

الأمان على الإنترنت والخداع والمحتوى غير المهم أو الاحتيالي

سيتعرف المشاركون على المستخدمين المتطفلين على الإنترنت الذين قد يحاولون استخدام نقاط ضعف أمنية لتجميع معلومات عنهم. سيتمكن المشاركون من وصف مخاطر التواجد على الإنترنت، ووضع استراتيجيات للتفاعل عبر سلوكيات أكثر أماناً، والتعرف على رسائل المحتوى غير المهم أو الاحتيالي، وإيضاح من يحق له طلب كلمات السر الخاصة بهم.

المواد

مذكرة المحتوى غير المهم أو الاحتيالي

المخاطر على الإنترنت

الجزء الأول

أخبر طلابك

عندما تستخدم الإنترنت، ربما تعرض نفسك للمخاطر من خلال مجرد الوصول إلى صفحة ويب أو الاتصال عبر الإنترنت أو تنزيل البيانات. في بعض الأحيان، تستطيع مواقع الويب التي تزورها أو الأشخاص الموجودون على نفس الشبكة أو حتى جهات خارجية معرفة موقعك أو معلومات أخرى عنك عند قيامك بالتصفح.

اطرح أسئلة على طلابك

من الذي قد يستفيد من نقاط الضعف الأمنية على الإنترنت للاطلاع على معلوماتك الشخصية؟

1. تشمل الإجابات المحتملة المخترقين الخيبيين والمراقبة الحكومية وما إلى ذلك.

أخبر طلابك

عندما تتصفح الويب، من الممكن للمخترقين الخيبيين تجميع بيانات عنك بنفس الطريقة التي يقوم بها مزود خدمة الإنترنت. للحد من هذه المخاطر، يجب عليك استخدام اتصال آمن بينك وبين موقع (مواقع) الويب التي تحاول الوصول إليها. بغض النظر عن اتصالك، تحاول العديد من مواقع الويب تتبع أنماط الاستخدام الخاصة بك عبر منصات متعددة. يمكنها مشاهدة متصفحك وموقعك وأنماط استخدامك الأخرى لمحاولة تكوين صورة عنك.

اطرح أسئلة على طلابك

لماذا يحاول المخترقون الخيبيون الوصول إلى معلوماتك على الإنترنت؟ ما المعلومات التي يبحث عنها الأشخاص؟ لماذا قد تحاول مواقع الويب التي لم تقم بتسجيل الدخول إليها أن تتبع هويتك؟

1. أي معلومات لتحديد الهوية الشخصية وأي معلومات يمكن بيعها أو استغلالها لتحقيق مكاسب مالية.

هل يعرف أحد ما المقصود بالبرامج الضارة؟ ما الذي يمكنها فعله؟

أخبر طلابك

البرنامج الضار عبارة عن تعليمية برمجية خبيثة تعمل خلسة على الكمبيوتر. تستطيع بعض البرامج الضارة تجميع البيانات من أي جزء في جهاز الكمبيوتر المحلي، بدءاً من محرك الأقراص ووصولاً إلى بيانات المتصفح. ويمكنها أيضاً أن تسمح للمخترقين بالتحكم في جهاز الكمبيوتر واستخدامه بالطريقة التي يريدونها. لكن معظم البرامج الضارة تكون أبسط من ذلك، مثل مواقع الويب التي تقلد البوابات الآمنة كالهيك أو الملحقات التي تضع الإعلانات في متصفحك لكسب المال.

اطرح أسئلة على طلابك

ما الذي يمكنك القيام به لحماية نفسك من البرامج الضارة أو التجسس أو التتبع؟

أخبر طلابك

توخّ الحذر عند النقر على الروابط أو الإعلانات أو منشورات وسائل التواصل الاجتماعي. هل يتطابق عنوان URL مع توقعاتك؟ هل تصل إلى الصفحة نفسها عندما تكتبه مرة أخرى بنفسك أو عندما تبحث عن موقع الويب؟ من القواعد الجيدة أن TLS/SSL يجب أن تحمي أي صفحة تسجيل دخول إلى حساب مهم (مثل Google أو فيسبوك أو Twitter أو الحسابات البنكية). تضع TLS/SSL عوائق منيعة أمام أي مخترق على الشبكة نفسها حتى لا يرسل إليك موقع ويب مزيفاً إذا كتبت عنوان URL الصحيح، والذي قد يكون بسيطاً للغاية.

ستتمكن بعض مواقع الويب من تشغيل تعليمية برمجية للوصول إلى معلوماتك الشخصية أو حساباتك عبر الإنترنت إذا ارتكبت تلك المنصات خطأ في الترميز. يمكنها بعد ذلك استخدام حساباتك لإرسال محتوى غير مهم أو احتيالي إلى الآخرين.

لا تقم بتنزيل البرامج أو تثبيتها إلا من مصادر موثوق بها فقط وفكر جيداً قبل تنزيل الملفات التنفيذية (ملحقات .exe أو .pkg أو .sh أو .dll أو .dmg). الملفات التنفيذية هي أي عنصر من شأنه تنفيذ إجراء. في بعض الأحيان، قد تكون تلك الإجراءات ضارة. على سبيل المثال، يمكن لأحدهم كتابة نص تنفيذي لمحو محرك الأقراص الخاص بشخص ما أو لتثبيت متصفح مزيف. لذلك، يجب عدم تثبيت المحتوى إلا من مصادر موثوق بها فقط.

يمكنك استخدام برنامج حماية من الفيروسات لمنعك من تشغيل البرامج الضارة. يأتي بعض برامج الحماية من الفيروسات مع جهاز الكمبيوتر (على سبيل المثال، Microsoft Essentials Security لنظام التشغيل Windows)؛ في حين أن بعض أنظمة التشغيل، مثل تلك الموجودة على أجهزة كمبيوتر قبل أجيد فكر. بها موثوق غير مصادر من الواردة البرامج تثبيت تمنع أمان إعدادات على تحتوي، Apple، تجاوز تلك الإعدادات.

يمكنك أيضاً مراعاة ملحقات المتصفح التي يمكنها، على سبيل المثال، حظر المكونات الإضافية التي تجعل من الصعب على مواقع الويب اكتشاف هويتك أو تتبعك. لكن نفس المكون الإضافي يمكنه حظر وظائف مواقع الويب، مثل إمكانية مشاهدة مقاطع الفيديو. يتوقف قرار تثبيت أو عدم تثبيت ملحقات المتصفح على تفضيلاتك والتنازلات التي أنت على استعداد لتقديمها في ما يتعلق بالأمان على الإنترنت. يمكنك أن تضع في اعتبارك أسئلة مثل، ما مدى انزعاجي عندما يتم تتبعي؟ ما قيمة خصوصيتي؟ إلى أي مدى أريد مشاهدة هذا المحتوى (على سبيل المثال، إذا كان ملحق المتصفح يحظر مكوناً إضافياً يعرض فيديو)؟

أدوات الأمان

الجزء الأول

تفاعل في الفصل

يرجى ملاحظة ما يلي: تمت تغطية جزء من محتوى هذا النشاط في "النشاط رقم 1: المخاطر على الإنترنت". يمكنك الاطلاع على هذه المادة مرة أخرى إذا كنت قد اشتركت بالفعل في النشاط رقم 1 أو تخطيها، حسب احتياجك.

اطرح أسئلة على طلابك

هل تعرف ما إذا كنت آمنًا عند استخدام الإنترنت أم لا؟

أخبر طلابك

من الصعب، إن لم يكن من المستحيل، حماية نفسك بنجاح ضد تلك المخاطر على الإنترنت [تلك الموضحة في القسم السابق]، دون اتخاذ الاحتياطات المناسبة.

كما أن المخاطر الجديدة على الإنترنت لا تتوقف عن الظهور طوال الوقت، لذلك من المهم أن تظل متيقظًا.

اطرح أسئلة على طلابك

ما الذي قد يفعله شخص ما إذا أقنعتك أن موقعه على الويب كان بالفعل موقع ويب مهمًا؟

هناك أدوات يمكنك استخدامها لتجنب تلك المخاطر أو الحد منها. هل يعرف أحدكم أيًا منها؟

أخبر طلابك

يمكن. الإنترنت عبر تمريرها يتم التي البيانات لتشفير الويب مواقع تستخدمه معيار هو HTTPS للتشفير أن يمنع جهة خارجية من عرض البيانات بسهولة أثناء اتصالك. إنه يوفر طبقة أمان إضافية ويمكن استخدامه في أي متصفح من خلال إضافة "https://" في بداية عنوان URL الذي تستخدمه (مثل https://www.mysite.com). لكن، ليست كل مواقع الويب تدعم HTTPS.

1. لا ينبغي إدخال المعلومات الحساسة (مثل كلمات السر ومعلومات بطاقة الائتمان) على صفحات الويب إلا باستخدام البادئة HTTPS://.

2. يمكنك استخدام أدوات البرامج لضمان استخدام HTTPS دائمًا كلما أمكن ذلك.

3. تحتوي معظم المتصفحات الرئيسية على مؤشرات أمان تشبه الأقفال بالقرب من شريط العنوان للإشارة إلى اتصالات HTTPS.

4. لسوء الحظ، لا يضمن HTTPS أنك في أمان حيث يمكن لبعض مواقع الويب الضارة دعم أصالة الويب موقع يكون أن يضمن لا ولكنه الاتصال تأمين على HTTPS يعمل. أيضًا HTTPS

يتم تأمين HTTPS عبر تقنية محكمة تحمل اسم طبقة مآخذ التوصيل الآمنة (SSL)/أمان طبقة النقل. كبير حد إلى الحقيقية المفاتيح مثل تعمل والتي، الرقمي التشفير مفاتيح SSL/TLS تستخدم. (TLS) إذا كتبت سرًا على ورقة لصديقك، فإن أي شخص يجد الورقة يستطيع رؤية سرّك. بدلاً من ذلك، تخيل أنك أعطيت في يده نسخة من مفتاح، ثم أرسلت أسرارك في صناديق مغلقة يمكن فتحها بذلك المفتاح. إذا عثر شخص ما على الصندوق، فسيجد صعوبة في رؤية سرّك دون وجود المفتاح. إذا حاول أحدهم استبدال الصندوق بصندوق مشابه في الشكل، فسوف تلاحظ أن مفتاحك لن يعمل. تعمل TLS/SSL بنفس الطريقة، ولكن مع موقع الويب.

كما ستقوم مؤشرات أمان المتصفح بتوصيل معلومات شهادة التحقق من الصحة الموسّع (EV). يتم منح شهادات EV إلى مواقع الويب التي يتم التحقق من صحة هويتها إلى مرجع مصدق. في المتصفحات، أحيانًا ما يأخذ مؤشر EV شكل اسم الموقع أو الكيان المسجل بجوار شريط العنوان. يتم منح شهادات EV إلى مواقع الويب التي يتم التحقق من صحة هويتها إلى مرجع مصدق. في المتصفحات، أحيانًا ما يأخذ مؤشر EV شكل اسم موقع الويب أو الكيان المسجل بجوار شريط العنوان. إذا كنت تشك في المحتوى الموجود على موقع ويب معين، يمكنك التحقق لمعرفة ما إذا كان عنوان عرض "على النقر طريق عن المتصفح في URL عنوان مع يتطابق الشهادة في الموجود URL الشهادة". [قد يكون من المفيد أن تشرح على شاشة العرض كيفية العثور على "عرض الشهادة". تختلف كيفية انتقالك إلى هذا الخيار حسب المتصفح. على سبيل المثال، على Chrome، ضمن "عرض"، انقر على "المطور" ثم "أدوات المطور". من "أدوات المطور"، انقر على علامة التبويب "الأمان"، ثم "عرض الشهادة".

إلى جانب عدم تشغيل برامج من مصادر غير موثوقة، يمكن أن تمنعك برامج الحماية من الفيروسات من زيارة الصفحات غير الموثوقة وتنزيل البرامج الضارة.

دائمًا ما يحدث "الخداع" في المقام الأول عبر رسالة بريد إلكتروني من مرسل المحتوى غير المهم أو الاحتيالي متظاهراً بأنه جهة شرعية. ومن ثم يطلب منك كلمة السر الخاصة بك، والتي يأمل في أن ترسلها عبر البريد الإلكتروني أو من خلال الدخول إلى موقع ويب مزيف. تستطيع فلاتر المحتوى غير المهم أو الاحتيالي منع ظهور بعض رسائل البريد الإلكتروني هذه في بريدك الوارد. لتحسين فلاتر المحتوى غير المهم أو الاحتيالي، احرص على تمييز أي رسائل بريد إلكتروني مريبة تنتهي في بريدك الوارد كمحتوى غير مهم أو احتيالي.

اطرح أسئلة على طلابك

ما الإجراءات التي يمكنك اتخاذها لمنع نفسك من تنزيل الملفات الضارة إلى جهاز الكمبيوتر عن طريق الخطأ؟

أخبر طلابك

احرص دائماً على عدم الوصول إلى التنزيلات إلا من مواقع الويب الموثوقة. كن حذراً للغاية بشأن فتح مرفقات البريد الإلكتروني التي لا تتعرف عليها والنقر على النوافذ المنبثقة ورسائل الخطأ. يمكنك أيضاً أن تفكر في تثبيت برامج شهيرة لمكافحة البرامج الضارة على جهاز الكمبيوتر.

مشاركة كلمات السر

الجزء الأول

اطرح أسئلة على طلابك

متى تعتقد أنه من المقبول مشاركة كلمة السر الخاصة بك؟

1. تتضمن الإجابات المحتملة الحسابات المشتركة (مثل Netflix).

ما المخاطر التي قد تكون مرتبطة بمشاركة كلمة السر الخاصة بك؟

1. إذا حصل شخص خبيث على كلمة السر الخاصة بك، يمكن اختراق حسابك. تؤدي مشاركة كلمة السر الخاصة بك إلى زيادة احتمال وصول شخص ما إلى حساباتك. إذا كانت كلمة السر نفسها مستخدمة على مواقع ويب أخرى، يمكن للمخترقين الوصول إليها أيضًا.

أخبر طلابك

من المعتاد عدم مشاركة كلمات السر مع أي شخص بالإضافة إلى التطبيقات التي يتم تسجيل الدخول إليها باستخدام كلمات السر تلك. كما هو موضح سابقًا، الخداع هو الاحتيال على شخص ما لمشاركة كلمة السر الخاصة به.

ومع ذلك، قد يطلب بعض الأشخاص كلمة السر الخاصة بك بشكل صريح من أجل الوصول إلى حساباتك، تحت ادعاء أن حسابك قد يكون في خطر. بينما قد تكون نوايا بعض هؤلاء الأشخاص حسنة، مثل صديق يريد مساعدتك في الاطلاع على شيء ما في حسابك يثير حيرتك، إلا أنه ليس من الحكمة مشاركة كلمة السر الخاصة بك، لا سيما إذا كنت تستخدم كلمة السر هذه لحسابات متعددة. إذا كنت تنوي مشاركة كلمة السر الخاصة بك، فتأكد من عدم استخدامها في أي مكان آخر واستخدم برنامجًا لإدارة كلمات السر لمشاركة الوصول.

في بعض الأحيان، قد يكون الأشخاص الذين يطلبون منك كلمات السر الخاصة بك بالغين تعرفهم وتشق بهم، مثل والديك أو معلميك أو صاحب العمل. على الرغم من أنك تعرف هؤلاء البالغين وتشق بهم، إلا أنه عادةً ما تكون تجربة إيجابية للجميع (لك ولهم) أن تجري محادثة حول سبب طلبهم هذا وكيفية تعاملهم مع كلمات السر الخاصة بك. بالنسبة لأي بالغين غير أفراد عائلتك، من الأفضل أن تسألهم مباشرة إذا ما كان هناك قانون أو أي نوع آخر من القواعد يوجب عليك منحهم كلمات السر الخاصة بك.

إن طرح أسئلة مهذبة واضحة حول القوانين والقواعد له أهمية خاصة عندما يأتي طلب كلمة السر من شخص بالغ ليس من عائلتك ولا تعرفه شخصيًا، مثل أحد مسؤولي إنفاذ القانون. إذا طلب منك أحد ضباط الشرطة أو أي مسؤول حكومي آخر كلمات السر الخاصة بحساباتك على وسائل التواصل الاجتماعي، فاحرص على التزام الهدوء والاحترام. اسأل عن سبب هذا الطلب وعن القانون (القوانين) أو القاعدة (القواعد) التي يعتقدون أنها تمنحهم الحق في الحصول على هذه المعلومات منك.

حسب الظروف المحيطة بالطلب المقدم من أحد الوالدين/ولي الأمر أو المعلم أو صاحب العمل أو مسؤول إنفاذ القانون أو مسؤول حكومي أو شخص بالغ آخر، قد تضطر إلى الإفصاح عن كلمات السر الخاصة بك. من الظروف التي قد تجعلك مضطرًا إلى كشف كلمات السر الخاصة بك وجود قانون أو

قاعدة توجب عليك القيام بذلك، أو أن ترى أن الفائدة التي ستنتج من مساعدة مقدم الطلب تفوق مخاطر مشاركة كلمة السر.

إذا وصلك طلب من شخص بالغ للحصول على كلمات السر الخاصة بك، بينما هذا الطلب يجعلك غير مرتاح بأي شكل من الأشكال، فاستشر والدك/ولي أمرك أو أي بالغ آخر موثوق به على الفور؛ ويفضل أن تقوم بذلك قبل أن تضطر إلى الرد على الطلب.

اطرح أسئلة على طلابك

ما الظروف التي في ظلها ينبغي عليك مشاركة كلمة السر الخاصة بك على الإنترنت؟

1. فقط عندما تتم مطالبتك بكلمة السر الخاصة بك على موقع الويب الذي تحاول الوصول إليه. لا تشارك أبداً كلمة السر الخاصة بك في أي مكان آخر، بما في ذلك عبر البريد الإلكتروني، والذي يكون عادة غير مشفر أو آمن.

المهمة

المذكرة

تكليف

قم بتقسيم المشاركين إلى مجموعات مكونة من اثنين أو ثلاثة. وزّع مذكرة "المحتوى غير المهم أو الاحتمالي" المخصصة للمشاركين. بعد ذلك، اطلب من كل مشارك تطوير مخطط انسيابي لثري الآخرين كيف يمكنهم التعرف على المحتوى غير المهم أو الاحتمالي وما إذا كان ينبغي لهم مشاركة معلومات خاصة مع أفراد/مجموعات معينة من الأشخاص.

أخبر طلابك

اقرأ كل السيناريوهات وناقش ما إذا كانت كل رسالة غير مهمة أو احتمالية وما إذا كان ينبغي لك مشاركة المعلومات مع الشخص أو مجموعة الأشخاص في السيناريو أم لا.

تفاعل في الفصل

امنح المشاركين 10 دقائق للقيام بذلك. بعد ذلك، اطلب من المجموعات مشاركة إجاباتهم.

اطرح أسئلة على طلابك

متى ينبغي لك مشاركة كلمة السر الخاصة بك عبر البريد الإلكتروني؟

أخبر طلابك

تنتهج مواقع الويب والشركات ممارسة معتادة تقتضي عدم طلب كلمة السر مطلقاً عبر البريد الإلكتروني. يجب عليك عدم تداول كلمة السر الخاصة بك مع أي شخص بهذه الطريقة، حتى إذا بدا أن المصدر جهة شرعية. البريد الإلكتروني غير آمن على الإطلاق تقريباً.

الجزء الثاني

تكليف

اطلب من المشاركين مغادرة مجموعاتهم حيث إن التدريب التالي سيكون لكل مشارك على حدة.

امنح المشاركين 15 دقيقة لإنشاء المخططات الانسيابية.

أخبر طلابك

الآن، على ورقة، قم بإنشاء مخطط انسيابي لثري الأفراد كيف يمكنهم التعرف على المحتوى غير المهم أو الاحتمالي وما إذا كان ينبغي لهم مشاركة معلومات معينة على الإنترنت مع الآخرين أم لا. قد يكون من المفيد استخدام سيناريو محدد لتأسيس المخطط الانسيابي بناءً عليه؛ إما أحد السيناريوهات المعروضة في المذكرة (إذا اخترت القيام بذلك، يرجى كتابة رقم السيناريو فوق المخطط الانسيابي)، أو سيناريو جديد كلياً! إذا اخترت تصميم سيناريو خاص بك، يرجى وصفه في فقرة موجزة فوق المخطط الانسيابي.

امنح المشاركين 15 دقيقة لإنشاء المخططات الانسيابية.