

موضوع الدرس

أمن المعلومات في شبكة الإنترنت

الفئة العمرية: الصف التاسع

المحور القيادي: المحور الأول – الاستهلاك الواعية واتخاذ القرار المالي

موضوع الدرس: أمن المعلومات في شبكة الإنترنت

مرتكزات الدرس

أمن المعلومات والاحتيال عبر الإنترنت: في عالم أصبح فيه أموالنا رقمية، أهم مهارة مالية هي أن نعرف كيف تحميه. في هذه الوحدة، سنتعلم كيف نتجنب ترك بصمة رقمية وكيفية التنقل بثقة في تطبيقات الدفع والتسوق عبر الإنترنت، كاشفاً عن أكثر الطرق الاحتيالية تطوراً – من التصيد الاحتيالي الكلاسيكي إلى فخاخ الذكاء الاصطناعي التي تبدو أكثر واقعية من أي وقت مضى. من خلال محاكاة "الحقيقة أو المزيفة"، سنتعلم كيفية التعرف على العلامات الحمراء في ونصبح مستخدمين أذكياء ومحميين في الحيز الرقمي.

مفاهيم أساسية:

المصفوفة الإلكترونية، البصمة الرقمية، الهندسة الاجتماعية، الاحتيال المتنكر، المصادقة الثنائية، أذونات الوصول، ملفات تعريف الارتباط. أنواع الاحتيالات: التصيد الاحتيالي، التصيد الصوتي، التهريب، التزييف العميق، برامج الفدية (الفيروسات)، عمليات الاحتيال "لديك طرد"، عمليات الاحتيال القروضية، التسوق الآمن عبر الإنترنت، المواقع الآمنة، منصات الدفع الآمنة.

المهارات الأساسية:

الثقافة المعلوماتية: يُطلب من الطلاب جمع المعلومات، وتحديد أنواع الاحتيالات البصرية، وتقييم مستوى موثوقية مصادر المعلومات والمواقع الإلكترونية.

التفكير النقدي: يُطلب من الطلاب تحليل التحيزات المعرفية، ومعالجة عمليات اتخاذ القرار فوق الإدراكية.

الثقافة الرقمية: يطلب من الطلاب فحص URL أي عناوين وتشغيل المنصات الرقمية لعرض البيانات والتحقق من المواقع الإلكترونية والرسائل والبريد الإلكتروني وغيرها، ومعرفة كيفية النشر والحذر من ترك بصمات رقمية قد تهددهم.

القيم الرئيسية:

المسؤولية الشخصية، النزاهة والموثوقية، المسؤولية المتبادلة، المرونة الرقمية

المدة الزمنية المقدّرة: (90 دقيقة)

رابط العرض المصاحب للدرس: عرض [מצגת](#)

كتابة وترجمة: فريال مسّاد



أهداف الدرس:

1. الهدف 1: **سيحدد الطالب** "الإشارات الحمراء" وآليات الخداع في رسائل التصيّد ومواقع التواصل، مع تحليل التحيزات المعرفية (مثل الإلحاح والخوف) والأخطاء اللغوية النموذجية للاحتيال الإلكتروني.
1. الهدف 2: **سيقارن الطالب** بين المواقع الإلكترونية ومصادر المعلومات المختلفة باستخدام أدوات الثقافة الرقمية (التحقق من العناوين URL، مقارنة الأسعار، وقراءة المراجعات) لتحديد مستوى مصداقيته قبل إجراء معاملة مالية.
1. الهدف 3: **يجب على الطالب أن ينجح بعرض** حالات احتيال من حياته الشخصية ويعرف كيف يتبنى ما تعلمه ليتمكن من الدفاع عن نفسه
1. الهدف 4: **سيحلّل الطالب** المعضلات الأخلاقية والحالات الاحتيالية من خلال المحاكاة وألعاب تقمص الأدوار، وسيضع نموذج عمل شخصي لتقديم المساعدة والمعلومات للآخرين في حال اكتشاف ضرر للفضاء الرقمي.

وسائل مساعدة للدرس

عارضه الشرائح، ورقة عمل، بطاقات ذات لونين (حمراء وخضراء)، جهاز عرض

קישור למצגת

خطة الدرس

مقدمة 10 دقائق: عرض للموضوع واستبيان لإثارة الاهتمام بالمادة التي ستتم دراستها.

مواضيع درس أمن المعلومات في شبكة الإنترنت هي:

1. السابير والبصمة الرقمية/ الإلكترونية
2. أنواع الاحتيال والهندسة الاجتماعية
3. الحماية من عمليات الاحتيال في الإنترنت
4. التسوق الآمن عبر الإنترنت

هدف الإفتتاحية: رفع الوعي بأن كل عمل رقمي هو بصمة أمامية.

النشاط:

يمنح كل طالب بطاقة خضراء وبطاقة حمراء. يعرض الشرائح من 3 إلى 9 ويطلب من الطلاب التصويت بحيث من يوافق على الجملة أو الحدث يرفع الكرت الأخضر، وأولئك الذين لا يوافقون أو لم يحدث لهم أن يرفعوا البطاقة الحمراء. وأثناء ذلك، أطلب من كل طالب أن ينظر حوله ويرى الوضع العام في الصف.



نص الدرس:

البصمة الرقمية، أنواع الاحتيال، الحماية، الشراء الآمن، والدفع الآمن

إذاً، وفقاً للأغلبية، الوضع هو أن معظم الطلاب قد مروا بمعظم الأحداث في العرض.

هنا أقول لهم: "مبروك على ترك بصمات رقمية"

نتقدم لشرح مفهوم "البصمة الرقمية": في كل مرة نحمل تطبيقاً جديداً، أو نشترى قطعة ملابس من المواقع المختلفة، أو ننقل ملفاً على ديسكورد، فإننا نترك باباً مفتوحاً أو بصمة رقمية. هل تعرف من لديه مفتاح هاتفك أو ساعتك أو معلومات بطاقتك الائتمانية؟

تشكل البصمات الرقمية جميع البيانات التي يتركها الشخص أثناء أنشطته عبر الإنترنت. يمكن أن تشمل هذه الرموز التعبيرية المفضلة، سرعة الكتابة، العبارات الرائجة، التطبيقات المفضلة، الإضافات المفضلة، المعلومات الشخصية، عادات التصفح، التفاعلات الاجتماعية، والمزيد.

كيف نترك بصمات رقمية، (الشريحة 12):

أطلب منهم أن ينظروا ويخبروني كيف يمكننا فعلياً ترك أثر رقمي. يبدأ الأطفال في إلقاء الإجابات. ثم أخص موضوع كيف نترك المشتتات الرقمية

الشرائح 13-16

كيفية ترك آثار رقمية: دعونا نتعرف على أنواع البصمات الرقمية

1. الشبكات الاجتماعية:

- التعليقات والإعجابات - كل تعليق محفوظ بتاريخ ووقت، ويمكنك إخفاء الإعجابات ولكنها لا تُحذف نهائياً
- الصور والستور يهات - حتى لو حذفت الصور والستور يهات، قد تكون قد حفظت في المواقع أو تم تسجيلها قبل آخرين
- المشاركة/النشر - النسخ والبحث عن المحتوى يخلق عدة "بصمات" على الشبكة، يصعب حذفها بالكامل بعد توزيع المحتوى

2. الألعاب والدردشات عبر الإنترنت:

- الرسائل في مجموعات واتساب - محفوظة من قبل جميع المشاركين في المجموعة
- محادثات ديسكورد - مسجلة على الخوادم والمدونات
- التفاعلات في ألعاب الفيديو عبر الإنترنت - محفوظة في تاريخ اللعبة وأحياناً تبث مباشرة

3. سجلات البحث:



- عمليات البحث في جوجل
- مدة المشاهدات في اليوتيوب
- وقت مشاهدة الفيديو – تتعلم الخوارزميات أنماط السلوك (الرموز التعبيرية المفضلة، عادات التصفح) لتخصيص الإعلانات بحسب الأنماط الخاصة بكل فرد

4. المعلومات عن الموقع GPS

- بيانات موقع GPS
- تطبيقات الخرائط
- رسم الموقع على وسائل التواصل الاجتماعي
- تطبيقات الطقس/الرياضة - تابعها في الخلفية حتى بدون وعي كامل للمستخدم

أنواع الاحتيال عبر الإنترنت:

كما ذكرنا في التصفح والإجراءات المختلفة التي نقوم بها، نترك بصمة رقمية تسمح للغرباء باستخدام المعلومات المتبقية لدينا بطريقة غير أخلاقية.

النوع 1: الهندسة الاجتماعية (الشريحة 17):

الهندسة الاجتماعية هي تقنية للتلاعب النفسي تستخدم لدفع الناس لاتخاذ إجراءات أو كشف معلومات سرية. على عكس الهجمات السيبرانية "العادية" التي تعتمد على ثغرات برمجية أو برمجية، تستغل الهندسة الاجتماعية أضعف حلقة في سلسلة الأمان: العامل البشري.

تعمل الهندسة الاجتماعية على مراحل:

الخطوة 1: جمع المعلومات: يحقق المهاجم مع الضحية (عبر الشبكات الاجتماعية، مواقع الشركات، إلخ) للعثور على المعلومات والثغرات.

الخطوة 2: التواصل: التواصل مع الضحية باستخدام هوية مزيفة (مثل ممثل الدعم التقني، مدير بنك، أو زميل).

الخطوة 3: التلاعب: اختلاق قصة لاستخراج المعلومات أو تحفيز إجراء.

الخطوة 4: تنفيذ المهمة: يقوم الضحية بتحويل كلمة المرور، أو النقر على الرابط، أو إجراء التحويل المالي.



ליکم مثالا لنفهم بالضبط كيف يحدث هذا:

نورا هي فتاة في الصف التاسع، يتابعها المحتال على مواقع التواصل ويلاحظ أنها من المعجبين جداً بمغني مشهور وفقاً لنشاطها (إعجابات، مشاركات، تعليقات...) من خلال متابعتها تركت لها بصمة رقمية. هذه هي مرحلة "جمع المعلومات". يُرسل لها المحتال رسالة يخبرها فيها أنها فازت بتذاكر لعرض المغني المشهور، وأن الكمية محدودة. هذه هي مرحلة التواصل. تحمست نورا جداً وقالت لنفسها: "بالطبع أريد، لقد انتظرت هذا طويلاً" فضغطت على الرابط في الرسالة التي تلقتها من المحتال. هذه هي خطوة التلاعب. كادت نورا أن "تنفذ المهمة" وتسلم تفاصيل بطاقة الائتمان.

النوع الثاني من الاحتيال: التصيد الاحتيالي (شريحة 19)

التصيد الاحتيالي هو محاولة لسرقة معلومات شخصية مثل أسماء المستخدمين، وكلمات المرور، وبطاقات الائتمان، والمزيد، وجعلنا نضغط على روابط خبيثة (مما يؤدي إلى الوقوع في الفخ).

وهناك عدة أنواع من التصيد الاحتيالي:

1. التصيد الصوتي: ينتحل المحتال شخصيات معروفة، مثل موظفو البنوك والوزارات الحكومية، ويحاولون جعل الضحية تكشف عن معلوماتها الشخصية وتقوم بتنفيذ إجراءات معينة عبر الهاتف.
من يمكنه أن يشاركنا في مثل هذه الحالة؟
ماذا تفعل في مثل هذا الموقف؟
ما هو الشيء الصحيح الذي يجب فعله لتجنب تفويت فرصة أو مكالمة مهمة هو أن تطلب رقم هاتف، وتطلب إنهاء المكالمات، وستصل لتتأكد من أنهم ينتمون بالفعل إلى المنظمة التي قدموا أنفسهم منها.
2. التصيد المستهدف: يجمع المهاجمون معلومات مستهدفة عن الضحايا عبر الإنترنت. يتظاهرون بأنهم أشخاص لديهم اهتمامات مشابهة ويجعلون الضحايا يعتقدون أنهم موثوقون.
ماذا يجب أن تفعل في مثل هذه الحالة؟
3. التصيد الاحتيالي عبر الرسائل النصية SMISHING. إذا تلقيت رسالة عبر الهاتف أو البريد الإلكتروني، فلا تضغط على الرابط بأي ظرف من الظروف. إنما إبحث عن وسيلة للتواصل مع الجهة المتصلة، حتى تتأكد من أن الرسالة موثوقة.
4. التزييف العميق: يستخدم المحتالون برامج الذكاء الاصطناعي وينتحلون شخصية معروفة مثل: الرؤساء التنفيذيين، المشاهير، الأصدقاء، وغيرهم.
على سبيل المثال، تسجل صوت شخص ثم تستخدم هذا التسجيل وتحدث بذلك الصوت مع أحد الأقارب، عادة كبار السن، وتطلب منه المال أو تفاصيل بطاقة الائتمان، وما إلى ذلك.



כלנו נעلم أنه مع الابتكارات التكنولوجية، يطور المجرمون المزيد والمزيد من الطرق للغش ويجب أن نكون حذرين.

5. الانتحال على الشبكات الاجتماعية: ينتحل المهاجمون الشخصيات على شبكات التواصل الاجتماعي ويطلبون معلومات شخصية تحت باسم صاحب الحساب. على سبيل المثال: صفحات تنتحل شخصية إنستغرام وتحذر من أن "حسابك ملغي"، أو انتحال شخصية موقع حكومي، وهكذا.

الانتحال على الشبكات الاجتماعية ظاهرة تزداد انتشاراً، وهناك عدد لا بأس به من الأشخاص الذين وقعوا فيها. هناك عدد لا بأس به من المحتالين الذين يحصلون على معلومات عنا عبر شبكات التواصل الاجتماعي. لكي نحمي أنفسنا، يجب أن نتجنب إضافة أصدقاء يبدوون مشبوهين، أشخاص ليس لدينا معهم أصدقاء مشتركين، وأسماءهم تبدو غريبة. عادة ما تشكل هذه المشاكل خطراً جدياً

فلنأخذ بعض الأمثلة لتوضيح ما تعلمناه:

المثال 1 - التصيد الاحتيالي "لديك طرد"

هذه عملية احتيال شائعة جداً مؤخراً. يستخدمونها المحتالون لأنها تبدو رسالة معقولة جداً.

كيف تعرف إذا كانت الرسالة التي تلقيتها من شركة الشحن حقيقية أم أنهم يحاولون خداعك؟

1. خلق الضغط والشعور بالإلحاح – طلب من الناس اتخاذ إجراءات فورية بدافع "الإلحاح" هو تقنية شائعة تهدف إلى جعل الناس يتصرفون بدافع التوتر.

2. نقص معلومات للتواصل – عادة ما تستخدم المنظمات الرسمية الاسم الأول للعميل وتخطبه شخصياً. قد يكون الطلب العام من "عميل عزيز" علامة مريبة.

3. إعادة التوجيه إلى مواقع خارجية – قد تبدو المواقع المنتحلة مشابهة جداً في المظهر للموقع والنطاق الأصلي، لذا ينصح بالدخول إلى الموقع عبر المتصفح (جوجل مثلاً) وعدم الضغط على الرابط.

4. التحقق من المعلومات – إذا تلقيت إشعار دفع لطرد ما، ينصح بالتحقق من رقم الطلب الظاهر في الرسالة، بالإضافة إلى التأكد من رقم الطلب وقت الشراء. إمكانية أخرى هي التحقق من الموقع الرسمي لبريد إسرائيل أو تطبيق البريد والتأكد من رقم الإرسالية والتفاصيل المتعلقة بالطرد

5. عدم إعطاء المعلومات – لقد تلقيت رسالة غريبة، أو رسالة تبدو منطقية، تطلب منك تفاصيل بطاقتك الائتمانية – توقف! كن يقظاً في تزويد هذه المعلومات الشخصية والرموز وكلمات المرور.

مثال 2: التصيد الاحتيالي "القروض"

تلقي العديد من الأشخاص مؤخراً رسالة تنص على إمكانية الحصول على قرض بشروط جيدة



يجب الانتباه الى أن العروض الجيدة جدا هي من دواعي القلق والشكوك.

يعتبر هذا تصيد احتيالي بواسطة الرسائل النصية، ولكنه أيضاً تصيدٌ مستهدف. لأن المحتالين أحيانا يحصلون على معلومات عنا من خلال التصفح ويعرفون من الجمهور يواجهون ضائقة مالية، فإذا تلقوا مثل هذه الرسالة، فهناك احتمال أن يوافقوا على العرض ويقومون بالضغط على الرابط وبهذا يكونوا قد وقعوا في الفخ. في حالة الضغط، يعني ذلك أننا أعطينا مفاتيحنا للغرباء ويمكنهم دخول مساحتنا الخاصة التي لم تعد محمية.

ما علينا فعله هو تجاهل هذه الرسائل، وبالطبع عدم الضغط على الروابط تحت أي ظرف من الظروف.

المثال 3: التصيد الاحتيالي "الطريق السريع رقم 6"

هذه أيضا رسالة شائعة تلقاها الكثير من الناس واتضح أنها عملية احتيال

المثال 4: التصيد الاحتيالي لكبار السن "اللسعة الروسية":

كبار السن هم فئة عمرية يسهل خداعها، وهذا ما حدث في السنوات الأخيرة:

بعد شرح الرسالة، سألت الطلاب عن العلامات التي تدل على أن الرسالة عملية احتيال؟

1. انتحال صفة المسؤولين: غالبا ما ينتحل المحتالون شخصية مسؤولي الضمان الاجتماعي، وضباط الشرطة، ومندوبي المبيعات، والشركات التي تقدم خدمات الطوارئ الطبية (متظاهرين بأنهم أطباء)، ويستخدمون حتى "مكالمات الخدمة" لكسب ثقة كبار السن واستخراج المال منهم
2. التركيز على مجموعات محددة: هناك ظاهرة معروفة تسمى "اللسعات الروسية" الموجهة لكبار السن من الاتحاد السوفيتي السابق. تلقت الشرطة أكثر من 400 شكوى حول هذا الموضوع، ومنذ بداية عام 2026، تم تقديم 171 لائحة اتهام في قضايا احتيال ضد هؤلاء السكان
3. المبالغ المالية والشبكات المنظمة: هذه عمليات احتيال تجمع مبالغ ضخمة تصل إلى ملايين الشكّل من ضحاياها، مثل حالة لسع فيها فريق مكون من 11 مشتبه به مسنين من كبار السن مقابل حوالي مليون شيكل، أو امرأة تبلغ من العمر 92 عاما لسعها عشرات الآلاف من الشيكل.

النوع 3: عمليات احتيال متكررة (الشريحة 25)

هناك عمليات احتيال كامنة وراء محاولات الجذب التي تعتبر جذابة جداً. على سبيل المثال:

عرض سعر رخيص للغاية، ميزة مميزة ولفترة محدودة.



كما أن عمليات الاحتيال تختبئ خلف وعد بمشاعر لطيفة. على سبيل المثال: الاتصال، الانتماء، الظهور، الاعتراف، التقدير، المكانة.

النوع 4 : اختيال طلب الفدية: الشريحة 26

برامج الفدية هي برمجيات خبيثة شائعة جدا تهدف إلى ابتزاز الضحايا عبر الإنترنت

غالبا ما تعمل عملية الاختيال على الخطوات التالية:

- الخطوة 1: التسلل إلى النظام والبرامج في الحواسيب: يصيب البرنامج جهازا محمولا أو حاسوبا أو شبكة حاسوبية كاملة
 - الخطوة 2: التشفير والقفل: يقوم البرمجيات الخبيثة بقلل الجهاز ومنع الوصول إلى النظام وإلى المعلومات والملفات المهمة المخزنة عليه. يتم تنفيذ هذه العملية أحيانا باستخدام مفاتيح التشفير والاتصال بخوادم التحكم عن بعد
 - الخطوة 3: ابتزاز أموال الفدية: يطالب المهاجمون الضحية بدفع مبلغ مالي (عادة بعملات افتراضية يصعب تتبعها)، وفي المقابل يعدون بإزالة التشفير والوصول الى الملفات
- بعد أن تعرفنا على أنواع الاختيال، دعونا نرى ما هو الأكثر شيوعا حقا وما هو الأقل شيوعا. لكن أولا أطلب منكم التخمين أي عملية احتيال يعتقدون أنها الأكثر شيوعا.

الشريحة 27: إحصائيات، انتشار أنواع الاختيال المختلفة في إسرائيل

1. التصيد الاحتيالي بواسطة الرسائل الرسائل النصية: يمثل 35٪ من عمليات الاختيال. غالبا ما يكون "طرد ينتظرك" أو "تم حظر حسابك"
2. اختراق وسائل التواصل الاجتماعي 25٪ من إجمالي عمليات الاختيال - السيطرة على إنستغرام
3. احتيالات الذكاء الاصطناعي أو التزييف العميق 20٪ (مواقع تسوق مزيفة)
4. فيروسات وبرامج الفدية 20٪

الشريحة 28: السؤال هو، كيف يمكننا تحديد ما إذا كانت الرسالة أو المكالمة مشبوهة؟ يجب الانتباه للعناصر التالية والتحقق منها:

1. هل المكالمة أو الرسالة منطقية؟



2. هل هناك عنصر من الضغط والإلحاح؟

3. هل يوجد فيها توجه شخصي للتقارب أو للراحة النفسية؟

4. هل كنا نتوقع تلقي هذه المكالمة أو الرسالة؟

دعونا نتدرب على:

تلقي آدم مكالمة هاتفية:

"مرحبًا آدم، يوجد على حسابك لدى شارع 6 دين بقيمة 47.90 شيكل. يرجى تسديد المبلغ خلال 24 ساعة لتجنب إضافة رسوم أو فوائد تأخير. نظرًا لعدم تسديد المبلغ حتى الآن، تم تحويل الملف إلى إجراءات المتابعة القانونية العاجلة. للاطلاع على تفاصيل المبلغ وإتمام عملية الدفع، يُرجى الدخول إلى الرابط التالي"

ما الذي تعتقدون أنه يثير الشكوك في هذه الرسالة؟

أعطي الطلاب وقتًا للهدوء، والفحص والتفكير في المحادثة التي تلقاها آدم.

في الواقع، المحادثة مشكوك بأمورها وتحتوي عناصر تثير القلق.

ماذا تنتصح آدم؟

الشباب والخصوصية الرقمية: (شريحة 32)

رأينا من خلال الاستبانة الذي أجريناه وبعضكم شارك تجربته ومعظمنا هنا وهناك تركنا بصمة رقمية. والكثير منا قد مر أو سمع عن حادثة احتيال عن قرب، خاصة بين الشباب.

أين أنتم المراهقون في موضوع الاحتيال عبر شبكة الأنترنت؟

أبناء الشببية موجودون كثيرا على الإنترنت وفي كل مكان

اتضح أن الشباب تحت سن 35 (بالإضافة إلى كبار السن الذين تحدثنا عنهم سابقا) يميلون إلى تقديم المعلومات الشخصية والمالية بسهولة أكبر عبر الإنترنت.

سؤال: ما السبب برأيكم؟ (سأستمع إلى الطلاب ثم أقدم الإجابات على الشريحة)

أعرض الأسباب وأطلب منهم مرة أخرى في التصويت أن يوضح ما إذا كان صحيحا إلى حد ما بالنسبة لهم.

إذا فأنتم موجودون في أوضاع مشابهة تقريبا. والسؤال هو ما هي البصمة الرقمية التي تتركونها أثناء وجودكم على شبكة الإنترنت.



ما يميز جيل أبناء الشبكية ما يلي: نقص الخبرة، الثقة المفرطة في عالم التكنولوجيا، الميل للسلوك الاندفاعي، نقص المعرفة، والرغبة في النجاح المالي السريع.

السؤال، في رأيك، هل من الممكن منع الاحتيال عبر الإنترنت؟

الإجابة هي نعم، فلنتعرف على قواعد الحماية (الشريحة 33)

1. كلمة مرور قوية:

القاعدة 1: استخدم كلمة مرور طويلة تحتوي على حوالي 12 حرفاً تتكون من الحروف الكبيرة والصغيرة، وأرقام، ورموز خاصة

القاعدة 2: تجنب استخدام كلمات مرور شائعة، مثل: تاريخ الميلاد، أرقام التسلسل، عنوان البريد الإلكتروني

القاعدة 3: ابحث عن طريقة إبداعية لتتذكر كلمة المرور، على سبيل المثال: كورس من أغنية مفضلة

القاعدة 4: استخدم برنامج لإدارة كلمات المرور الآمن، وحدد كلمة مرور قوية لتغيير كلمة المرور بانتظام. وقم بإعداد المصادقة الثنائية لبرنامج إدارة كلمات المرور الخاص بك.

1. تجنب الإفراط في المشاركة: لتقليل البصمة الرقمية

2. إعدادات الخصوصية – والتحقق من الدخول بمرحلي أمان

3. لا توافق على العضوية على الشبكات الاجتماعية إذا لم يكن لديك أصدقاء مشتركين –

4. تحقق أولاً عند تحميل تطبيق أنك لا توافق على أي أذونات للوصول الى الهاتف، دليل أرقام الهواتف، الموقع وغير ذلك. فقط الأذونات الضرورية فقط في حال وأثناء استخدام التطبيق.

ملخص:

بعد أن تعلمنا ما هي البصمة الرقمية، وما هي أنواع الاحتيال، ورأينا أمثلة، دعونا نفحص مدى فهمنا للمواضيع التي تعلمناها/

أسئلة لتفعيل الصف: الشرائح 34-39

التسوق الآمن عبر الإنترنت: الشريحة 40

بعد أن تعلمنا ما هي البصمة الرقمية وكيف نترك معلومات عن أنفسنا عند تصفح الإنترنت، وتعلمنا أيضاً كيف يستخدم الناس هذه المعلومات لارتكاب الاحتيال وما هي أنواع الاحتيال، يجب أن ننقل الآن إلى الأهم وهو جيبونا وأموالنا.



אعداد الكثير من الناس التسوق عبر الإنترنت، لكن هذا يزيد من فرص الاحتيال لأننا أحياناً نضطر لإعطاء معلومات حساسة ، بما في ذلك وسائل الدفع والتفاصيل الحساسة.

أولاً، دعونا نتحدث بواسطة الأسئلة ونستمع إلى قصص زملائنا في الصف.

النشاط: توزيع ساعة الاجتماع على المتدربين:

[رابط إلى ساعة الاجتماعات](#)

https://drive.google.com/file/d/1imDD-QGD8trDew4Gt0biNUdad7ELmvMR/view?usp=drive_link

أطلب من الطلاب التجول وتحديد مواعيد اجتماعات مع خمسة طلاب في الصف

أستخدم الجرس، بحيث عند كل قرعة جرس ينتقل الطلاب الى اللقاء التالي مع زميل آخر. واستمر في طرح الأسئلة.

القضايا التي يتحدث عنها الطلاب بحسب الأسئلة التالية:

1. ماذا يعني لك مصطلح "التسوق الآمن عبر الإنترنت"؟
2. ما هي عواقب الشراء "الغير" آمن عبر الإنترنت؟
3. كيف يمكنك التأكد من أنك تتسوق بأمان عبر الإنترنت؟
4. ما هي وسائل الدفع التي تستخدمها عند التسوق عبر الإنترنت؟
5. ما هو أصعب ما حدث لي/لأحد أفراد العائلة أثناء عملية الشراء عبر الإنترنت؟

التسوق الآمن عبر الإنترنت: الشرائح 45-51 للمواقع الآمنة

كيف يمكنك معرفة ما إذا كانت المواقع التي تتصفحها آمنة؟

1. بجانب الرابط يتم وضع قفل مغلق، وينتهي الرابط بحروف https (وليس HTTP فقط)

2. ينتهي الموقع بلاحقة .com أو .co.il

3. ينصح بالتصفح فقط عبر شبكة WI-FI خاصة آمنة أو عبر WI-FI العام في أماكن مألوقة



4. أخطاء إملائية – قد تشير الأخطاء الإملائية أو في الصياغة إلى أن هذا موقع احتيالي. انتبه للصياغة التي تظهر على الموقع وانتبه للأخطاء والنواقص.

5. المراجعات وآراء الزبائن – ينصح بالتحقق مما إذا كانت هناك مراجعات أو آراء حول الموقع وما إذا كان الموقع لديه صفحة نشطة على الشبكات الاجتماعية.

6. التفاصيل التعريفية – ابحث في الموقع عن تفاصيل للتواصل بالشركة في قسم "من نحن" أو "تواصل معنا" والعنوان.

7. الوصول المباشر إلى الموقع وليس عبر الروابط – من الأفضل تصفح المواقع من خلال بحث مستقل على جوجل وليس عبر الروابط أو النقرات المباشرة.

الشريحة 52 - التسوق الآمن عبر الإنترنت - الدفع الآمن

الأهم هو جيبنا - لذا يجب أن نتنبه لأي وسيلة دفع نستعمل عند الشراء عبر الإنترنت:

أسمع من 4-5 طلاب كيف يدفعون، ثم أعرض وألخص طرق الدفع الآمنة عند الشراء عبر الإنترنت:

1. التعرف الذكي - في أي خدمة تم فيها إدخال تفاصيل بطاقة الائتمان، أو عند استخدام المحفظة الرقمية، ينصح بالتأكد من تفعيل التعرف الآمن باستخدام رمز شخصي لمرة واحدة قبل إجراء المعاملة. يمكن تفعيل التعرف

الآمن من خلال شركات بطاقات الائتمان Face ID

2. بطاقة ائتمان مسبقة الدفع (כרטיס נטען) – يمكنك من خلالها خصم مبلغ محدود. يمنع الحساب البنكي من التعرض للاحتيال، وفي حال حدوث تسريب، يحد من نطاق الضرر.

3. منصات الدفع عبر الإنترنت – البيانات المخزنة في منصات الدفع عبر الإنترنت مشفرة ولا تنقل إلى البائع وقت الدفع. ينصح باستخدام هذه الأنواع من المنصات مثل PayPal و Google Pay و Apple Pay و Bit وما شابه، باستخدام التحقق من الشيفرة، أو بصمة الإصبع، أو التعرف على الوجه، بدلا من إدخال تفاصيل بطاقة الائتمان مباشرة على الموقع.

4. PCI DSS – معيار تضعه شركات بطاقات الائتمان الكبرى لضمان حماية بيانات بطاقات الائتمان أينما تم تخزينها. في مرحلة الشراء على الموقع الإلكتروني، ينصح بالتحقق مما إذا كان علامة PCI DSS القياسية الخاصة بشركات بطاقات الائتمان تظهر على شاشة الشراء في هوامش الصفحة.

في الختام،

إذا وقعت في عملية احتيال، فلا تخجل من مشاركتها مع والديك أو أي شخص يتفقون عليه لوقف الضرر.



מידע נוסף להעשרה והרחבת הידע למורה

העשרה למורה

הרחבה והעמקה של נושאים למורה או חומר עזר רלוונטי לשיעור

קישורים רלוונטיים

[סביבת סייבר לחטיבת ביניים](#)

[מערך הסייבר הלאומי](#)

[אתר טעימות פיננסיות](#)

צידה לדרך- נספחים

[رابط لورقة عمل 1](#)

[رابط لورقة عمل 2](#)

[קישור שעון פגישות](#)

[اختبار تلخيصي](#)





חינוך פיננסי

משרד החינוך

למידה בונה אדם
המוסדות הפדגוגיים
אנף א'- תחומי בחירה ורב תחומי
הפיקוח על הוראת מדעי החברה

