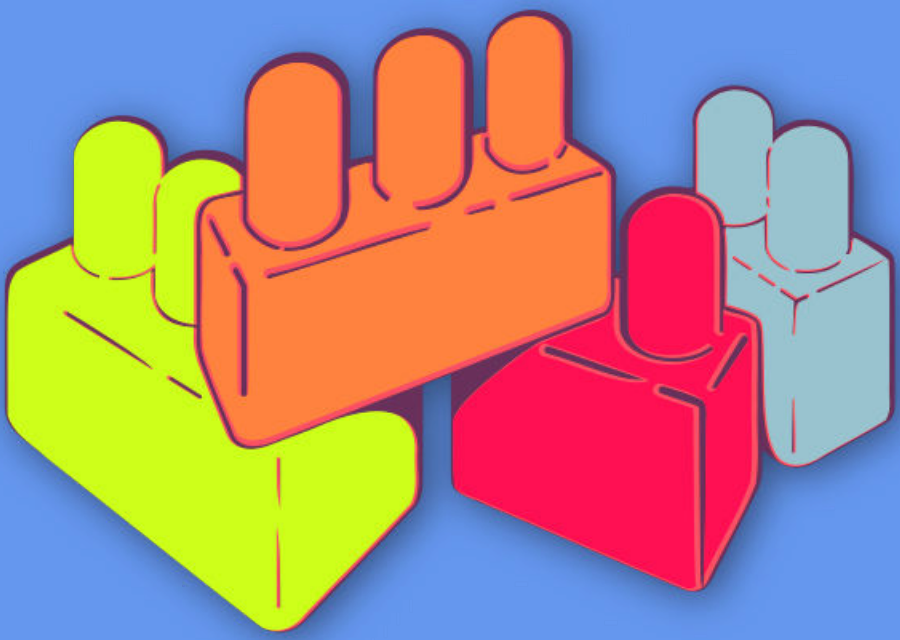

أسس الأمن الرقمي الجولة الأولى

بناء كلمات سرّ قويّة

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

بناء كلمات سرّ قويّة

- **الأهداف:** في هذه الجلسة، ستقمن مع المشاركات بمراجعة تداعيات سرقة كلمة سرّ، وكيفية تعرضها للسرقة عادةً، وكيفية إنشاء كلمات سر أقوى، واكتساب عادات أفضل خاصة بكلمات السرّ.
- **الطول:** 45 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - كيفية حماية حاسوبكن[٢]
- **المواد اللازمة:**
  - جهاز عرض
  - شرائح

[١] https://vrr.im/7ba9
[٢] https://vrr.im/ac95

- أوراق
- إمكانية اتصال بشبكة إنترنت لاسلكي/إنترنت من أجل تنزيل برمجية "كي باس" KeePass

تستند هذه الجلسة إلى وحدة "ممارسات كلمات السرّ الآمنة" الموضوعة من قبل تشيكاي سينكو Cheekay Cinco وكارول واترز Carol Waters وميغان ديبلوا Megan DeBlois لصالح "ليفل أب" LevelUp

إدارة الجلسة

الجزء الأوّل - المقدمة

١. إبدأن هذه الجلسة بطرح الأسئلة التالية على المشاركات:

متى كانت المرة الأخيرة التي قمن بها بتغيير أي من كلمات سرّهن؟

هل لديهن كلمات سرّ مختلفة لحساباتهن المختلفة؟

هل كلمات سرّهن مكتوبة على أوراق ملصقة في مكان ما؟

هل قمن بتخزين كل كلمات السرّ في أحد المستندات؟

هل هواتفهن مزودة بكلمة سرّ؟

الجزء الثاني – ما أهمية كلمات السرّ؟

٢. قبل أن تبدأن بالتحدث عن أهمية كلمات السرّ، أطلبن من المشاركات وضع لائحة بكل المعلومات المحمية بواسطة كلمة سرّ. ما هي المعلومات المتوفرة لديهن على حسابات بريدهن الإلكتروني وحساباتهن على مواقع التواصل الإجتماعي وهواتفهن المحمولة؟ ماذا قد يحصل في حال تمكن شخصٌ آخر من الوصول إلى تلك المعلومات؟

٣. والآن، شاركن مع المشاركات بعض الأسباب التي تبرر أهمية كلمات السرّ:

توفر كلمات السرّ إمكانية الوصول إلى عدد من الحسابات المهمة كحساب البريد الإلكتروني والحسابات المصرفية ومواقع التواصل الاجتماعي، إلخ.

غالبًا ما تحتوي هذه الحسابات على معلومات حساسة، ونحن في الغالب نتصرف على سجيتنا ونتفاعل بتلقائية مع الآخرين بواسطة خدمات رقمية متنوعة ونقوم بتبادل معلومات عديدة حساسة – وقد يتضمن ذلك إرسال رسائل عبر شبكات التواصل الإجتماعي أو إرسال رسالة بريدية إلكترونية أو إجراء علميات شراء على الإنترنت...،إلخ.

الحصول علي كلمات سر الأشخاص الآخرين تسمح بإنتحال صفاتهم/ن الشخصية- فأي شخص قادر على الوصول إلى كلمة سرّ حساب ما، يمكنه فعليًا التصرّف على الإنترنت وكأنه صاحب الحساب.

تمنح كلمات السرّ أيضًا إمكانية الوصول إلى عدد من الأمور الأخرى – نقاط التواصل مع شبكة الإنترنت اللاسلكية وفك كلمات سر الأجهزة المحمولة وتسجيل الدخول إلى الحواسيب وفكّ تشفير الأجهزة والملفات وغيرها.

الجزء الثالث – ماذا قد يحصل في حال تعرض كلمة سرّكم للسرقة؟

٤. في هذا الجزء من الجلسة، سنقوم بتوزيع الأوراق على المشاركات وسنطلب منهن وضع لائحة بكل المنصات التي يتذكرن أنه لديهن حسابات عليها. والآن أطلبن من المشاركات وضع لائحة بما قد يحصل في حال إستحوذ أحدهم على كلمة سرّهن وتمكن من الدخول إلى حساباتهن أو أجهزتهن:

قد تتعرض معلومات أو ملفات مهمة للسرقة (للنسخ) أو للحذف، في حال تعرضها للسرقة، قد لا تلاحظن ذلك مباشرة. وقد تكون المعلومات المسروقة أي شئ مثل مستندات أو ملفات مهمة أو حساسة جدًا أو قائمة جهات إتصال أو رسائل بريدية إلكترونية.

قد تتعرض أموال وحسابات بنكية للسرقة أو الصرف من خلال إمكانية الوصول إلى البطاقات الإئتمانية أو معلومات الدخول على الحسابات المصرفية.

يمكن إستخدام حسابات البريد الإلكتروني أومواقع التواصل الإجتماعي لإرسال الرسائل المزعجة أو لإنتحال شخصيتكن أو شخصية أصدقائكن أو أفراد عائلتكن أو زملائكن.

قد تصبح إمكانية الدخول إلي حساباتكن محتجزة إلى أن تقمن بدفع شكل من أشكال "الفدية" – قد يتضمن ذلك، دفع المال أو منح إمكانية وصول إلى جهات إتصال أو إلى حسابات أخرى.

قد يستخدم شخص ما كلمة السرّ الموجودة بحوزته للوصول إلى إتصالاتكن ونشاطاتكن ومراقبتها من دون علمكن.

قد تؤدي إمكانية الوصول إلى بريدكن الإلكتروني إلى تعرض حساباتكن الأخرى للخطر، إذ تستخدم لإعادة ضبط كلمات سرّ الحسابات الأخرى من خلال طلب روابط إعادة ضبط كلمات السرّ، وفي نهاية المطاف يصبح من المستحيل عليكن الوصول إلى حسابات أخرى كثيرة في حال لم تغيّرن كلمة السرّ.

الجزء الرابع – كيفية تعرّض كلمات السرّ للسرقة عادةً؟

٥. شاركن بعض الممارسات الشائعة التي قد تؤدي إلى حصول أشخاص آخرين على كلمات سرّكن:

حين تشاركنها مع الآخرين، أو تخزنّها بطريقة سهلة الكشف – من ضمن الأمثلة الشائعة، كتابة كلمة السرّ الخاص بتسجيل الدخول إلى حاسوبكن على ورقة صغير ملصقة على الحاسوب نفسه أو بالقرب منه. حين يرى أحدهم كلمة السرّ أثناء إدخالها على شاشتكن ويكتبها أو يحفظها عن غيب.

في حال إستخدام مقدم لخدمة البريد الإلكتروني من دون بروتوكول طبقة المنافذ الآمنة

(https) على مدى الجلسة، أو إستخدامه فقط على صفحة تسجيل الدخول، حيث يعرض ذلك كلمات السرّ والمعلومات الحساسة الأخرى للكشف أمام أي شخص لديه إمكانية الوصول إلى الرابط بعد تسجيل الدخول. يمكن الوصول إلى جهاز يدوياً، أما كلمات السرّ فيمكن الحصول عليها من خلال خاصيتيّ "احفظ كلمة سرّي" "Save My Password" أو "تذكرني" "Remember Me" الموجودتين على مواقع إلكترونية من خلال أي متصفح – يصبح ذلك ممكنًا بشكلٍ خاص في حال لا يتم إستخدام تشفير شامل للقرص على أي جهاز. البرمجيات الخبيثة كبرمجيات "كي لوغر" keylogger التي تعمل على توثيق كل نقرة على لوح المفاتيح على جهازٍ ما ومن ثمّ إرسالها لطرف آخر يريد هذه المعلومات. هذه البرمجيات الخبيثة ليست قادرة على كشف كلمات السرّ وحسب بل قد تصل أيضًا إلى معلومات حساسة أو شخصية. من الممكن أيضًا إختراق المنصات أو نقاط الضعف الموجودة في أنظمتها مما يتسبب بكشف معلومات مستخدميها.

الجزء الخامس – كيف يمكننا جعل كلمات سرّنا أقوى؟

٦. إشرحن للمشاركات أنه في حال إستخدامنا كلمات السرّ ذاتها لكل الحسابات، وتعرّض إحداها للسرقة، ستصبح كل حساباتنا مكشوفة. شاركن بعض ميزات كلمات السرّ الأكثر أمنًا وقوةً مع المجموعة:

الطول: بكل بساطة، كلما زاد طول كلمة السرّ كلما صارت أفضل! يوصى بإستخدام 14 حرفًا كحدٍ أدنى للحصول على كلمات سرّ قوية وفي حال إستخدام 20 حرفًا تصبح كلمة السرّ أقوى بكثير.

التعقيد: إستخدمن كلمة سرّ فيها أحرف وأرقام مع أحرف كبيرة وصغيرة مع تشكيلة غنيّة من الأرقام والرموز.

التغيير المستمر: غيّرن كلمات سركن بشكلٍ دوريّ، لا سيما تلك الخاصة بحساباتكن الحساسة، ولابد من تغييرها في حال وصلتكن رسائل بريدية موثوقٍ بها (ليست رسائل

تصيّد) تذكرن بأن حسابات المستخدمين آخرين وكلمات السرّ لديهم تعرّضت للسرقة.

إستخدام جمل سرّ بدلا عن كلمات السر (تخيلن كلمات سرّ مرتبطة ببعضها ضمن جملة) مثال آخرى عن ممارسة كلمات سرّ قوية – إليكن بعض الأمثلة:

SayNoToSexualHarassmentInMiddleEast ("لا للتحرش الجنسي في الشرق الأوسط")

MyRightToDecentShelter ("حقي في مسكن لائق)

WeDidNotChooseToBecomeRefugeesWeWereForcedToComeHere (لم نختر أن نصبح لاجئين/ات، بل أجبرنا على المجيئ إلى هنا)

٧. أطلبن من المشاركات التفكير لبضع دقائق قبل البدء بإنشاء بعض الأمثلة عن كلمات السرّ القوية. ذكرن المشاركات أنه يتوجب عليهن التفكير في مدى حساسية المعلومات الموجودة في حساب معيّن أثناء تفكيرهن في طول وتعقيد كلمات سرّهن – قد يرغبن في إستخدام أقوى كلمات السرّ لأهم حساباتهن، وفي الوقت عينه إستخدام أقلها تعقيدًا (مع المحافظة على قوتها) للحسابات الأقل أهمية.

المراجع

- https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/