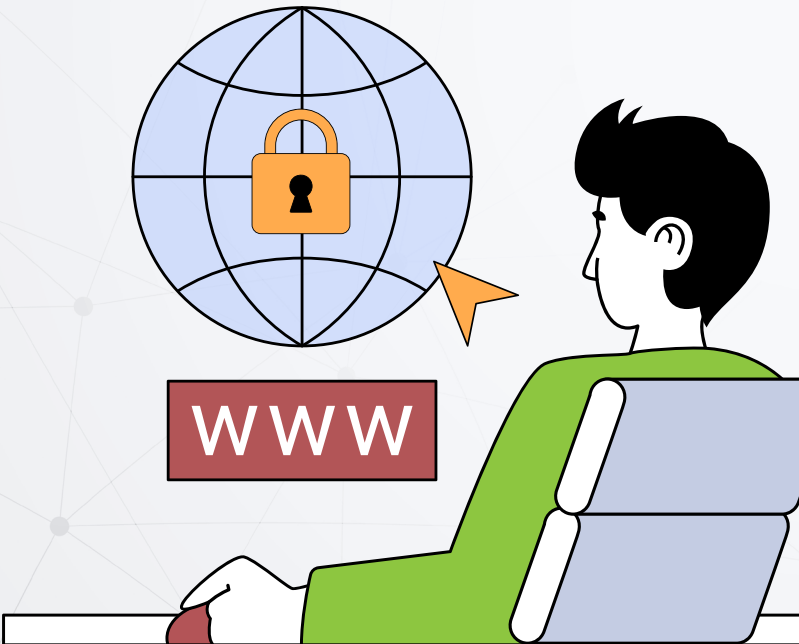
حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

دليل تعليم الأمان الرقمي لليافعين



حملة – المركز العربي لتطوير الإعلام الاجتماعي
دليل تعليم الأمان الرقمي لليافعين

حزيران 2025

تأليف: حملة – المركز العربي لتطوير الإعلام الاجتماعي
المراجعة اللغوية: شاهين نصار
تصميم: أمل شوفاني

اتصلوا بنا:

البريد الإلكتروني: info@7amleh.org

الموقع الإلكتروني: **www.7amleh.org**

الهاتف: 774020670 (0) 972+

صفحاتنا على وسائل التواصل الاجتماعي: **7amleh**

الفهرس

كيف يعمل الإنترنت؟

الإنترنت بالمفهوم التقني هو شبكة مكوّنة من عدة شبكات، وكل من هذه الشبكات تحتوي على عدة مكوّنات (أجهزة الحاسوب، الهاتف النقال، الراوترات، الخوادم، الخ..)، لكن قد يصعب على الأطفال بسنّ 10-13 سنة فهم هذا المفهوم. وعليه، بالإمكان تبسيطه لأفكار مرتبطة بحياتهم اليومية.

على سبيل المثال، لنتخيَّل الإنترنت كشبكة طرق عملاقة تربط ملايين المستخدمين والمباني حول العالم؛ يمكن تشبيه البيانات بالرسائل البريدية، والخوادم بالمباني الضخمة مُتعددة الطوابق والغرف. بفضل الانترنت، يمكننا إرسال الرسائل، مشاهدة الفيديوهات، البحث عن المعلومات، ولعب الألعاب في ثوانٍ معدودات. لكن كيف يحدث كل هذا؟ دعونا نشرح الأمر بالتبسيط!

1. الإنترنت مثل شبكة طرق ضخمة

فكّـر في الإنترنـت على أنـه نظـام طـرق سريعـة يربـط بين مـدن مختلفـة. بـدلاً مـن السـيارات، يقـوم الإنترنـت بنقـل البيانـات (مثـل الرسـائل، مقاطـع الفيديـو، والمواقـع الإلكترونيـة) بين الأجهـزة.

- جهـازك (الهاتـف، الحاسـوب/ الكمبيوتـر، أو الجهـاز اللـوحي/ تابلـت) هـو مثـل منزلـك المربـوط بهـذه الطرقـات.

- المواقـع الإلكترونيـة والتطبيقـات (مثـل يوتيـوب وجوجـل) أشـبه بالمبـاني الضخمـة في مـدن أخـرى.

- مـزوّد خدمـة الإنترنـت (ISP) أشـبه بشركـة الطـرق المحليـة الـتي تمنحـك وسـيلة التنقـل عـبر هـذه الشـبكة وتسـمح لـك باسـتخدام الطـرق الدوليـة الـتي تمكنـك مـن الوصـول لمنـازل في دول أخـرى.

2. عناوين رقمية لتحديد المواقع

- كل موقـع إلكـتروني لـه عنـوان يُسـمى عنـوان URL (مثـل www.google.com). لكـن أجهـزة الحاسـوب لا تفهـم الأسـماء كمـا نفهمهـا نحـن، فهـي تسـتخدم عناويـن بروتوكـول الانترنـت IP Internet Protocol مثـل (123.456.789.159) وهـو المُعـرّف الرقمـيّ لأي جهـاز مرتبـط بشـبكة معلوماتيـة عـبر حزمـة شـبكات الانترنـت.

- لتسـهيل الأمـور، نسـتخدم خـوادم DNS (نظـام أسـماء النطـاق Domain Name System) الـتي تعمـل كدليـل لأرقـام الهواتـف، إذ أنهـا تحتـوي عـلى أسـماء المواقـع مـع عناويـن الـ IP المرتبطـة بهـا حـتى يتمكـن جهـازك مـن الوصـول إليهـا بسـهولة عندمـا تقـوم بتزويـده باسـم الموقـع فقـط.

- يساعد مزوّد خدمة الإنترنت (مثل شركة بالتل أو مدى) في تنفيذ هذه العملية عبر إيجاد أسرع طريق لنقل البيانات، وهذا الطريق غير ثابت وقد يتغيّر باختلاف مستويات الازدحام على الشبكة (تماما كما الطرق) خلال اليوم.

3. أين تعيش المواقع الإلكترونية والتطبيقات؟

عندما تزور موقعًا إلكترونيًا أو تستخدم تطبيقًا، فأنت تتصل بـ خادم (Server) وهو جهاز حاسوبيّ ضخم يقوم بإرسال واستقبال وتخزين المعلومات حسب الحاجة.

على سبيل المثال:

- عندما تكتب www.youtube.com في المتصفح، يقوم جهازك بإرسال طلب إلى خادم DNS حتى يتمكن من استخراج عنوان الـ IP الخاص بيوتيوب، ثم يقوم بإجراء اتصال مع خوادم يوتيوب ويطلب منها مجموعة الفيديوهات المعروضة على الصفحة الرئيسية.

- يعثر الخادم الخاص بيوتيوب على مقاطع الفيديو المطلوبة ويرسلها إلى جهازك بسرعة فائقة.

4. المعلومات تنتقل على شكل رُزم بيانات

عندما ترسل رسالة أو تفتح موقعًا، لا تنتقل المعلومات كقطعة واحدة، بل تتم تجزأتها وتُرسل كمجموعة من الرُزم أو الحُزم الصغيرة التي تُسمى Packets.

تخيل أنك ترسل لعبة ليجو إلى صديقك في مدينة أخرى:

- تفكّك اللعبة إلى قطع صغيرة.
- يتم إرسال كل قطعة في طرد منفصل.
- عند وصولها، يقوم صديقك بإعادة تجميع اللعبة.

هـذا بالضبـط مـا يحـدث مـع البيانـات على الإنترنـت! تنتقـل الـرُزم عبر مسـارات متنوّعـة (مثـل الكوابـل، و الأقمـار الصناعيـة، والشبكات اللاسـلكية) حتى تصـل إلى وجهتهـا النهائيـة.

5. دور مزوّدي خدمات الإنترنت

مـزوّد خدمـة الإنترنـت هـو الشركـة التي تمنحـك القـدرة على الاتصـال بالإنترنـت. إذا أردنـا أن نمثـل دوره في تشبيـه الطـرق، بالإمـكان اعتبـار مـزوّد الخدمـة كالطـرق الداخليـة في الدولـة، كمـا ويشـكل نقطـة لاسـتلام و توزيـع البريـد العابـر للحـدود والـذي بـدوره يمكـن أن يصـل مـن وإلى أي مـكان على سـطح الكـرة الأرضيـة.

يقوم مزوّد الخدمة بذلك عن طريق الخطوات التالية:

- يوصلك بالشبكة المحلية من خلال الشبكات السلكية أو اللاسلكية.
- يحدد لك عنوان IP حتى تتمكن من التواصل عبر الشبكة.
- يقـوم بإرسـال جميـع المعلومـات المطلـوب إرسـالها عـبر الشـبكة عـبر الطريـق الأسرع.

وإذا كانـت الوِجهـة خـارج الشـبكة المحليـة، يقـوم بتحويـل البيانـات للدولـة الأخـرى حيـث يسـلمها مـزوّد خدمـة الانترنـت للجهـاز المُتلقي ويقـوم بتحويلها إليـه.

فعالية 1: كيف يعمل الانترنت

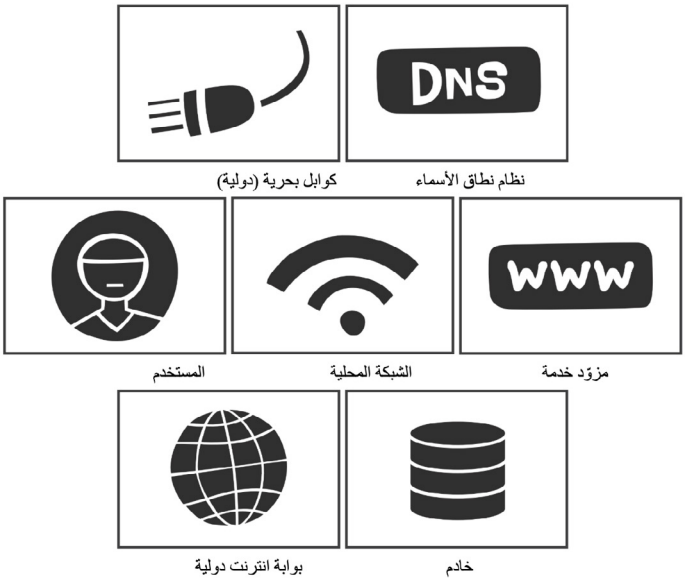
المحتوى: يسأل المدرب الطلبة هل فكروا مرة كيف يعمل الإنترنت؟ ثم يُقسّم الطلاب إلى 3 مجموعات وتوّزع عليهم البطاقات المُرفقة في ورقة العمل، ويطلب منهم أن يبنوا شبكة الإنترنت من هذه البطاقات. بحيث يقوم (شخص، مثلا مصطفى) بفتح اليوتيوب على جهازه، مع اعتبار أنه يوجد خادم لنظام نطاق الأسماء في نفس الدولة، وخادم يوتيوب الأقرب على مصطفى يقع في ألمانيا.

هدف التعلم: تعريف الطلبة بكيفية عمل الانترنت وكيف تُبنى الشبكة.

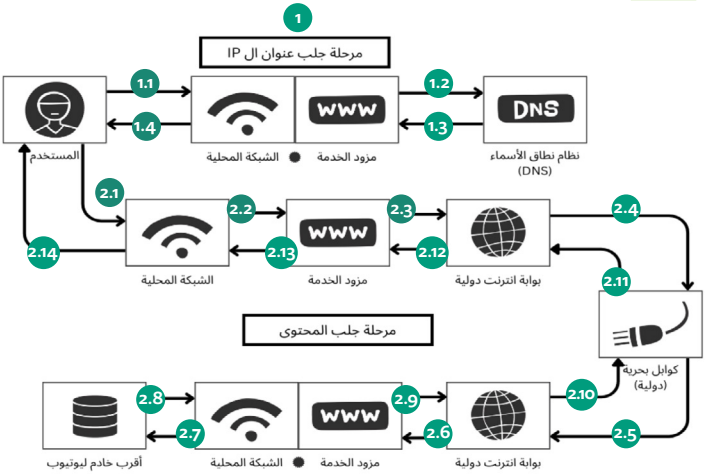
الطريقة: مسابقة

الأدوات اللازمة: أوراق عمل

الملاحظات: يحرص المدرب على طباعة أوراق العمل بحسب عدد المجموعات. على المدرب أن يصحح الأخطاء عند العرض على الفور (مرفق رسم توضيحي للمدرب حول بناء الشبكة).



الحـل



* يتم التنقل عبر الشبكة المحلية وفق تعليمات مزود الخدمة حيث يقوم بتحديد الطريق الأسرع لتبادل البيانات والذي يمكن أن يتغير خلال اليوم حسب الازدحام على الشبكة.

** توجد عدة طرق لرسم الشبكة رسمًا سليمًا، إذ قد تختلف طريقة تعبير الطالب عن بعض الخطوات أو أسلوب عرضه لها. الحل المُقترح ليس إلا أحد الحلول الصحيحة.

البيانات والمخاطر الرقمية

1. ما هي البيانات وتصنيفاتها؟

البيانات هي أي نوع من المعلومات يمكن تخزينه أو مشاركته، كالأسماء، الصور، الرسائل، المواقع، أو الملفات. يتعامل الأطفال مع البيانات طوال الوقت، سواء عند إرسال رسالة، حفظ صورة، أو تسجيل الدخول إلى لعبة من دون أن يعوا ذلك.

يمكن تصنيف البيانات على نحوين. أولًا، من حيث التخزين، وقد يأخذ أحد شكلين رئيسيين: البيانات المحلية، المخزّنة على الجهاز نفسه، مثل الصور المحفوظة بالهاتف أو المستندات بالحاسوب؛ والبيانات السحابية، المخزّنة عبر الإنترنت في خوادم مملوكة لشركات معيّنة كالملفات المحفوظة في خدمة Drive Google أو الرسائل الإلكترونية على منصات التواصل الاجتماعي (Facebook, Whatsapp, Tiktok).

النحو الثاني لتقسيم البيانات يُعنى بالنوعية؛ ويمكن تقسيمه إلى 3 أنواع: البيانات التعريفية (PII)، وهي البيانات التي يمكن أن تعرّف عن صاحبها بشكل مباشر (الاسم، العمر، الجنس، الخ..)؛ البيانات الحساسة، وهي البيانات التي لا يرغب أصحابها بأن تصبح معروفة على الملأ، وهو تصنيف يعتمد على أصحاب المعلومات ذاتهم، فيمكنهم إدراج

أي معلومة تحت هذه الجُزئية (قد تشمل معلومات كالآراء، الأشياء المفضلة، حجم الثروة الشخصية، إلخ..) مهما بدت المعلومات ساذجة بنظر الآخرين؛ البيانات العامة، وهي المعلومات التي لا يكترث أصحابها لهُوية من يعرفها (المنشورات العامة على منصات التواصل الاجتماعي، الاسم المستعار في الألعاب، إلخ..).

من شأن فهم الفوارق بين هذه الأنواع والتصنيفات أن يساعد الطلاب على إدارة بياناتهم بشكل أكثر أمانًا ومنهجية، وتصنيف البيانات بشكل مسبق يجنبهم التفكير في هذا الموضوع واتخاذ القرارات إزاءه بسرعة.

2. الخصوصية على الإنترنت وحماية البيانات

عند مشاركة المعلومات على الإنترنت، حتى أبسط الإجراءات مثل "إعجاب" أو "بحث" يمكن أن تترك أثرًا رقميًا. يطلق على هذا الأثر اسم "البصمة الرقمية". لا تقتصر البصمة الرقمية على مُجرد الاعجاب أو البحث عن شيء ما على الشبكة، بل تمتد لتطال كل ما يتركه المستخدم من أثر أثناء استخدامه للإنترنت، سواء كان منشورًا، تعليقًا، صورة، تصفح الصفحات المتنوّعة والتنقلّ بين المواقع، تصفّح التطبيقات المختلفة وشبكات التواصل الاجتماعي، أو حتى سجّل البحث في مواقع مثل جوجل مثلًا؛ حتى لو تم حذف بعض هذه الأشياء، قد تبقى موجودة على خوادم المواقع أو التطبيقات، وحتى قد تكون محفوظة من قبل أشخاص آخرين.

تقوم معظم التطبيقات والمواقع بجمع بيانات المستخدمين لتقديم خدمات أفضل، أو لغرض تقديم منشورات مُشخصنة، أو بغية عرض إعلانات مُشخصنة. أحيانًا تقوم بجمع هذه البيانات بهدف بيعها لطرف ثالث وجني الربح على حساب المستخدم؛ وعليه، يتوجب على المستخدمين تقليص هذه البصمة قدر الإمكان لتجنب انتشار معلوماتهم الحساسة والشخصية.

من أهم الطرق التي تُستخدم لتتبع المستخدمين هي ملفات تعريف الارتباط والتي تُعرف باسم الكُعيكات أو الكوكيز (Cookies)، وهي ملفات صغيرة تراقب ما يفعله المستخدم على المواقع. من بالغ الأهمية توعية الطلاب على أهمية التفكير قبل مشاركة أي معلومة شخصية في المواقع والتطبيقات، وتشجيعهم على التحقق من إعدادات الخصوصية وتجنّب الضغط على "أوافق على الكل" دون قراءة الطلب والتحقق من الجهات المستفيدة وتعطيل قدر ما أمكن منها.

يمكن تعديد بعض الممارسات الآمنة الأخرى لتعزيز الخصوصية لدى الطلاب مثل:

- استخدام أسماء مستعارة على المنصات الرقمية التي تتضمن التواصل مع الغرباء مثل ألعاب الفيديو الجماعية (Multiplayer).
- عدم نشر أي من المعلومات الشخصية على أي منصة تضم غرباء مثل:
  - الموقع الجغرافي الحي
  - العمر
  - الجنس
  - مكان الإقامة
  - موقع المدرسة
  - الهوايات
  - الأماكن التي يرتادها الطلاب بشكل متكرر (النادي الرياضي، المقاهي الالكترونية، مراكز التسوق، إلخ..)
  - يمكن حث الطلاب على تعديد معلومات شخصية أخرى
- القيام بالإبلاغ عن أي مستخدم يتطرق لمواضيع شخصية أو لا أخلاقية.
- إستخدام المتصفح الخفي عند استخدام الأجهزة العامة.
- ضبط إعدادات الخصوصية على منصات التواصل الاجتماعي.
- عليك أن تعي أن كل ما ينشر على الانترنت قد يبقى هناك إلى الأبد فتوخّى الحذر بالنسبة لما تقوم بنشره.

3. التصفح الآمن

إستخدام متصفح آمن يساعد المستخدمين على الحفاظ على خصوصيتهم، **فبدلا من استخدام متصفحات Google Chrome, Microsoft Edge ,Opera يمكن استخدام متصفح Brave الأكثر أمنًا**، إذ أنه قبل كل شيء متصفّح مفتوح المصدر على عكس الثلاثة السابق ذكرهم، كما أنه لا يقوم بجمع بيانات عن المستخدمين.

يمكن كذلك تثبيت **إضافات تعزز الخصوصية بشكل أكبر مثل: Privacy Badger ,UBlock Origin, Cookie AutoDelete**.

يمكن العثور على جميع هذه الإضافات على متاجر الإضافات الموجودة على المتصفحات مثل ChromeWebStore في حالة استخدام Brave، أو Firefox Browser Add-Ons.

4. التعرّف على التصيّد الاحتيالي

يستخدم المحتالون رسائل مزيّفة لخداع الناس بهدف سرقة معلوماتهم الشخصية. قد يتظاهرون بأنهم جهة رسمية مثل مصرف، أو وكالة دولية، أو صديق، أو حتى لعبة محبوبة. وغالبًا ما تتضمن هذه الرسائل وعودًا بجوائز أو طلبات عاجلة.

بعض الاشارات التي قد تدل على محاولة تصيّد احتيالية: **وجود أخطاء إملائية، روابط غريبة، احتواء الرسالة على محتوى عاجل يحث المستخدم على التصرّف مباشرة، أو طلبات للحصول على كلمات مرور أو بيانات حساسة؛ علمًا أن الخدمات الرقمية لا تطلب كلمات المرور بشكل مباشر أبدًا**. من المهم تدريب الطلاب على تجاهل هذه الرسائل، عدم التفاعل معها، وإبلاغ شخص موثوق وبالغ (إما الأهل أو المرشد التربوي في حال القاصرين) عند ظهور مخاوف أو الشك بمصدر الرسالة وطابعها.

5. التنمّر الإلكتروني وطرق الوقاية

يأخذ التنمّر الإلكتروني أشكالًا متعددة، مثل **إرسال رسائل مؤذية، استبعاد شخص من المجموعات، أو نشر شائعات عنه. يمكن أن يحدث هذا عبر الرسائل، الألعاب، أو وسائل وشبكات التواصل الاجتماعي**.

على المعلّمين تعزيز ثقافة الاحترام، وتشجيع الطلاب على عدم الرد على الرسائل المسيئة، حفظ الأدلة مثل لقطات الشاشة، والإبلاغ عن الحادثة للأهل أو الإرشاد أو الجهة المسؤولة في المنصة.

ينبغي تشجيع الطلاب على استخدام إعدادات الخصوصية، قبول الأصدقاء الذين يعرفونهم فقط، وعدم المشاركة في سلوكيات مؤذية تجاه الآخرين، والتحذير

من مشاركة المعلومات الشخصية على أية منصة علنية، لأن من المحتمل أن ينطوي عن هذا الفعل عواقب وخيمة قد تمتد إلى الواقع الملموس.

6. الألعاب والسلامة على الإنترنت

يُمضي الكثير من الأطفال وقتًا طويلًا في الألعاب الإلكترونية، والتي يمكن أن تتضمّن محادثات مع أشخاص لا يعرفونهم. بعض هؤلاء قد يحاول الحصول على معلومات شخصية أو إرسال روابط ضارة، وبسبب انكشاف الأطفال بشكل كبير جدًا على هذه البرمجيات، ارتأينا أن نخصص لها فصلًا كاملًا. كما ويعتبر هذا الفصل من أكثر الأقسام التي يستطيع الطلبة المشاركة فيها فيفضل حثهم على المشاركة به قدر الإمكان.

يجب توعية الطلاب على **عدم مشاركة أسماءهم الحقيقية، مواقع تواجدهم، مكان إقامتهم، أو صورهم أثناء اللعب. كما ينبغي حثّهم على اعتماد إعدادات الخصوصية، وعدم الضغط على روابط مشبوهة. يجب أيضًا تحذيرهم من تحميل ألعاب مقرصنة أو برامج من مصادر غير موثوقة، لأنها قد تحتوي على برمجيات خبيثة.**

يُعتبر موضوع البرامج المقرصنة وخصوصاً الألعاب منها، موضوعًا بالغ الأهمية لهذه الشريحة؛ حيث إنه يشكل النافذة الأكبر للبرمجيات الخبيثة للولوج إلى والتموضع في أجهزتهم، على خلفية كون هذه الألعاب مجانية مما يشكل إغراءً كبيرًا جدًا للأطفال؛ وبمجرد تحميل هذه البرامج، تكون كافة الاحتمالات واردة ويمكن إخفاء أو غرس البرمجيات الخبيثة بشتى أنواعها داخل هذه الألعاب (سيتم مناقشة البرمجيات الخبيثة على اختلاف أشكالها وأنواعها بالفصل التالي).

كما ويمكن أن تؤدي منصات الألعاب الجماعية لجميع ما ذكر آنفًا من احتيال وتسريب للمعلومات الشخصية والحساسة والتنمّر الرقميّ. لذا يجب تشجيع الطلاب على توخي الحيطة والحذر عند النشاط في هذه المنصات. كما يجب تشجيعهم على التواصل مع الأهل أو طلب الارشاد في المدرسة عند التعرض أو الشك بالتعرض لأي نوع من الانتهاكات الرقمية مهما كانت تبدو ساذجة بنظرهم.

فعالية 2: الممارسات الرقمية

المحتوى: يتم تقسيم الطلاب إلى مجموعات صغيرة وتُوزَّع على كل مجموعة بطاقات تحتوي على عادات استخدام الإنترنت (أو تُعرض على الشاشة/السبورة). يتوجب على كل مجموعة تصنيف العادات إلى آمنة وغير آمنة مع تقديم مبرراتهم. ثم وبعد تصنيف جميع العادات، يتم مناقشتها بشكل جماعي مع توضيح سبب كونها آمنة أو غير آمنة. يمكن إضافة عنصر المنافسة عبر منح نقاط للإجابات الصحيحة.

هدف التعلم: تعليم الطلاب كيفية التعرّف على العادات الرقمية الآمنة وغير الآمنة.

الطريقة: مسابقة في حال إعطاء جميع المجموعات نفس البطاقات، أو نشاط جماعي بدون مجموعات.

الأدوات اللازمة: بطاقات تحتوي على ممارسات رقمية بعضها آمن وبعضها غير آمن.

الملاحظات: يمكن تكرار هذه الفعالية في كل مرحلة عمرية مع استخدام الممارسات الجديدة التي قام الطلاب بتعلمها كنوع من المراجعة، ويمكن استخدام ذات الفكرة لتصنيف الأشخاص كموثوقين وغير موثوقين (الأهل، الأصدقاء، المعارف عبر الانترنت، إلخ..) وتصنيف البيانات الحساسة والخاصة والعامة.

غيـر آمن

إستخدام نفس كلمة المرور لعدة حسابات.

النقر على الروابط في رسائل البريد الإلكتروني المشبوهة أو الرسائل العشوائية أو البريد غير الهام (Spam Email, Junk Mail).

تحميل تطبيقات أو ملفات من مصادر غير موثوقة أو غير رسمية.

مشاركة المعلومات الشخصية (العنوان، رقم الهاتف، المدرسة، العادات) علنًا وعلى الملأ.

قبول طلبات الصداقة من الغرباء وتجاهل إعدادات الخصوصية.

تجاهل تحديثات البرامج.

إستخدام كلمات مرور ضعيفة مثل "123456" أو "password".

نشر الصور الشخصية دون التفكير في مخاطر الخصوصية.

الاتصال بشبكات الانترنت اللاسلكي (واي فاي) العامة دون إجراءات حماية إضافية.

آمــن

إستخدام كلمات مرور قوية ومختلفة لكل حساب.

التفكير قبل النقر على الروابط أو تحميل الملفات.

تحميل التطبيقات من المصادر الرسمية.

التحقق من عناوين المواقع الإلكترونية وصفحات التواصل الاجتماعي
قبل إدخال المعلومات الشخصية.

ضبط إعدادات الخصوصية على وسائل وشبكات التواصل الاجتماعي.

تحديث البرامج والتطبيقات بانتظام.

تفعيل المصادقة الثنائية (2FA).

إستشارة شخص بالغ قبل مشاركة المعلومات الشخصية
(للأطفال الأصغر سنًا).

تسجيل الخروج من الحسابات عند استخدام
أجهزة مشتركة.

فعالية 3: التعرف على التصيّد الاحتيالي

المحتوى: يتم تقسيم الطلاب إلى مجموعات صغيرة وتُوزَّع على كل مجموعة بطاقات أو أوراق تحتوي على أمثلة لرسائل احتيالية وأخرى حقيقية، يطلب من كل مجموعة فرز هذه الرسائل وتدوين الملاحظات التي ساعدتهم وواجهتهم عند فرزها.

هدف التعلم: تعليم الطلاب كيفية التمييز بين الرسائل الاحتيالية والآمنة.

الطريقة: مسابقة إذا تم إعطاء نقاط لكل رسالة مفرزة بشكل صحيح، أو نشاط جماعي.

الأدوات اللازمة: أوراق أو بطاقات تحتوي على نماذج لرسائل بعضها احتيالي.

الملاحظات: سيتم ادراج بعض الأمثلة على رسائل احتيالية، ولكن يحق للمعلم إدراج المزيد.

الرسالة:

المرسِل: apple-rewards@gmail.com

الموضوع: تهانينا! لقد ربحت هاتف آيفون جديد

مرحبًا [اسم الشخص]،

نودّ إعلامك بأنك أحد الفائزين المحظوظين في سحبنا السنوي!

لقد ربحت هاتف iPhone 16 pro max جديد! لاستلام جائزتك، **الرجاء**

الضغط على الرابط أدناه وتعبئة بياناتك الشخصية:
https://claim-your-prize-now.vip

يُرجى تعبئة النموذج خلال 24 ساعة فقط لتأكيد استلام الجائزة.

إذا لم تقم بذلك، سيتم اختيار فائز آخر.

فريق دعم آبل

الأسباب:

- **البريد الالكتروني المستخدم لا يعود لشركة آبل (سيتم التعرف على طريقة التحقق لاحقًا).**
- **الرابط غريب وغير تابع لآبل.**
- **تُوّظف الرسالة أسلوب الإلحاح (24 ساعة فقط).**
- **ستخدام الرموز التعبيرية في رسالة رسمية لجذب الانتباه.**

الرسالة:

المرسِل: support@bool.com

الموضوع: تحذير: حسابك البنكي مهدد بالإغلاق!

عميلنا العزيز،

لاحظنا نشاطًا غير معتاد في حسابك، وقد تم إيقافه مؤقتًا للحماية.

لإعادة تفعيل الحساب، الرجاء الدخول فورًا إلى الرابط التالي وتأكيد معلوماتك:
https://secure-update-bank-login.com
إذا لم يتم التحديث خلال 12 ساعة، سيتم إغلاق حسابك نهائيًا.

نحن نهتم بأمانك.

قسم الأمن – بنك الحياة

الأسباب:

- **تُوّظف الرسالة أسلوب الإلحاح والتخويف.**
- **الرابط غريب وغير تابع للمصرف.**
- **الرسالة تطلب منك معلومات حساسة لا تقوم المؤسسات الرسمية بطلبها من المستخدمين أبدًا.**
- **يبدو عنوان البريد الالكتروني المُستخدم ذا طابع رسميّ، لكن bool لا تتبع لمصرف اسمه بنك الحياة.**

الرسالة:

مرحبًا،

آسف على الإزعاج، لكني في موقف طارئ الآن ولا أستطيع الوصول إلى هاتفي.

هل يمكنك شراء بطاقة شحن أو بطاقة هدايا Apple بقيمة 100 شيكل وارسال الكود هنا؟ سأعوضك غدًا.

رجاءً لا تخبر أحد، الموضوع محرج جدًا.

أعدك أني سأشرح كل شيء لاحقًا.

شكراً كثيرًا!

الأسباب:

- **تستغل الرسالة العاطفة وخصوصًا علاقات الصداقة.**
- **إسم المُرسِل غير مذكور.**
- **الرسالة تطلب مبلغ مادي بطريقة ملّحة وسرّية.**
- **ملاحظة: حتى إذا أتت الرسالة من حساب أحد الاصدقاء، تحقق دائمًا من مصدرها عن طريق محادثة صوتية.**

فعالية 4: نصائح للّاعبين الجدد

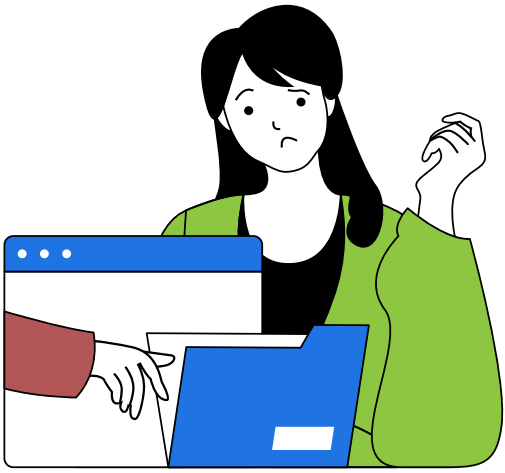
المحتـوى: يتـم تقسـيم الـطلاب إلى مجموعـات صـغيرة ثـم يقـوم المعلـم بطلـب 3 نصائـح هامـة للأطفـال الذيـن ينـوون البـدء باللعـب الجماعـي عبر الانترنـت. لاحقًا بالإمـكان إنتـاج قائمـة أو لوحـة بسـيطة بأهـم هـذه النصائـح وتعليقهـا في الصـف أو في باحـات المدرسـة لمشـاركة هـذه المعلومـات مـع بقيـة الـطلاب.

هـدف التعلـم: ترسـيخ الممارسـات الآمنـة للعـب الجماعـي عبر الانترنـت في عقـول الطلبـة ونشر المعرفـة مـع بـاقي الطلبـة.

الطريقة: نشاط جماعي.

الأدوات اللازمة: أوراق فارغة ليكتب الطلاب أهم 3 ممارسات من وجهة نظرهم.

الملاحظـات: تـم إدراج بعـض الأمثلـة في نقطـة 2 ولكـن بوسـع الطلبـة أن يذكـروا نقاطًا إضافيـة وقـد تكـون الفعاليـة مشتركـة مـع فعاليـة 1.



حماية الأجهزة والحسابات

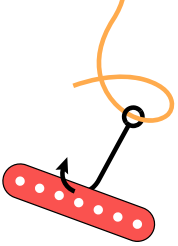
1. مقدمة

هـذه المواضيـع مـن أهـم المواضيـع التي يجـب على الـطلاب فهمهـا، وبالرغـم مـن كـون موضوعـا تـأمين الأجهـزة والحسـابات منفصلـين إلا أننـا قررنـا جمعهمـا في فصـل مُشترك إذ أن العديـد مـن القواسـم المشتركـة تجمـع بينهمـا.

يفضـل البـدء بهـذا الفصـل مـع الـطلاب مـن الصـف الثامـن أو التاسـع فمـا فـوق لأنـه يحتـوي على معلومـات أكثر تعقيـدًا مـن الفصـول السـابقة.

2. كلمات المرور

يُعـد اسـتخدام كلمـة مـرور قويـة وفريـدة حجـر الأسـاس بالنسبة لأمان الأجهزة والحسابات، بمعنى أن تتكون كلمة السر من **12 خانة على الأقل وتحتوي على حروف لاتينية** (إنجليزية) كبيرة وصغيرة وأرقام ورموز. كما يجب ألا تحتوي كلمة المرور



على أية معلومات شخصية (الاسم، العمر، تاريخ الميلاد) لتجنب احتمال تخمينها من قبل المهاجمين. وأخيرًا يمنع استخدام كلمة المرور ذاتها لأكثر من حساب أو جهاز بنفس الوقت، للحد من الخسائر في حال تم تسريب إحداها.

قد تبدو الشروط المذكورة أعلاه تعجيزية، إذ أنه من الصعب على أي شخص تذكر 15 كلمة مرور ليس لها علاقة بالشخص نفسه وتحتوي على رموز وأرقام وحروف قد تكون مختلفة ومتنوّعة، لذلك يفضل استخدام برامج إدارة كلمات المرور.

مدير كلمات المرور هو برنامج يقوم بحفظ كلمات المرور بالنيابة عنا بطريقة آمنة ومشفرة تسمح لنا بالولوج إليها، وتكون هذه القائمة مؤمنة بكلمة سر كحدٍ أدنى. بهذه الطريقة يُحصر دور المستخدم بحفظ كلمة مرور واحدة، التي بدورها ستمكنه من الوصول إلى بقية كلمات المرور التي يستخدمها.

يجدر التنويه بالنسبة لهذا الموضوع أن مدير كلمات المرور المُدمج بالمُتصفّح يُعتبر خيارًا غير جيد، بل ويُنصح بتعطيله لأن إجراءات الحماية على هذه البرمجيات غالبًا ما تكون أضعف من البرامج المتخصصة بهذه المهمة. كما أنها بالغالب لا تطلب من المستخدم كلمة مرور للحصول على القائمة وبذلك بإمكان أي شخص نجح بالوصول لجهازنا وهو غير مقفول أن يدخل على هذه القائمة ويستخرج منها أية كلمة مرور تروق له. خير مثال على برامج إدارة كلمات المرور المستقلة والمجانية سهلة الاستخدام، مفتوحة المصدر، والتي يمكن إضافتها لاحقًا إلى المُتصفّح بطريقة آمنة (Bitwarden).

3. إجراءات حماية إضافية للحسابات

يمكن تأمين الحسابات بإجراءات أخرى إضافة لكلمات المرور، بعضها يزيد من الأمان بشكل ملحوظ، ويفضل عدم تفعيل البعض الآخر لأنها تشكل عبئًا مُضافًا خاليًا من المنافع الفعلية، بل وقد تكون ضارة في بعض الأحيان.

أول هذه الإجراءات، خاصية التوثيق **الثنائي (2FA)**، والتي تعمل عن طريق إرسال رمز لجهة مُحددة مُسبقًا للحد من الدخول غير المُصرّح به. يمكن تفعيل هذه الخاصية بعدة أنماط؛

- **أولها** عن طريق البريد الإلكتروني، وتعتبر هذه الطريقة سيئة وغير مجدية إذ أنها تتيح لأي شخص ذي إمكانية الوصول إلى بريدك الإلكتروني الولوج إلى حسابك، كما أن بروتوكولات نقل البريد الإلكتروني تُعتبر بدائية مقارنة بالطرق الأكثر حداثة؛ وأخيرًا تتطلب هذه الطريقة اتصالاً بالانترنت لتعمل.
- **الطريقة الثانية** لعمل FA2، عن طريق الرسائل النصية القصيرة (SMS)، تعتبر هذه الوسيلة سيئة كذلك تقريبًا للأسباب ذاتها المذكورة أعلاه؛ إذ أن بروتوكول نقل الرسائل النصية القصيرة يُعتبر بدائيًا ويمكن اعتراض محتواه بسهولة كبيرة جدًا لكونه غير مشفر (سيُناقَش مفهوم التشفير لاحقا)؛ كما أنه يتطلب الاتصال بشبكة الخليوي بهدف الحصول على الرمز.
- أخيرًا، **الطريقة الثالثة** والتي تعتبر أفضل الطرق وأكثرها أمانًا، استخدام تطبيقات مستقلة غرضها الوحيد هو القيام بتزويدك بهذه الرموز؛ فهذه التطبيقات لا تتطلب اتصالًا بالانترنت أو بشبكة الخليوي ويكون محتواها مُشفرًا ويمكن حد الوصول إليها عن طريق البصمات البيومترية أو كلمات المرور للتأكد من حد الوصول غير المُصرّح به. يتيح هذا الإجراء للمستخدمين إصدار مجموعة من الأرقام الاحتياطية التي يمكن استخدامها لتعطيل هذا الإجراء في حال ضياع أو سرقة الهاتف الذي يحتوي على التطبيق، من أفضل هذه التطبيقات Free OTP ,OTP Auth.

مفاتيح الأمان (Security Keys)، وتكون عبارة عن أداة ملموسة صغيرة تشبه وحدات التخزين (الفلاش) يمكنها السماح لحاملها بالدخول للحساب، تقوم هذه الأداة فعليًا بنقل وسط الدفاع من الوسط الرقمي المعقد إلى الوسط الملموس البسيط؛ حيث يمكن لأغلب الأشخاص أن يقوموا بحماية هذه الأداة بسهولة على عكس الوسط الرقمي الذي قد يبدو مُربكًا للوهلة الأولى.

مفاتيح الولوج (Passkeys)، يُمّكن هذا الإجراء المستخدمين من الولوج إلى حساباتهم وأجهزتهم عن طريق عدة أساليب، مثل الرموز القصيرة (PIN)، أو البصمات الإلكترونية

(بصمة الاصبع، بصمة ملامح الوجه، إلخ..)؛ ومع أن هذه الأساليب تُسهل عملية تسجيل الدخول بشكل ملحوظ، إلا أنه يمكن اجتيازها وتخطي العقبات الأمنية؛ فعلى سبيل المثال، يستطيع أحدهم أن يضع الهاتف أمام وجه المستخدم، أو يمكن إرغام المستخدم على فتح حساباته بسهولة كبيرة. لذا، من المفضل تعطيل هذا الإجراء.

الطلبات (Prompts)، حيث يقوم مزوّد الخدمة بإرسال طلب لتأكيد عملية تسجيل الدخول إلى هاتف آخر موثوق. من غير المُفضل استخدام هذه الخاصية؛ لأنه يمكن استغلالها في حال ضياع الجهاز، أو سرقته، أو بيعه، إلخ..

4. التشفير

يمكن تعريف التشفير على أنه عملية تحويل المعلومات من شكلٍ قابل للقراءة إلى شكلٍ غير مفهوم، بحيث لا يمكن لأي شخص كان قراءتها، فهمها، أو استخدامها. وفقط من يملك "المفتاح" لفك التشفير وإعادة صياغة الرموز يمكنه قراءتها وفهمها. على سبيل المثال، يتم تحويل كلمة "مرحبًا" إلى "k#dSg32" ثم إعادتها لما كانت عليه باستخدام المفتاح.

من الصعب شرح مبادئ التشفير الحديثة لطلاب المدرسة، بالتالي، من المُفضل استخدام طرق التشفير البدائية مثل تشفير قيصر ليفهموا الآلية المذكورة أعلاه. لكن المهم هو طرح مفهوم التشفير كأداة أساسية لحماية البيانات، سواء في مرحلة نقلها عن طريق استخدام VPN للحفاظ على الخصوصية بشكل أكبر، أو تخزينها عن طريق تشفير الملفات التي تحتوي هذه البيانات.

بادئ ذي بدء، لنتطرق إلى التشفير في عملية التواصل. يُفضل استخدام برامج دردشة تدعم التشفير بين طرفين (Encryption End to End)، وهو ضرب من التعمية لا يمكن بموجبها إلا لأطراف الاتصال قراءة الرسائل المرسلة، أي أن الاتصالات تظل معمَّاة بين طرفي الاتصال أثناء تبادل الرسائل ولا يستطيع أحد، حتى الشركة التي تقوم بتشغيل الخدمة، الاطلاع على الرسائل سواء أثناء النقل أو التخزين؛ ومن أفضل الأمثلة على هذه التطبيقات تطبيق Signal.

ثم، يمكن أن نتطرق لأهمية تشفير

البيانات أثناء النقل عن طريق التأكد من أن الرابط يبدأ بـ https وليس http لأن ذلك يدل على أن عملية النقل تتم بطريقة مُشفّرة. كما يمكن استخدام الشبكات الخاصة الافتراضية (VPN)، التي تقوم بدورها بتشفير كافة البيانات الصادرة عن جهاز المستخدم أثناء مرحلة النقل، وتمنع أية جهة متطفلة من الاطلاع على هذه البيانات (يمكن مراجعة الفعالية الأولى في الفصل الأول للاطلاع على من يمكنه الاطلاع على البيانات أثناء مرحلة النقل). لكن لا بُد من التنويه أنه بمُستطاع الجهة المتطفلة مشاهدة أن المستخدم يقوم باستخدام VPN فقط، من دون معرفة أو كشف ماهية البيانات الجاري نقلها. كما يجب التنويه أن مزوّد خدمة الـ VPN هو الجهة الوحيدة التي يمكنها الاطلاع على الوجهة الحقيقية للبيانات؛ لذلك يجب اختيار مزوّد خدمة موثوق ومعروف بسياسات عدم تخزين بيانات المستخدمين؛ من أفضل هؤلاء المزوّدين ProtonVPN.

وأخيرًا، سنتحدث عن تشفير البيانات أثناء عملية التخزين، وذلك عن طريق تشفير وحدة التخزين ذاتها، على أن تُحجب إمكانية الوصول إلى محتويات الجهاز من دون إدخال كلمة سر خاصة لفك التشفير (زيادة على كلمة السر الخاصة بالجهاز)؛ يمكن استخدام برنامج VeraCrypt لهذا الغرض. يمكن كذلك إنشاء ملف واحد (خزنة) بحيث يكون هو وحده المُشفّر بدلًا من تشفير وحدة التخزين بشكل كليّ، ويمكن استخدام CryptoMator لهذا الغرض.

5. البرمجيات الخبيثة (Malicious Software - Malware)

يمكن تعريف البرمجيات الخبيثة على أنها كل برمجية تقوم بخدمة هدف خبيث، وتأتي هذه البرمجيات في أشكال عدة ولها وظائف كثيرة ومتنوعة، سنتطرق لأشهرها ولكيفية إصابة الأجهزة بها عادة، ولأفضل الممارسات للحد من التعرض لها.

من أشهر هذه البرمجيات:

الفيروسات: هي برمجيات خبيثة بمجرد ما أن تدخل على جهاز الكومبيوتر (الحاسوب) تبدأ بنسخ نفسها لتصل إلى أكبر كم من البرامج النظيفة لتستقر فيها، فتصنَف هذه البرامج كبرامج مصابة بالعدوى (infected).

الديدان: تشبه الفيروسات، لكنها تنسخ نفسها لتصيب الأجهزة الأخرى على الشبكة.

برمجيات التجسس: هي برمجيات تقوم بجمع أكبر كم ممكن من البيانات مع الإبقاء على سِريّة وجودها على الجهاز قدر المستطاع.

البرمجيات المموّهة (حصان طروادة): هي برمجيات تبدو نظيفة ومُفيدة في ظاهرها، ولكنها خبيثة في طابعها الخفيّ، نحصي منها على سبيل المثال لا الحصر، برنامج تعديل فيديوهات يقوم بدور برمجية تجسس في الخلفية. غالبًا ما تكون إصدارات مقرصنة من برامج معروفة.

برامج الفدية: هي برامج تشفير الملفات مقابل ابتزاز مالي.

مسجل لوحة المفاتيح (keylogger): هو عبارة عن برنامج يقوم بتسجيل كل ضغطة زر يقوم بها المستخدم، لمشاركتها فيما بعد مع الجهات المُنتهِكة.

يمكن تلخيص غايات البرمجيات الخبيثة بعدة نقاط:

- من المحتمل أن تكون الغاية هي الاستيلاء على موارد الجهاز ثم استخدامها لمهاجمة أجهزة أخرى.
- قد تكون الغاية هي التسبب بتعطيل مؤقت أو دائم للأجهزة.
- من الوارد أن تكون الغاية هي الاستيلاء على البيانات الشخصية أو الحساسة ثم نقلها لوحدة تخزين مركزية.
- تتضمن البرمجيات الخبيثة في مُعظم الحالات، ما يُسمى بعامل التحكم عن بعد (RAT) و الذي يكون عادة متصل بوحدة تحكم مركزية (C2). ويمكن أن تكون البرمجية عبارة عن برمجية مركبة؛ كأن تكون مثلًا دودة وبرمجية تجسس في الآن ذاته، وبالتالي، يقوم البرنامج باستنساخ نفسه ومحاولة إعداء أكبر كمّ من الأجهزة مع مواصلة التجسس

عليها كلها في آن واحد ليرسل النتائج إلى وحدة التحكم المركزية والتي تكون بالعادة تابعة للجهة المُهاجمة.

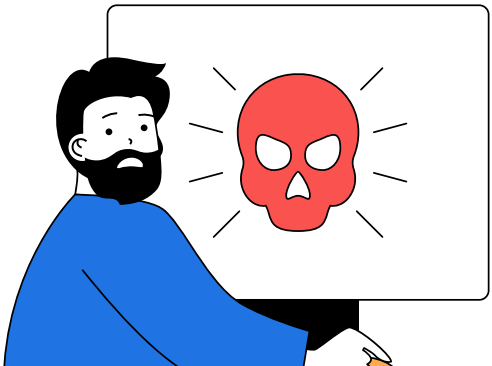
من أكثر الطرق استخدامًا لنشر هذه البرمجيات:

- **البرامج المُقرصنة** التي سبق وتطرقنا إليها آنفًا، وبالنسبة للطلاب تُعدّ الألعاب المُقرصنة المُسبب الأكبر لنقل البرمجيات الخبيثة في صفوفهم.
- **النقر على الروابط المشبوهة والملغومة** التي تحتويها بعض الرسائل والتي جئنا على ذكرها سابقًا، وسنتطرق لكيفية التعامل معها في هذا الفصل.
- **إستخدام وحدات التخزين** (Hard Disk, USB Flash Drive, CD, إلخ..) المُستحصلة من أشخاص آخرين، الغرباء أو المجهولين منهم بالذات. حيث أنه لا حدود للاحتمالات عند الحديث عن هذه الوحدات، لأنها قد تحتوي على أي نوع من البرمجيات أو الملفات المَعدية أو المُعدية.

للوقاية من هذه البرمجيات هناك عدة أساليب قد تختلف باختلاف

نوع التهديد:

- بالنسبة للروابط المشبوهة؛ يمكن **فحصها على موقع VirusTotal**، والذي بدوره سيقوم بإخبار المستخدم إذا كان قد تم الإبلاغ عن الرابط من قبل أي مؤسسة أمان رقميّ مرموقة، ويفضل عدم تفحّص أو النقر على هذه الروابط بأي حال من الأحوال، باستثناء الحالات الضرورية أو عند الوثوق بالمستخدم تمامًا. كما يمكن فحص مُلكية الرابط أو مُرسله، أي، لمن يعود الرابط، عن طريق محركات بحث WhoIs.



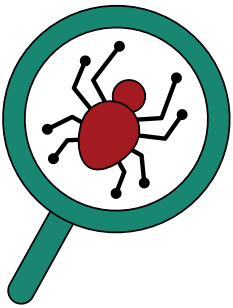
- **عدم تحميل أي برنامج أو لعبة إلا إذا كانت من المصدر الرسمي**، والابتعاد كل البُعد عن البرامج المُقرصنة.
- **إبقاء جميع البرامج وبالأخص أنظمة التشغيل على آخر تحديث**. خصوصًا أن التحديثات عادة ما تشمل أحدث التصحيحات للثغرات الأمنية المكتشفة حديثًا.
- **إستخدام برامج حماية من شركات مرموقة ومعروفة**؛ لأن هذه الشركات تتمتع بالعادة بأحدث الطرق والوسائل لمكافحة هذه البرمجيات الخبيثة على أجهزة المستخدمين، على عكس برامج الحماية الأساسية المُدمجة بنظام التشغيل. من أفضل هذه البرامج نوصي على ESET, Norton, Kaspersky, BitDefender.

6. البرامج مفتوحة المصدر

البرامج مفتوحة المصدر هي البرامج التي تعرض كل برمجياتها على الملأ، حيث يمكن لأي شخص كان أن يستطلع ويتفقد كيفية عمل هذه البرامج من الألف إلى الياء، مما يتيح للمستخدمين التأكد من كل تغيير على البرمجيات والتحقق من مدى أمن البرنامج، أو اذا كان قد فقد من موثوقيته ودرجة خصوصيته وأمانه.

يمكن تلخيص محاسن هذه البرامج بـ 4 نقاط:

- **الشفافية**: يستطيع الجميع مراجعة البرمجيات المضمونة، مما يقلل من احتمال وجود أدوات تجسس أو أبواب خلفية خفية .
- **التحكّم**: ليس المُستخدم ملزمًا بقبول شروط استخدام طويلة ومعقدة، وغالبًا ما لا يتم جمع بياناته.
- **التحديث السريع**: لأن المجتمع يشارك في التطوير، يتم اكتشاف الثغرات الأمنية وتصحيحها بسرعة.
- **الحرية**: يمكن استخدام هذه البرامج في أي مكان، وغالبًا ما تكون مجانية.



بعض البدائل للبرامج غير مفتوحة المصدر:

البديل مفتوح المصدر	البرنامج غير مفتوح المصدر
Brave	Google Chrome
Signal	Whatsapp / Facebook Messenger
Jitsi Meet	Zoom
Open Street Map / OsmAnd	Google Maps / Apple Maps / Waze
Libre Office	Microsoft Office

ملاحظات شاملة للفصل:

- يمكن عرض الكثير من المعلومات المكتوبة في هذا الفصل بشكل عملي أمام الطلاب لكي تثبت المعلومات لديهم، وفيما بعد يمكن إشراكهم في الفعاليات أدناه. مثل أن يعرض عليهم المعلم كيف يعمل Bitwarden ثم يضع كلمة المرور على موقع https://www.passwordmonster.com وعقب ذلك، يستطيع أن يطلب من الطلاب اختراع كلمات مرور جديدة لتجربتها ومقارنتها مع كلمة المرور التي كوّنها برنامج BitWarden.
- ستكون الفعاليات التالية شاملة للدليل بأسره، بهدف قياس مدى استفادة الطلاب منه، والتأكد من أنهم صاروا على أتم الاستعداد والجاهزية على صعيد الأمان الرقميّ.

فعالية 5: سباق الأمان

المحتوى: يتم تقسيم الطلاب إلى مجموعات صغيرة، ثم يطلب المعلم منهم القيام باختراع سيناريوهات لحسابات وهمية تتمتع بعدة خطوات للحماية. من ثم يصف المُعلم كيف يقوم المستخدمون بالوصول إليها وما هي إعدادات الخصوصية المُرفقة بها. في المرحلة التالية، يستعرض الطلاب الحسابات وخطوات الحماية، على أن تفوز المجموعة صاحبة الحساب الأكثر أمانًا. أو يستطيع المعلم اختراع هذه الحسابات الوهمية ثم يطلب من الطلاب التصويت على أي الحسابات والممارسات هي الأكثر أمانًا.

هدف التعلم: ترسيخ الممارسات الآمنة والإجراءات الأمنية اللازمة لتأمين الحسابات.

الطريقة: نشاط جماعيّ أو مسابقة.

الأدوات اللازمة: أوراق فارغة ليكتب الطلاب عليها السيناريو الخاص بهم.

فعالية 6: شيفرة قيصر

المحتوى: يقوم المعلم باقتراح شيفرة قيصر معيّنة؛ على سبيل المثال، إزاحة 3 لليمين، ثم يكتب جملة على السبورة (اللوح)، ويكون الفائز أول طالب أو طالبة ينجحون بفك الشيفرة. بعد ذلك يشرح المعلم أن الإزاحة بهذه الحالة شكلت المفتاح المُوظّف للتشفير و فك التشفير.

هدف التعلم: تطرح فهمًا بسيطًا لآلية عمل التشفير، مع العلم أنه لا يمكن مقارنة آليات التشفير الحديثة بهذه الطريقة، إلا أن من شأن بساطتها أن تساعد الطلاب على استيعاب وفهم مبدأ مفتاح التشفير (أي أنه عبارة عن المعلومة التي إذا أدخلتها في خوارزمية التشفير نفسها لكن بالمقلوب تقوم بفك التشفير).

الطريقة: مسابقة.

الأدوات اللازمة: أوراق فارغة ليكتب الطلاب النتيجة عليها.

فعالية 7: تصويب الأخطاء

المحتوى: يتم تقسيم الطلاب إلى مجموعات صغيرة، ثم يزوّدهم المعلم بأوراق عمل يوجد عليها عدة سيناريوهات تحتوي على ممارسات خاطئة. يقوم بعدها الطلاب بتحديد هذه الممارسات وتصحيحها، ليتبع ذلك نقاش مفتوح، حيث يناقش المعلم مع الطلبة إجابات كل مجموعة على كل سيناريو.

هدف التعلم: توفير مراجعة شاملة للمادة.

الطريقة: نشاط جماعي.

الأدوات اللازمة: أوراق عمل عليها مجموعة من السيناريوهات.

أمثلة على سيناريوهات:

- يوسف أراد تحميل لعبة مشهورة لكن مدفوعة. وجد نسخة "مجانية بالكامل" على موقع غير رسمي، وقام بتحميلها. بعدها بدأ جهازه يبطئ، وتظهر نوافذ منبثقة غريبة، وتطبيق غريب اسمه "updateHelper.exe" يعمل دائمًا في الخلفية.

الممارسة الخاطئة: قام بتحميل برنامج (لعبة) من مصدر غير رسمي، وغالبًا ما قد تحتوي هذه اللعبة برمجيات خبيثة تسيطر وتتحكم بموارد الجهاز.

الحلول والوقاية: عدم تحميل أي لعبة أو تطبيق إلّا من المصدر الرسمي.

إزالة التطبيق المشبوه فورًا، وإعادة فحص الجهاز بالكامل باستخدام برنامج حماية (Antivirus) موثوق للتأكد من عدم انتشار العدوى إلى تطبيقات أخرى.

- لينا حملت تطبيق تعديل صور من موقع مجهول بعد أن رأت إعلانًا جذّابًا على موقع إلكتروني. بعد تثبيته، بدأ التطبيق يطلب منها أن تضمن له صلاحيات كثيرة (الوصول للكاميرا، الميكروفون، الرسائل، والملفات)، رغم أنه تطبيق بسيط لتعديل الصور. في اليوم التالي، لاحظت رسائل غريبة تُرسل من حسابها على تيليغرام.

الممارسات الخاطئة: تحميل برنامج من موقع غير رسمي، ومنحه صلاحيات زائدة عن الحد اللازم

الحلول والوقاية:

- مسح التطبيق فورًا وتغيير كلمات مرور الحسابات التي حصل على إذن بوصولها.
- عدم تحميل أي لعبة أو تطبيق إلّا من المصدر الرسمي.
- عدم منح التطبيقات صلاحيات إلا عند الحاجة وبما يتناسب مع وظيفتها.

- نشرت تالا صورة جماعية على حسابها العام في إنستغرام. بعد فترة، لاحظت أن أحد أصدقائها كان منزعجًا لأن الصورة التُقطت دون إذنه، وطلب منها حذفها. حذفت تالا الصورة من حسابها، لكن بعد أيام وجدتها منشورة على حسابات غريبة وعلى موقع meme ساخر.

الممارسة الخاطئة: نشر محتوى سلبي دون التفكير بالعواقب والتبعات.

الحلول والوقاية:

- لا يوجد حل، إذ أن أي شيء يدخل الإنترنت فهو باقٍ هناك للأبد.
- طلب إذن الأشخاص قبل نشر صورهم.
- توعية الطلاب على أن الحذف لا يضمن بالضرورة إزالة الأثر الرقمي.

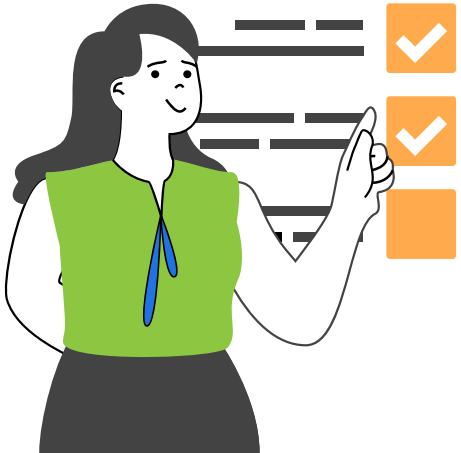
فعالية 8: سفراء الأمان الرقمي

المحتوى: ينفذ المعلم هذه الفعالية بعد الانتهاء من الدليل. يسأل الطلاب أن يحددوا أهم المخاطر وأهم النصائح لتجنبها حسبما تعلموا. بعد الاستماع للإجابات الأولية يستطيع المعلم أن يطرح أسئلة مُحددة ودقيقة أكثر وأن يربطها بأجوبة أخرى، مما يقدم مراجعة شاملة لنصائح الأمان الرقمي التي جاءت في الدليل. بعدها، يقسّم المعلم الصف إلى مجموعات ويطلب من كل مجموعة تحضير شرائح تلخص أحد المواضيع التي تعلموها لعرضها في الحصة التالية أو في أسبوع الأمان الرقمي.

هدف التعلم: تشجيع الطلاب على تطبيق ما تعلموه وحثهم على المبادرة لرفع الوعي حول السلامة والأمان الرقمي.

الطريقة: حوار مفتوح.

الأدوات اللازمة: لا شيء.



اتصلوا بنا:

info@7amleh.org | www.7amleh.org

تابعونا على وسائل التواصل الاجتماعي : **7amleh**