لا تقعوا في المصيدة!

المفتاح لحماية ا الاطفال الصغار والشبيبة على الأنترنت هو تثقيفهم بشأن الأخطار التي قد يوجهونها؛ تأكد من تواصل متبادل بينك وبينهم، وتثقيفهم بشأن المخاطر المحتملة وما ينبغي القيام به لحماية أنفسهم.

ما هو الموضوع؟

الاتّصال مع الأصدقاء، الزملاء، المعلين وغيرهم أصبح أكثر سهولةً مع التكنولوجيا الرقميّة. يمكننا الاتّصال مع العالم عبر عددٍ كبيرٍ من الوسائل: البريد الإلكتروني، النصوص، الرسائل الفوريّة؛ بالكلمات، بالصوَر، بالفيديوهات؛ باستعمال الهواتف، لوحات التابلت، والحواسيب النقالة. (كيف تتّصلون بأصدقائكم؟
ولكنّ الوسائل التي تجعل مشاركة المعلومات أمرًا سهلًا بالنسبة لنا، هي نفسها الوسائل التي تُسهّل على قراصنة النّت والمخادعين سرقة تلك المعلومات واستعمالها لإلحاق الضرر بأجهزتنا، علاقاتنا، وسُمعتنا الجيّدة.
إنّ حماية كلّ الأشياء التي تُساهم في إنشاء سُمعتنا في شبكة الإنترنت يتطلّب منا عمل أشياء بسيطة وذكية مثل استعمال أقفال للشاشة في أجهزتنا، أن نكون حذرين من وضع معلومات شخصيّة في أجهزتنا التي يُمكن أن تتعرّض للسرقة، والأهم من ذلك كلّه، اختيار كلمات مرور جيّدة.

إنّ تعلّم حماية معلومات الهويّة الشخصيّة، إنشاء كلمات مرور قويّة، واتّخاذ خطوات الحذر لدى تحميل برامج وملفات، يُعتبر أمرًا بالغ الأهميّة للحفاظ على أمان الاطفال الصغار والشبيبة إلى جانب الحفاظ على أمن المعلومات المُخزَّنة في أجهزتهم الرقمية. إنّ غياب ذلك كلّه من شأنه أن يُعرَّض الاطفال الصغار والشبيبة أنفسهم وعائلاتهم إلى تهديدات رقميّة مثل فيروسات الحاسوب، سرقة البيانات والهويّة والسيطرة على الحاسوب عن بُعد. من أجل فهم الأمن والأمان الرقميّ، قد تحتاجون إلى تعلّم بعض الكلمات غير المألوفة: انتحال رقمي، برمجيات خبيثة، برمجيّات تجسُّس، بريد إلكتروني غير مرغوب فيه، ونعم، حتّى رسائل القمامة. تُشير هذه المصطلحات إلى برامج صغيرة وجشعة تربط نفسها ببرمجيّات تظهر على أنها محترمة و- على سبيل المثال، لعبة قابلة للتحميل تبدو جميلة حقًّا – ثمّ ما تلبث أن تخرّب حاسبوكم فور تركيبها. لماذا هذا الأمر مهم؟ إذا لم يقم الاطفال الصغار والشبيبة بحماية معلوماتهم الشخصيّة، فإنّهم يعرّضون أنفسهم إلى الكثير من المخاطر المحتملة: إلحاق الضرر بمكوّنات الحاسوب، سرقة الهويّة، والخسارة الماليّة. قد لا يُدرك الأطفال أنّهم يضعون معلوماتهم في خطر لأنّ علامات التنبيه ليست واضحةً دائمًا. على سبيل المثال، يمكن لطفلٍ ما أن يطلب من طفلك كلمة المرور الخاصّة

به للعب لعبة، الأمر الذي يسمح له بالدخول إلى حساب البريد الإلكتروني الخاصّ بالطفل. أو يمكن أن يستعمل الاطفال الصغار والشبيبة برنامجًا لمشاركة الملفات ينقل معه فايروسًا لحاسوبكم. يمكن يُطلَب من طلاب المرحلة الابتدائية المتقدمة أن يوفّروا معلومات عن الهويّة الشخصيّة مثل رقم الهاتف المنزلي، العنوان، تاريخ الميلاد، أو رقم الضمان الاجتماعي الخاصّ بكم من خلال سارق ينتحل شخصيّة أخرى، الأمر الذي من شأنه أن يُعرّض العائلة إلى خطر سرقة الهويّة. تمامًا كما هو الحال في الحياة الواقعيّة، يجب على الاطفال الصغار والشبيبة الذين يُبحرون في شبكة الإنترنت أن يعرفوا بمن يمكن الوثوق به .

هدف الفعاليّة:

رفع الوعي بخصوص تقنيّات يستعملها الناسُ لسرقة الهويّات من خلال فعاليّة يدرسُ فيها الطلاب عددًا من الرسائل والنصوص الإلكترونيّة ويحاولون أن يقرّروا أيّ الرسائل حقيقيّة وأيها رسائل تصيُّد مزيّفة

الأهداف التعليمية

- ☐ **تعلُّم** تقنيّات يستعملها الناسُ لسرقة الهويّات.
- ☐ **مراجعة** أساليب لمنع سرقة الهويّة.
- ☐ **تعلُّم** الحديث مع شخصٍ بالغٍ موثوق إذا شعروا أنّهم ضحية لسرقة الهويّة.
- ☐ **التعرّف** على علامات محاولات الخداع.
- ☐ **الحذر** من كيفية مشاركة المعلومات ومن الشخص الذي تتم هذه المشاركة معه.

مدّة الفعاليّة: 90 دقيقة
جمهور الهدف: طلاب الصفوف الخامس-الثامن

ما معنى التصيُّد على أيّ حال؟

التصيّدُ معناه أن يحاول شخصٌ ما سرقة معلومات مثل تفاصيل دخولكم أو حسابكم عن طريق انتحال شخصيّة أخرى تثقون بها. يُرسل إليكم هذا الشخص رسالة إلكترونيّة، نصّ إلكتروني أو يتواصل معكم بطريقة أخرى عبر الإنترنت. رسائل التصيّد – والمواقع غير الآمنة التي تحاول هذه الرسائل أن ترسلكم إليها أو مواد التحميل والمرفقات التي تحاول أن تجعلكم تفتحونها – يمكنها أيضًا أن تزرع فيروسات في حاسوبكم بحيث يتم استعمال قائمة المتّصلين لديكم لاستهداف أصدقائكم وعائلتكم بمزيد من رسائل التصيّد. قد تحاول بعض الرسائل المزيّفة الأخرى أن تخدعكم بتحميل برمجيات خبيثة أو برمجيات غير مرغوب فيها حيث تخبركم بأنّ هناك مشكلة ما في جهازكم. تذكّروا: لا يمكن لأيّ موقع أو إعلان أن يحدد ما إذا كان هناك خللٌ ما في جهازكم!

بعض هجمات التصيّد تبدو مزيّفة بشكلٍ واضح. ولكن هناك رسائل تصيّد أخرى يمكن أن تكون متطوّرة ومقنعة. على سبيل المثال، عندما يُرسل إليكم شخصٌ مخادع رسالة تشمل بعض المعلومات عنكم، يُدعى ذلك تصيُّد بالرُّمح، حيث يمكن أن يكون هذا النوع من التصيّد فعّالًا جدًّا.

من المهمّ بمكان أن نعرف كيفيّة تحديد أيّ شيء غريب أو غير عادي في رسائل البريد الإلكتروني أو النصوص الإلكترونية في مرحلة مبكرة قبل الضغط على روابط مُريبة أو إدخال كلمة المرور في مواقع خطيرة.

إليكم بعض الأسئلة التي يجب طرحُها لدى فحص رسالةٍ أو موقع:

- ☐ هل في الرسالة مؤشّرات عن موقع يمكن الوثوق به، مثل وجود شعارات؟
- ☐ هل رابط الموقع يتلاءم مع الاسم والعنوان الذي تبحثون عنه؟
- ☐ هل هناك نوافذ تظهر أمامكم فجأة؟ (عادةً ما يكون ذلك إشارةً سيئة.)
- ☐ هل يبدأ الرابط بـ https:// يسبقه قفل أخضر؟ (ذلك يعني أنّ الاتّصال مُشفّر وآمن.)
- ☐ ماذا يوجد في النصوص ذات الخطّ الصغير؟ (هناك يضعون الأشياء المُريبة.)

<u>سير الفعاليّة:</u>

1. <u>مجموعات تدرس أمثلة.</u>

تقوم المعلّمة بتوزّيع الصف إلى مجموعات، تحصل كلّ مجموعة على بطاقة فيها **أمثلة** لرسائل ومواقع إنترنت. على أفراد المجموعة ان **يحدّدو خياراتهم**، أيّ الرسائل حقيقيّة وأيها رسائل تصيُّد مزيّفة ومناقشة الخيارات المرفقة للأمثلة.

- قرّروا ما هو "حقيقي" أو "مزيّف" بالنسبة لكلّ مثال، ورتّبوا أسباب قراركم أدناه
- أيّ الأمثلة يبدو حقيقيًّا وأيُّها يبدو مثيرًا للريبة؟ هل تفاجأتم بأيٍّ من الإجابات؟

إليكم بعض الأسئلة الإضافية لطرحها على أنفسكم لدى تقييم الرسائل والمواقع التي تجدونها في شبكة الإنترنت:

- ☐ هل تبدو هذه الرسالة سليمة؟
ما هو شعوركم الأوليّ؟ هل تلاحظون جوانب معيّنة من الرسالة تثير الريبة؟
- ☐ هل يعرض عليكم الموقع شيئًا مجّانيًّا؟
العروض المجّانيّة لا تكون مجّانيّةً في العادة.
- ☐ هل تطلب الرسالة معلومات شخصيّة عنكم؟
بعض المواقع يطلب معلومات شخصيّة ليتمكّن من إرسال رسائل إلكترونيّة مزيّفة إليكم. على سبيل المثال، "اختبارات الشخصيّة" يمكن أن تجمع حقائق عنكم ليصبر من السهل أن يكشف أحدهم كلمة المرور الخاصّة بكم أو بعض المعلومات السريّة. معظم المصالح التجاريّة الحقيقيّة، بالمقابل، لا يطلب معلومات شخصيّة عبر البريد الإلكتروني.

- ☐ هل تطلب منكم الرسالة إرسالها لأشخاص آخرين أو هل هي نشرة اجتماعيّة؟
إنّ رسائل البريد الإلكتروني والنشرات التي تطلب منكم تمريرها إلى جميع من تعرفون، يمكن أن تضعكم أنتم وغيركم في خطر. لا تفعل ذلك ما لم تحرص على التأكّد من سلامة المصدر وسلامة الرسالة قبل تمريرها.
- ☐ هل فيها نصّ بخطّ صغير؟
أسفل الصفحة في معظم المستندات تضمّ "نصًّا صغيرًا". عادةً ما يحتوي النصّ الصغير على الأشياء التي يُفترض بكم ألّا تلاحظوها. على سبيل المثال، عنوانٌ في أعلى الصفحة يمكن أن يدّعي أنّكم فزتم بهاتف مجانيّ، ولكن في النصّ الصغير ستكتشفون أنّ عليكم دفع 200 دولار شهريًّا للشركة.

بعد إجراء نقاش في الصفّ داخل المجموعات ، يقوم الطلاب بصياغة وطرح توصيات تشمل نقاط مُشدَّدة وعِبَر لكيفية توخي الحذر من هجمات التصيّد.

2. ختام الفعاليّة

لاختتام النقاش داخل الصفّ، تقول المعلّمة للطلاب "عندما تُبحرون في شبكة الإنترنت، كونوا على حذرٍ دائمٍ من هجمات التصيّد في بريدكم الإلكترونيّ، نصوصكم، ورسائلكم التي تنشرونها – واحرصوا على أن تُخبروا الأشخاص المناسبين بذلك إذا حدث وتعرّضتم للخداع".

للمعلّمة: أمثلة عن القواعد (يمكن إضافة قسمٍ منها في حال لم يطرحها الطلاب):

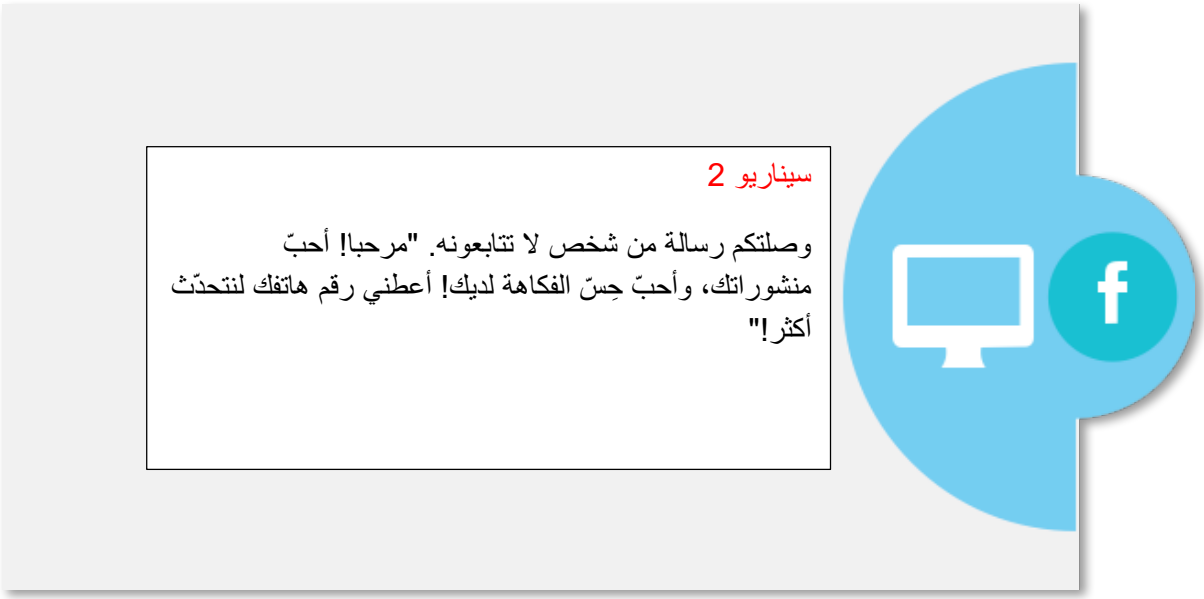
<u>وماذا لو وقعتم في فخّ الرسائل المزوّرة؟ ابدأوا بهذا: لا ترتعبوا!</u>

- ✓ **أخبروا أهلكم، معلّمكم، أو شخص بالغ تثقون به على الفور. كلما انتظرتم فترة أطول، أفسحتم المجال لحدوث شيءٍ أسوأ.**
- ✓ **غيّروا كلمات المرور الخاصّة بكم في حساباتكم على شبكة الإنترنت.**
- ✓ **لو وقعتم، فعلًا، في فخّ التصيّد أو الرسائل المزيّفة، أبلغوا أصدقاءكم الذين قد يكونون مستهدَفين نتيجةً لذلك.**
- ✓ **استعملوا إعداداتٍ لإرسال بلاغٍ بأنّ الرسالة مزيّفة، إذا كان ذلك ممكنًا.**

سيناريو 1

بعد حصّة الرياضيّات مع المعلم مؤنس ، وصلتكم هذه الرسالة على هاتفكم النقال: "أنا زاهي من صفّ الرياضيّات مع المعلم مؤنس. هل فهمت الواجب المنزليّ؟"

- ☐ **تجاهلوا زاهي**. كما هو الحال دائمًا، إذا لم تكونوا تعرفون هذا الشخص، ليس عليكم أن تردّوا على الإطلاق.
- ☐ **احجبوا زاهي**. سيكون خيارًا جيّدًا أن تحجبوا مارك إذا كنتم متأكّدين من عدم وجود شخص اسمه **زاهي**. في حصّة الرياضيّات مع المعلم مؤنس.
- ☐ **"أهلا، م زاهي. هل أنت مَن يجلسُ خلفي؟"** إذا لم تكونوا متأكّدين، تستطيعون السؤال.
- ☐ **"طبعًا. سأشرح لك بعد الدوام."** هذا خيارٌ جيّد فقط إذا كنتم متأكّدين من هويّة الشخص.
- ☐ **"أنا لا أتعلّم الرياضيّات مع المعلم مؤنس – بل مع المعلمة نهى."** إذا كنتم لا تثقون بهذا الشخص اعتمادًا على ما قاله، فإنّ أفضل خيارٍ هو تجاهل الرسالة. بالطبع، يجب ألّا تعطوهم معلومات شخصيّة مثل اسم معلّم الرياضيّات الخاصّ بكم.
- ☐ **"اتّصل بي على 555-3444 (650)."** غالبًا، لا تفعلوا ذلك؛ ما لم تكونوا متأكّدين من أنّكم تعرفون هذا الشخص، فليس من الحِكمة بمكان أن ترسلوا إليه معلومات شخصيّة عنكم.



- ☐ **تجاهلوا soccergirl12@**. ليس عليكم أن تردّوا إذا كنتم لا تريدون ذلك.
- ☐ **احجبوا soccergirl12@**. إذا وجدتم أنّ هذا الشخص مثير للريبة وقمتم بحجبه، فلن تسمعوا منه أيّ شيء آخر.
- ☐ **"مرحبا، هل أعرفك؟"** إذا لم تكونوا متأكّدين، اطرحوا أسئلة قبل إعطاء معلومات شخصيّة عنكم.
- ☐ **"حسنًا، رقمي هو..."** إيّاكم أن تفعلوا ذلك! حتّى إذا تأكّدتم من هويّة هذا الشخص، ليس من الحكمة بمكان أن تعطوا معلومات شخصيّة عبر وسائل التواصل الاجتماعي. جِدوا طريقة أخرى للتواصل من خلال الأهل، المعلّمين، أو أيّ شخص آخر تثقون به.

سيناريو 3

وصلتكم رسالة دردشة من شخصٍ لا تعرفونه. "رأيتك في صفّ الرياضيّات اليوم. أنت ظريف جدًّا! ما هو عنوانك؟ أستطيع أن أزورك لنخرج معًا."

- ☐ **تجاهلوا هذا الشخص**. غالبًا، هذا خيارٌ جيّد.
- ☐ **احجبوا هذا الشخص**. لا تتردّدوا في فعل ذلك إذا انتابكم شعورٌ بعدم الراحة تجاه أيّ شخص.
- ☐ **"من أنت؟"**. غالبًا لا تجيبوا. إذا كانت الرسلة تبدو لكم مُريبة، فمن المفضّل ألّا تجيبوا أو أن تحجبوا الشخص.
- ☐ **"هل هذه أنتِ يا ليزي؟ أنت ظريفة جدًّا كذلك! أنا أسكن في شارع الباشا رقم 240."** هذه ليست فكرة جيّدة، حتّى إذا كنتم تعتقدون أنّكم تعرفون هويّة الشخص. قبل أن تعطوا شخصًا تعرّفتم عليه حديثًا عنوانكم أو معلومات شخصيّة عنكم، افحصوا هذا الشخص حتّى وإن افترضتم أنّك تعرفونه.

.

سيناريو 4

وصلتكم هذه الرسالة: "مرحبا، التقيت صديقتك قبل قليل! وقد أخبرتني عنك. أحب أن ألتقي بك. ما هو عنوانك؟"

- ☐ **تجاهلوا.** إذا لم تكونوا تعرفون هذا الشخص ولكن لديكم صديقة اسمها سامانثا، فإنّ أكثر خيارٍ آمِن بالنسبة إليكم هو أن تفحصوا الأمر مع سامانثا أولًا قبل أن تردّوا على هذه الرسالة.
- ☐ **احجبوا.** إذا لم تكونوا تعرفون هذا الشخص وليس لديكم صديقة اسمها سامانثا، فإنّ من الحكمة، غالبًا، أن تستعملوا إعداداتكم الشخصيّة لحجب هذا الخص من قائمة المتّصلين بشكل نهائي.
- ☐ **"من أنت؟"** ليست أفضل فكرة، في الغالب؛ إذا كنتم لا تعرفون هذا الشخص، فإنّ من الأفضل ألّا تُجيبوا، على الأقلّ حتّى تكونوا قد حصلتم على إجابة من سامانثا أولًا.