الإنترنت).
- القواعد الخاصة باستخدام شبكات التواصل الإجتماعي وإنشاء هويات الإنترنت وحماية أسماء المستخدمين وكلمات المرور.
- تنزيل المواد بما في ذلك المحتوى المحفوظ بحقوق الطباعة والنشر.
- قواعد الخصوصية.
- السلوكيات غير المقبولة.

وقد تتضمن السلوكيات غير المقبولة على سبيل المثال، إنشاء المستندات أو الصور أو المواد العدائية ونقلها والمصممة لمضايقة الأشخاص، كما تتضمن السلوكيات المحظورة الأخرى كل ما ينتهك حقوق الطبع والنشر الخاصة بشخص آخر والوصول غير المرخص والمقصود إلى خدامات أخرى عن طريق الاتصال بالإنترنت.

3-1-8-2 فهم سياسات تعديل عامل تشغيل الهاتف المحمول مع الأخذ في الاعتبار الوصول إلى غرف الدردشة أو الألعاب والتحكم في رسائل البريد الإلكتروني غير المرغوب فيها

تحتوي غرف الدردشة وألعاب الإنترنت على مشرفين للتأكد من عمر المستخدمين الجدد، ويقوم المشرفون أيضًا بمراقبة المحادثات، كما يمكنهم تعليق عضوية المستخدمين الذين يستخدمون لغة غير مناسبة والمستخدمين الذين يتحرشون بغيرهم أو يضايقونهم أو يرسلون رسائل بريد إلكترونية غير مرغوب فيها، فإذا شعرت بشيء من هذا القبيل مثلا، أبلغ المشرف على الفور.

برنامج بال توك (Paltalk) الخاص بجوجل هو مثال لغرف الدردشة، انظر الشكل 43 أدناه:



الشكل 43: مثال لغرف الدردشة على الهاتف المحمول - http://www.paltalk.com

ينشر برنامج بال توك (Paltalk) السياسات الخاصة بالمحادثات المعتدلة، وفيما يلي نموذج منها.
: http://www.paltalk.com/support/RoomAdmin.html

تحتوي معظم غرف الدردشة على مشرفين أو مسؤولين، ويتميز هذا المسؤول بوجود علامة @ قبل اسمه، ويساعد المسؤول في السيطرة على الغرفة وإدارة موضوعات المحادثات وتحديد من يخاطب المستخدمين الموجودين في الغرفة عن طريق الميكروفون.

يتوفر لمسؤولي غرف الدردشة الكثير من أدوات التحكم للسيطرة على ترتيب الخصائص والمحادثات في الغرف، فيمكنهم استخدام "النقطة الحمراء" للتحكم في من يتحدث أو يرسل مقاطع فيديو أو رسائل نصية، كما يمكنهم "الرد بشكل مفاجئ" أو "حظر" أي مستخدم في الغرفة يتكلم بطريقة عدائية أو يخالف النظام.

تتبع كل شركات المحمول سياسات مشابهة تهدف إلى الإشراف على المحادثات المعتدلة.

8-2 السياسة المتبعة

2-8-2 حقوق الطبع والنشر

1-2-8-2 الدراية بقوانين حقوق الطبع والنشر وأثرها في حالة التنزيل غير القانوني من خلال خدمات مشاركة الملفات

حقوق الطبع والنشر هي حق المؤلف في أعمال النسخ والترخيص أو غير ذلك من طرق الاستفادة من الأعمال الأدبية أو الموسيقية أو الفنية، ويمكن للمؤلف نقل حقوق الطبع والنشر إلى ناشر أو شخص آخر، ويعد صاحب هذه الحقوق هو الوحيد الذي يحق له نسخ هذه الأعمال، ويحتاج باقي الأشخاص إلى تصريح يمنح مقابل رسوم معينة تسمى عوائد المؤلف.

أصبح التنزيل غير القانوني للمحتويات أحد أكبر مشكلات العصر الرقمي، وتمتد آثاره عبر كافة أشكال المحتويات والوسائط الرقمية مثل: - الأفلام والموسيقى والكتب وغير ذلك من المحتويات الرقمية، ويمكن تنزيل أحد هذه الملفات بالنقر فوق ملف لمقطوعة موسيقية أو مقطع فيديو أو كتاب أو ملف من خلال أحد مزودي الخدمة الشرعيين مثل موقع iTunes أو موقع Amazon، وقد يلزم دفع رسوم لاستخدام الملف ثم تنزيله إلى أحد أنظمة الكمبيوتر وإعادة استخدامه مرة أخرى على أجهزة iPods، أو أجهزة الألعاب، أو الهواتف المحمولة أو أجهزة الكمبيوتر وذلك على حسب الرخصة الممنوحة.

2-2-8-2 إدراك عدم شرعية قرصنة الموسيقى والأفلام والبرامج وإدراك تأثيرات هذه الأعمال

تكون بعض هذه المواد متاحة للجميع مما يعني إمكانية نسخها واستخدامها دون قيود ومن بينها، المواد الأدبية والموسيقية والصور (وكذلك الأفلام) والبرامج، ولا يجوز نسخها بأي شكل إذا كانت محفوظة بحقوق طبع ونشر، ويساءل من يقوم بذلك قانونيًا أمام المحاكم وقد يعاقب في بعض البلدان بتعليق خدمة الإنترنت لديه.

إن القرصنة واحدة من المشكلات المتزايدة في مجتمع الإنترنت، فمتوسط قيمة قرصنة الموسيقى لجهاز iPod تقدر بـ 800 دولار - http://www.go-gulf.com/blog/online-piracy/. تفضلوا بزيارة موقع مدونة قرصنة الإنترنت بالأرقام لمزيد من المعلومات: - http://www.go-gulf.com/blog/online-piracy/

اختبار

س1- توجد وثيقة لتفصيل قواعد استخدام أجهزة الكمبيوتر، ولابد من الموافقة على ما بها من قواعد قبل الوصول إلى شبكة معينة، وتحمل الوثيقة الاختصار AUP، فإلام يشير هذا الاختصار؟

أ- مبادئ الاستخدام المقبول
ب- برنامج الاستخدام المقبول
ج- سياسة المستخدم المقبول
د- سياسة الاستخدام المقبول

س2- فكر في العبارات التالية: "كل شيء مجاني على الإنترنت" هل العبارة صواب أم خطأ؟

أ- صواب
ب- خطأ

س3- مَنْ لديه حق تعليق نمط المحادثات في المنتديات أو غرف الدردشة الموجودة على الإنترنت؟

أ- المراقب
ب- المشرف
ج- القائد
د- المستخدم

س4- ما المصطلح المستخدم لوصف الحق الحصري في نسخ الأعمال الأدبية أو الفنية أو ترخيصها؟

أ- حقوق المستخدم
ب- حقوق الطباعة
ج- حقوق الطبع والنشر
د- الحقوق الفنية

الإجابات في الصفحة التالية

الإجابات

س1- د- سياسة الاستخدام المقبول (AUP)
س2- ب- خطأ
س3- ب- المشرف
س4- ج- حقوق الطبع والنشر

تمارين

2-ت-1 فيس بوك

2-ت-2 تويتر

2-ت-3 يوتيوب

2-ت-4 جوجل+

2-ت-5 لينكدإن

2-ت-6 المدونات

ملاحظة: ينبغي استخدام التعليمات والصور الواردة في هذا الفصل كدليل لتحقيق الأهداف، فمواقع التواصل الاجتماعي يمكن أن تغير نظام أو محتوى كل خطوة في أي وقت، ومن ثم فإننا ننصح بمراجعة كل تمرين لفهم الهدف منه قبل أداء الأنشطة.

تمارين - فيس بوك

بعد أن قمت بإنشاء حسابك على موقع التواصل الاجتماعي فيس بوك وبدأت في إضافة الأصدقاء وأصدقاء الأصدقاء والأشخاص الذين تعرفهم أو لا تعرفهم، كل ما عليك الآن هو النظر في سلامتك على الإنترنت، حيث يتم معالجة كلاً من مسألة الخصوصية والحماية في التمرين الوارد أدناه، اقرأ الخطوات وتتبع الصور للقيام بهذه العملية.

تدابير السلامة على موقع التواصل الاجتماعي فيس بوك:

1- على صفحتك الرئيسية على موقع فيس بوك انقر فوق رابط رمز الحماية الذي يشبه القفل ( ) الموجود أعلى يسار النافذة من القائمة الرئيسية، حيث يمكنك أن ترى اختصارات الخصوصية.

2- أول شيء تراه تحت العنوان (كما هو معروض في الشكل أعلاه هو Privacy Check-up (التحقق من الخصوصية)، ولكن بدلا من ذلك اضغط على Who can see my stuff? (من يستطيع رؤية محتواي؟) حيث سيظهر سؤال آخر عن منشوراتك وهو مضبوط على وضع Public (عام)، وهنا اضغط على السهم واضبط هذا الخيار على Friends (الأصدقاء) لكي يتمكن الأصدقاء فقط من رؤية منشوراتك، (انظر الشكل الموجود بالصفحة التالية).

3- لقد تعلمنا كيفية استخدام اختصارات الخصوصية في النشاط السابق، والآن اضغط على خيار See More Settings (اعرض مزيدا من الإعدادات) الموجود بالجزء السفلي، حيث ستختار من القائمة المنسدلة Privacy Settings (إعدادات الخصوصية و أدواتها)، وسوف تلاحظ أن هناك بعض النقاط المشتركة مع قسم اختصار الخصوصية، (انظر الشكل أدناه).

4- في نافذة Privacy Settings and tools (إعدادات الخصوصية وأدواتها) اضغط على الخيار Review all your posts and things you're tagged in (مراجعة كل منشوراتك والمحتوى الذي تتم الإشارة إليك فيه) الذي سينقلك إلى صفحة اليوميات الخاصة بك وسيعرض كل المنشورات والأماكن التي تتم الإشارة إليك فيها منذ شهر أو حتى منذ سنة، إذا كنت ترغب في عدم ظهور الإشارة للجميع في أي مكان، اضغط على زر القلم الرصاص ( ) وحدد خيار Remove Tag (إزالة الإشارة).

5- استخدم قسم Who can look me up? (من يستطيع البحث عني؟) إذا كنت ترغب في تحديد عدد الأشخاص الذين يبحثون عن بريدك الإلكتروني أو رقم الهاتف الخاص بك على فيس بوك، أو إذا كنت ترغب في الحد من البريد المزعج من المصادر غير المعروفة، اضغط على مربع التعديل واختر Friends of Friends (أصدقاء الأصدقاء) أو Friends (الأصدقاء)، (كما هو موضح بالشكل أدناه).

6- يحدد الخيار Who can look me up? (من يستطيع البحث عني؟) ما إذا كان الآخرون يستطيعون البحث عنك من خلال أي محرك بحث مثل جوجل على سبيل المثال، لتخصيص ملفك الشخصي تأكد من إزالة العلامة الموجودة في المربع المجاور لعبارة Let other search engines link to your timeline (هل ترغب في ربط محركات بحث أخرى بيومياتك؟)، (مربع علامة التحديد موضح أدناه).

7- توجد فئة خصوصية أساسية أخرى في لوحة المعلومات الموجودة بالجانب الأيمن من الشاشة هي Timeline and Tagging Settings "إعدادات اليوميات والإشارة" حيث يمكنك التحكم في الأشخاص الذين يرون اليوميات خاصتك. مع ملاحظة أن اليوميات هو عبارة عن تصميم الرسومات التي تعرض قائمة الأنشطة والأحداث والمشروعات والتوجهات وغير ذلك مصنفة وفقًا للتواريخ ووفقًا للترتيب الزمني، وعند الدخول في هذا القسم سوف يظهر جدول إعدادات، (انظر الشكل أدناه).

8- في قسم Who can add things to my timeline? (من يستطيع إضافة محتوى إلى يومياتي؟) يمكنك تحديد من يمكنه النشر على يومياتك، ولجعل هذا الخيار أكثر خصوصية، اضبط الإعداد على Friends (الأصدقاء).

9- يتيح لك خيار Review all your posts and things you're tagged in ((هل ترغب بمراجعة المنشورات التي يشير إليك فيها أصدقاؤك قبل ظهورها في يومياتك؟، الموافقة على أي صور أو منشورات تمت الإشارة إليك فيها قبل عرضها على يومياتك، وبمجرد الضغط على خيار Edit (تعديل) الموجود ناحية اليسار يمكنك اختيار الخيار النشط من القائمة المنسدلة.

10- اضغط على الرمز ليظهر Privacy Shortcuts (اختصارات الخصوصية) وانزل إلى خيار who can send me friend requests (من يستطيع إرسال طلبات الصداقة لي) المنسدل من خيار who can contact me (من يستطيع الاتصال بي) واختر Friends of Friends (أصدقاء الأصدقاء) لتقييد تلقي طلبات من الجميع. (انظر الشكل أدناه).

11- الإعداد الأخير الذي يظهر على القائمة المنسدلة Privacy Shortcuts "اختصارات الخصوصية" متعلق بمسائل الحظر، اضغط على السهم القريب من السؤال How do I stop someone from bothering me? (كيف أمنع أحد من مضايقتي؟) ثم أدخل الاسم أو البريد الإلكتروني للشخص الذي تريد حظره أو إلغاء الصداقة معه أو منعه من بدء المحادثات معك أو رؤية محتوى ما تنشره على يومياتك، وهذا الإعداد له أهميته الخاصة بالنسبة للآباء حيث يمكنهم الدخول على مزيد من المعلومات من خلال خيار Privacy Settings (إعدادات الخصوصية) المذكور أعلاه لتوفير المزيد من الأمن لأبنائهم.

تمارين - تويتر

لكي تدير إعدادات الخصوصية على تويتر، سجل الدخول على حسابك وقم بمراجعة العديد من الإعدادات الافتراضية، اضغط على الرمز الموجود في أعلى الجانب الايسر من الشاشة، ،واختر Settings (الإعدادات) من القائمة المنسدلة. (انظر الشكل أدناه).

1- يظهر العديد من الإعدادات ناحية اليسار، أولها Account (الحساب) المفتوح بالفعل يسار الشاشة.

2- اضغط على Security and Privacy (الأمان والخصوصية) وابحث عن خيار Discoverability (قابلية الاكتشاف) أسفل الصفحة للسماح للآخرين بالعثور عليك بواسطة البريد الإلكتروني الخاص بك، والأمر متروك لك في وضع علامة على المربع أو لا، (انظر الشكل أدناه).

3- من خلال Security and Privacy (الأمان والخصوصية)، يمكنك الاختيار بين عرض الموقع الذي تغرد منه من عدمه عن طريق وضع علامة في المربع الموجود في الناحية اليسرى لخيار Add location to my Tweets (إضافة الموقع الجغرافي إلى تغريداتي) (كما هو موضح بالشكل أدناه)، يرجى الانتباه إلى أن إضافة الموقع الجغرافي إلى تغريداتك قد تجعلك أكثر عرضة للمتحرشين، لذا يُنصح بترك هذا المربع دون وضع علامة.

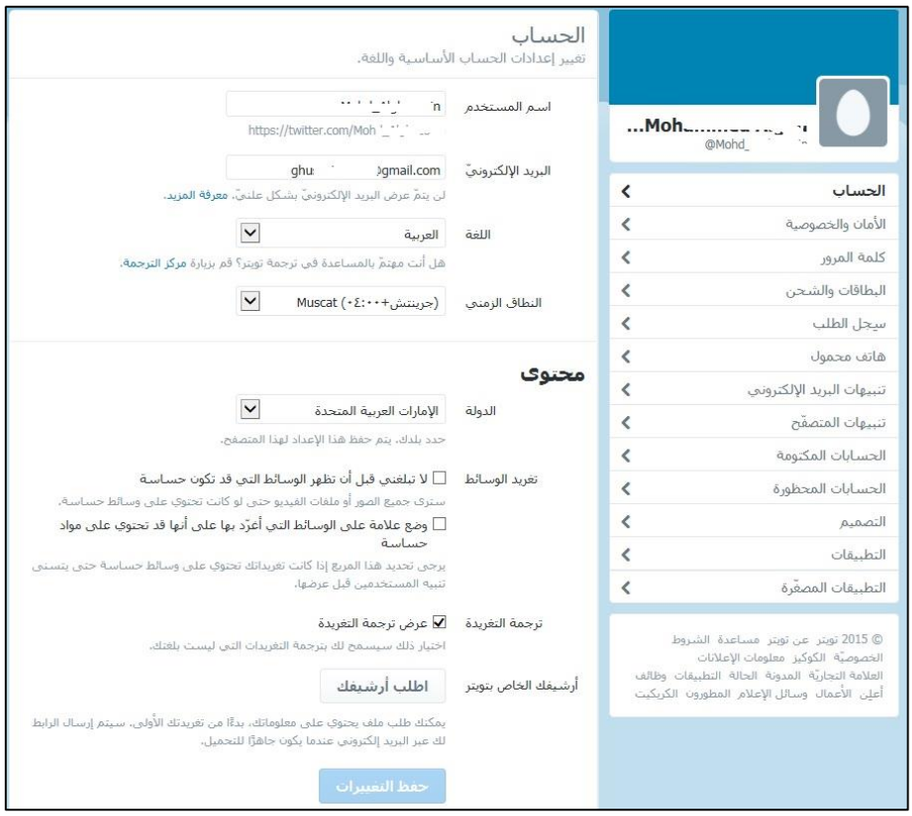
4- في خيار Tweet Privacy (خصوصية التغريد)، إذا قمت باختيار Protect my Tweets (حماية تغريداتي) فأنت تسمح لمجموعة معينة من الناس برؤية تغريداتك بينما تمنع غيرهم، وهذا الخيار مهم جدًا لمساعدة الآباء في حماية أطفالهم من الأشخاص الذين يتفاعلون معهم.

5- لا تنس حفظ التغييرات بعد الانتهاء من التعديل، فقد تحتاج عندئذٍ إلى إدخال كلمة المرور مرةً أخرى للتأكيد.

الفئة الثانية للإعدادات الموجودة في القائمة اليمنى هي Password (كلمة المرور)، ومن خلالها يمكنك تغيير كلمة المرور إذا احتجت لذلك.

1- أدخل كلمة المرور الحالية.
2- أدخل كلمة مرور جديدة وقم بتأكيدها، واحرص على اختيار كلمة مرور صعبة حتى لا يتسنى للآخرين تخمينها بسهولة.
3- من الضروري حفظ التغييرات.

اختيار Profile (الحساب) من القائمة الموجودة في الناحية اليمنى يعرض عدة خيارات، (كما هو موضح بالشكل أدناه).



1- تظهر صورتك في المقدمة، والأمر إليك في إضافة صورة جديدة أو تغيير الصورة القديمة أو ترك مكانها فارغًا.
2- املأ الحقول وفقًا للدليل المعروض على الشاشة، وانتبه إلى ما تقوم بالإعلان عنه على صفحة تويتر الخاصة بك.
3- وكما تعودنا في الخيارات السابقة، لا تخرج قبل الضغط على Save Changes (حفظ التغييرات)، (انظر الشكل أدناه).

غالبًا ما يستخدم الأشخاص خدمات الارتباطات القصيرة لتقصير عناوين الويب، وذلك لأن عدد الحروف المسموح به في التغريدة الواحدة هو 140 حرفًا كحد أقصى. وهذا يمنع القارئ من رؤية وجهة الارتباط الحقيقية، مما قد يؤدي به إلى مواقع الويب الخبيثة.

اتبع الإجراءات الوقائية التالية:

ثبت سهم الماوس على الرابط الموجود في التغريدة وتحقق من وجهته التي تظهر لك قبل الضغط عليه. (كما هو موضح بالشكل في الصفحة التالية).

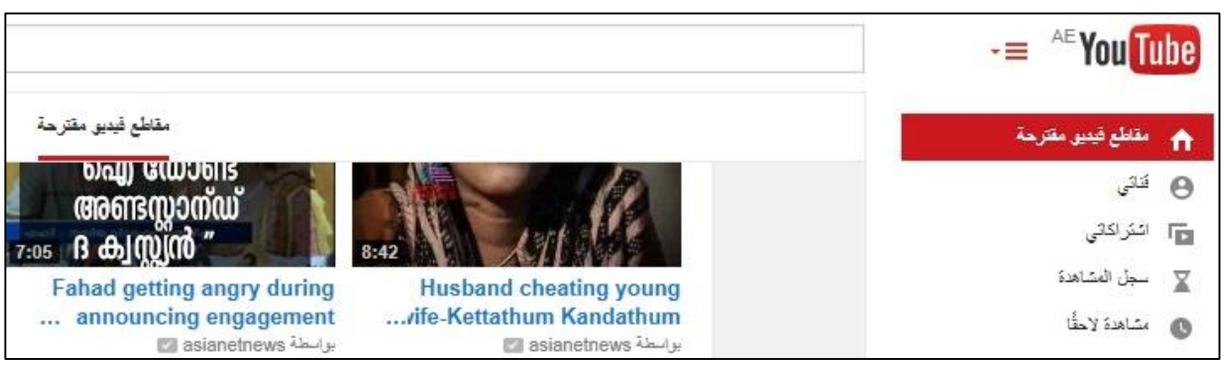
لا تنس تسجيل الخروج من الموقع عند الانتهاء.

تمارين - يوتيوب

بعد تسجيلك الدخول على حساب يوتيوب، يمكنك الاستمتاع بالعديد من الميزات على الموقع والحفاظ على الخصوصية في الوقت نفسه.

وكما تناولنا الحديث عن منصات التواصل الاجتماعي الأخرى، ينبغي عليك القيام بما يلي:

1- اضغط على صورة الملف الشخصي في أعلى الجانب الأيمن من الشاشة وحدد YouTube settings (إعدادات يوتيوب) من قائمة YouTube (يوتيوب) (انظر الشكل أدناه).



2- اختر Privacy (الخصوصية) من لوحة المعلومات الموجودة بالناحية اليمنى تحت Account Settings (إعدادات الحساب)

3- يمكنك وضع علامة على Keep all my subscriptions private (الحفاظ على خصوصية الاشتراكات) أسفل عنوان Likes and Subscriptions (إبداءات الإعجاب والاشتراكات) إذا كنت لا ترغب في مشاركتها مع الآخرين. (كما هو موضح بالشكل أدناه).

4- لا تنس حفظ التغييرات التي أجريتها.

5- وتذكر دائمًا أن تسجيل الخروج من أي حساب يسهم بشكل كبير في حماية خصوصيتك على الإنترنت. ويمكنك فعل ذلك عن طريق العودة إلى صورة الملف الشخصي والضغط عليها وتحديد الخيار "تسجيل الخروج".

تمارين - جوجل+

كما هو الحال مع أي خدمة للتواصل الاجتماعي، من المهم فهم المخاطر المحتملة لما تقوم بمشاركته مع الآخرين، وإليك بعض التوصيات للمساعدة.

1- من شاشة Home (الصفحة الرئيسية) لجوجل+ اضغط علامة

الموجودة أعلى اليمين تحت+ Google (جوجل+) واختر Settings (الإعدادات) من القائمة المنسدلة. (انظر الشكل أدناه).

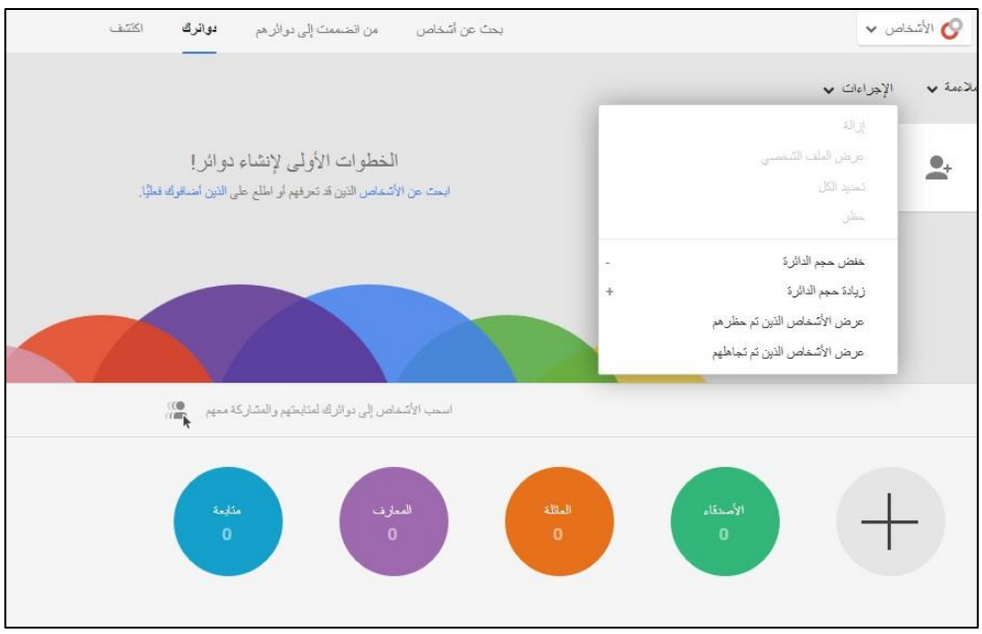
2- انتقل للأسفل وصولاً إلى Profile (الملف الشخصي). (كما هو موضح بالشكل أدناه).

3- أزل علامة التحديد من خيار Help others discover my profile in search results (مساعدة الآخرين في اكتشاف ملفي الشخصي في نتائج البحث) لجعل الملف الشخصي أكثر خصوصية على جوجل+ حيث إن ذلك سيمنع محرك البحث جوجل وغيره من فهرسة ملفك الشخصي.

على شاشة People (الأشخاص) التي يمكن الوصول إليها من شاشة Home (الصفحة الرئيسية) اضغط علامة الموجودة أعلى اليمين أسفل +Google (جوجل+) واضغط الزر Your circles (دوائرك).

1- من خلال الضغط على هذا الزر، ستنتقل إلى صفحة دوائر أخرى (انظر الشكل أدناه)، يمكنك اختيار أي شخص في أي دائرة من الدوائر المعروضة.

2- عقب ذلك، اضغط على السهم الموجه لأسفل من زر Actions (الإجراءات) في أعلى الزاوية اليمنى من الشاشة.
3- يمكنك تحديد (إزالة/عرض الملف الشخصي/حظر،إلخ) الشخص المراد. (انظر الشكل أدناه).



4- يمكنك أيضًا في إطار الخيار ذاته (الإجراءات) اختيار عرض الأشخاص الذين تم حظرهم أو تجاهلهم.

ومن خلال نافذة Photos and Videos (الصور والفيديوهات) الموجودة في صفحة Settings (الإعدادات) يمكنك إجراء تعديلات على الوصول والخيارات. (انظر الشكل أدناه).

1- انتقل الآن إلى أعلى صفحة Settings (الإعدادات) من أجل التفاعل والمشاركات، اضغط الزر المكون من سهمين موجهين والمجاور للسؤال الأول، حيث يمكنك اختيار المجموعات التي من الممكن أن ترسل لك الإشعارات من خلال القائمة المنسدلة، (كما هو موضح بالشكل أدناه).

2- الاختيار الأمثل هو Extended circles (الدوائر الممتدة) ولكن من الممكن أن تختار Anyone (أي شخص) للسماح لأي شخص بإرسال إشعارات إليك، ويفضل اختيار Your Circles (دوائرك) لجعل الملف الشخصي أكثر خصوصية.

3- يجب أن ننظر في بقية القائمة لفهم الخيارات المتاحة وإجراء التعديلات المناسبة لمستويات الراحة الخاصة بك.

لا تنس تسجيل الخروج من الموقع بالضغط على في أعلى الزاوية اليسرى من الشاشة، والضغط على زر sign out (الخروج).

تمارين - لينكدإن

لينكد إن هو موقع تواصل مهني قد تسبب فيه (الأخطاء) دمارًا لحياتك المهنية وقد تسبب مسائل الخصوصية المهملة خطرًا للمهنة بأكملها.

ومن الضرورة إتباع الخطوات الواردة أدناه لأنظمة الأمان والسلامة على شبكة الإنترنت مع العلم أننا نقدم لك المفهوم الذي يتناسب مع الخطوات العملية ونترك باقي الخطوات لك لتكتشفها بنفسك.

1- بعد تسجيل الدخول على حساب لينكد إن، يتعين عليك أن تحرك الماوس أعلى صورة الملف الشخصي الموجودة أعلى يسار الشاشة ثم اختر Privacy & Settings (الخصوصية والإعدادات). (كما هو موضح بالشكل أدناه)،

2- سيتم عرض صفحة أخرى على الشاشة مع فتح بعض الخيارات لك. (انظر الشكل أدناه).

الملف الشخصي

في نافذة Privacy Controls (عناصر التحكم في الخصوصية) الخاصة بالملف الشخصي اضغط الخيار Turn on/off your activity broadcasts (تشغيل/إيقاف عمليات بث الأنشطة) النافذة المكونة من جملة.

Let people know when you change your profile، make recommendations، or follow companies اسمح للأشخاص بمعرفة متى أجريت تغييرًا على ملفك الشخصي، أو قدمت تزكيات، أو تابعت شركات

إذا اخترت تشغيل هذا الخيار عن طريق وضع علامة داخل المربع الصغير، سيتم إبلاغ كل شخص من الاتصالات المباشرة بشأن كل تغيير يحدث على ملفك الشخصي، وإذا لم ترغب في رؤية مديرك الحالي للتغييرات التي تحدث في ملفك الشخصي، يمكنك إيقاف هذا الخيار، مع العلم بأنه يتعين عليك Save Changes (حفظ التغييرات) لأي من هذين الخيارين.

3- عند التعامل مع الإعداد What others see when you've viewed their profile (تحديد ما يراه الآخرون عندما تشاهد ملفاتهم الشخصية)، سوف تظهر نافذة أخرى على الشاشة وبها ثلاثة خيارات:

- خيار Your name and headline (اسمك وعنوانك) (وهذا هو الخيار الوحيد الموصى به، وذلك عن طريق الضغط داخل الدائرة، للسماح للشخص الذي رأيت ملفه الشخصي قبل ذلك).
- خيار Anonymous Profile characteristics (خصائص الملف الشخصي التي لا تحدد الهوية) سوف يظهر فقط الصناعة والعنوان.
- خيار Anonymous Profile characteristics (خصائص الملف الشخصي التي لا تحدد الهوية) سوف يظهر فقط الذي قمت بعرضه لشخص لآخر.

4- لا تنس ان تضغط Save Changes (حفظ التغييرات).

من خلال خيار Change your profile photo & visibility (تغيير صورة ملفك الشخصي والظهور) يمكنك:
(انظر الشكل أدناه).

1- تحميل صورة (مع الأخذ في الاعتبار المظهر المهني)
2- اختيار الأشخاص الذين ستظهر لهم الصورة (يوصي باستخدام خيار لكل شخصٍ).
3- تأكد من Save Changes (حفظ التغييرات).

الإخطارات

سترى ثلاث عناوين من خلال Communications (الاتصالات).
(انظر الشكل أدناه).

- **Emails and Notifications (رسائل البريد الإلكتروني والإشعارات)**
- **Member Communications (اتصالات الأعضاء)**
- **LinkedIn Communications (اتصالات لينكد إن)**

1- اضغط الخيار Select the types of messages you are willing to receive (تحديد أنواع الرسائل التي ترغب في استلامها) الموجود في Member Communications (اتصالات الأعضاء).
2- في النافذة التي تظهر على الشاشة، يوصي باختيار Introductions and InMail only (التعارفات وInMail فقط (تمت التوصية)، اختر الخيارات المناسبة لك ثم اضغط Save Changes (حفظ التغييرات).

يسمح لك الإعداد Select who can send you invitations (تحديد من يمكنه إرسال الدعوات إليك) بثلاثة خيارات: (انظر الشكل أدناه).

3- يوصي لينكد إن بالخيار الأول ثم Save Changes (حفظ التغييرات).

Companies & Applications،Groups (المجموعات والشركات والتطبيقات)

من خلال الانتقال إلى Companies & Applications،Groups (المجموعات والشركات والتطبيقات)، ستلاحظ أربع فئات: (انظر الشكل في الصفحة التالية)

- **Groups (المجموعات)**
- **Companies (الشركات)**
- **Applications (التطبيقات)**
- **Privacy Controls (عناصر التحكم في الخصوصية)**

يمكنك الدخول إلى أي مما سبق وتخصيص حساب لينكد إن وفقًا لذلك.

Account (الحساب)

يشمل إعداد Account (الحساب) ما يلي: (انظر الشكل أدناه).

- **Privacy Controls (عناصر التحكم في الخصوصية)**
- **Settings (الإعدادات)**
- **Email & Password (البريد الإلكتروني، والهاتف، وكلمة المرور)**
- **Helpful Links (روابط مفيدة)**

1- يمكنك إضافة وتغيير عناوين البريد الإلكتروني من خلال Email،Phone & Password (البريد الإلكتروني والهاتف وكلمة المرور).

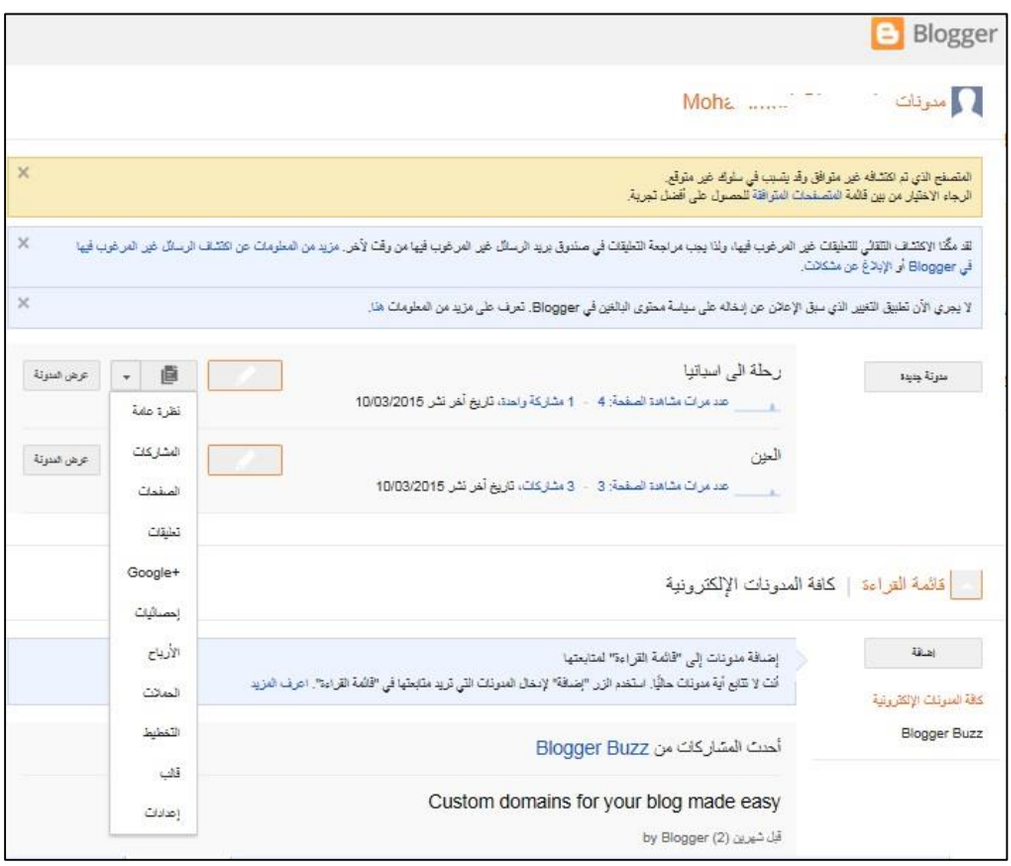
2- ومن خلال نفس الخيار يمكنك تغيير كلمة المرور بالضغط على Change password (تغيير كلمة المرور) وإدخال كلمة المرور القديمة ثم اختيار كلمة مرور جديدة قوية يصعب تخمينها ثم تأكيد الكلمة الجديدة.

تمارين ـ المدونات

بعد الدخول إلى حساب المدونة:

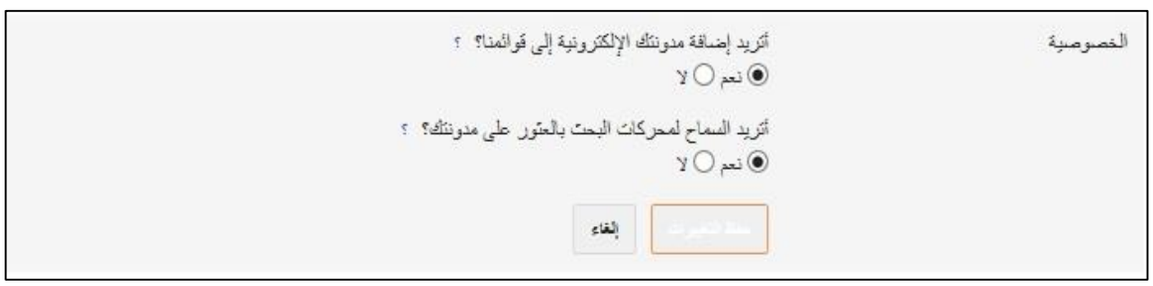
1- اضغط السهم المتجه لأسفل جانب زر ( ) (الانتقال إلى قائمة المشاركات) على لوحة التحكم بالمدونة.

2- اختر **Settings (الإعدادات)** من القائمة المنسدلة، (كما هو موضح بالشكل أدناه).



3- اضغط الزر Edit (تعديل) المواز لعلامة التبويب **Privacy (الخصوصية)** في صفحة Settings (الإعدادات). (انظر الشكل أدناه).

4- يوصى باختيار yes (نعم) كإجابة على السؤالين. (كما هو موضح بالشكل أدناه).



5- احفظ التغييرات.

انتقل لأسفل نحو علامة التبويب **Permissions (الأذونات)**:

1- ستلاحظ أنه تم ضبط كلمة Public (عام) افتراضيًا بجوار Blog Readers (قراء المدونة).

2- إذا كنت ترغب في عدم تقييد القراء من الوصول، فمن المستحسن أن تبقي هذا الخيار وتحفظ التغييرات.

لا تنس تسجيل الخروج في كل مرة للسلامة.