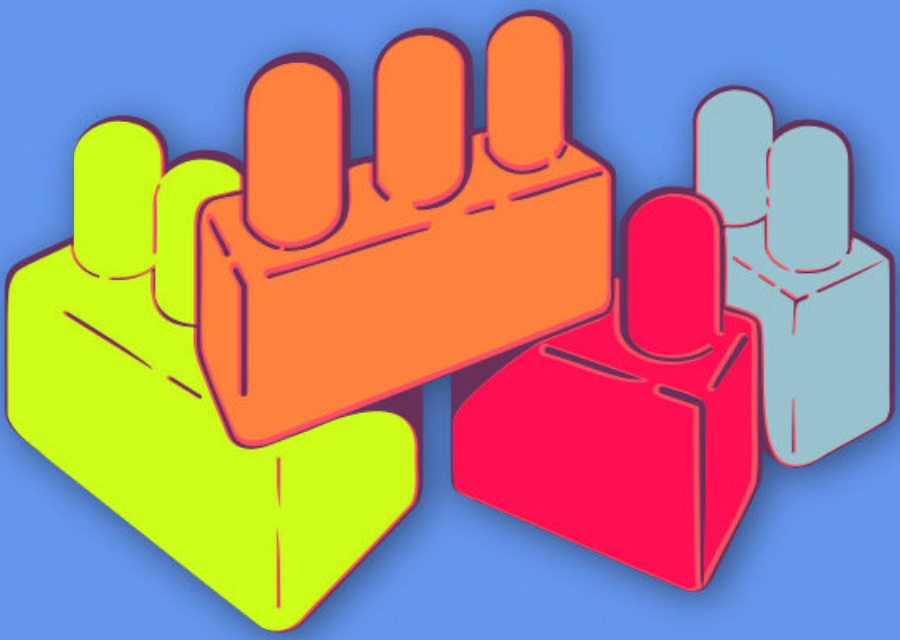
CIBERMUJERES



Principios básicos de seguridad digital 1

Creando contraseñas más seguras

https://iwpr.net/

Índice general

Creando contraseñas más seguras

- **Objetivos:** Revisar vulneración de contraseñas - cómo son comprometidas, cuáles son las implicaciones-, cómo crear contraseñas más robustas y desarrollar mejores hábitos en relación con nuestras contraseñas.
- **Duración:** 45 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Cómo hacer más segura tu computadora[2]
- **Materiales requeridos:**
  - Proyector
  - Diapositivas

[1] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

[2] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

- Papel
- Conexión a Internet/WiFi para descargar KeePass

Esta sesión está basada en el módulo "Prácticas de contraseñas más seguras", desarrollado por Cheekay Cinco, Carol Waters y Megan DeBolis para LevelUp.

Conducir la sesión:

Parte 1 - Introducción

1. Comienza preguntando a las participantes:
    - ¿Cuándo fue la última vez que cambiaste alguna de tus contraseñas?
    - ¿Tienes contraseñas diferentes para cada cuenta?
    - ¿Anotaste tu contraseña en alguna parte como un post-it?
    - ¿Almacenas todas tus contraseñas en un documento sin cifrar?
    - ¿Tus contraseñas están en tu celular?

Parte 2 - Por qué las contraseñas son importantes

2. Antes de empezar a hablar de la importancia de las contraseñas, pide a las participantes enumerar toda la información que es asegurada con una contraseña. ¿Qué información tienen en sus cuentas de correo, cuentas de redes sociales y celulares? ¿Qué pasaría si otra persona pudiera acceder a esta información?
3. Ahora, comparte algunas razones por las que las contraseñas son importantes:

    Las contraseñas brindan acceso a un abanico de cuentas importantes como tu correo, cuentas bancarias, redes sociales, etc.

Estas cuentas suelen contener información muy sensible y nos permiten ser "nosotras mismas" en interacción orgánica con las demás a través de diferentes servicios digitales: enviar un mensaje a través de una plataforma de red social, enviar un correo, realizar una compra online, etc. También pueden darnos la oportunidad de asumir otras identidades - cualquier persona que accede a una contraseña de una cuenta puede, en efecto, simular ser la propietaria de la cuenta. Las contraseñas también dan acceso a otras cosas - puntos de acceso Wi-Fi, desbloquear celulares, iniciar sesión en computadoras, descifrar dispositivos, archivos y mucho más.

Parte 3 - ¿Qué pasa si comprometen tu contraseña?

4. Comparte papeles con las participantes y pídeles hacer una lista de todas las plataformas donde se acuerden que tienen cuentas. Después, que anoten qué pasaría si alguien tuviera su contraseña y pudiera acceder a sus cuentas o dispositivos.

    - Pueden robar (copiar) o borrar información importante o archivos; si esto sucede, quizás no te des cuenta de ello inmediatamente. Podría ser desde documentos y archivos con información confidencial, hasta contactos del directorio y correos electrónicos.
    - Podrían robar o malversar fondos a través del acceso de tarjetas de crédito o cuentas bancarias.
    - Pueden usar cuentas de correo o plataformas de redes sociales para enviar spam o hacerse pasar por ti o tus amigo/as, familiares y compañero/as.
    - O secuestrar tu cuenta a cambio de un "rescate" que podría ser dinero, acceso a contactos.
    - Alguien indebido con una contraseña podría acceder y revisar tus comunicaciones y actividades sin tu conocimiento.
    - A través del acceso de una cuenta de correo, se podría desencadenar un "efecto dominó" y restablecer las contraseñas de otras cuentas a través de links de solicitud, hasta dejar a la persona

legítima fuera de todas de sus cuentas.

Parte 4- ¿Cómo son las maneras más comunes de comprometer una contraseña?

5. Comparte algunas prácticas que pueden resultar en que otras personas tengan acceso a tus contraseñas:
    - Cuando las compartes con otras personas o las almacenas en lugares fáciles de descubrir, por ejemplo, en un post-it pegado cerca de la computadora.
    - Cuando alguien te ve escribiendo una contraseña en tu pantalla y lo anota o se acuerda de ella.
    - Si estás usando un cliente de correo que no utiliza SSL (https) durante toda la sesión (y no sólo en el login), las contraseñas y demás información queda potencialmente expuesta a cualquiera que tenga acceso a tu conexión.
    - Al acceder físicamente a un dispositivo, se puede obtener las contraseñas a través de la configuración "Save My Password" ("Guarda mi contraseña") o "Remember Me" ("Recuérdame") de tu navegador. Esto es aún más probable si el disco de tu dispositivo no está cifrado.
    - Malware, como los keylogger (registrador de teclas), puede registrar cada golpe de tecla de un dispositivo y enviarlo a un tercero, revelando no sólo contraseñas sino potencialmente una cantidad mucho más amplia de información confidencial.
    - Las brechas de seguridad de una plataforma también pueden exponer información sobre sus usuarias.

Parte 5 - ¿Cómo podemos crear contraseñas más robustas?

6. Explica que si utilizan la misma contraseña para todo y esa contraseña es comprometida, todas las cuentas podrán ser vulneradas. Comenta algunas características para contraseñas más seguras y robustas:

Duración: en pocas palabras, ¡cuanto más larga, mejor! 12 caracteres es el mínimo recomendable para contraseñas robustas y 20 es mejor todavía.

Complejidad: utiliza una contraseña alfanumérica, con mayúsculas y minúsculas, una mezcla generosa de números y caracteres especiales.

Cambios frecuentes: cambia a menudo tus contraseñas, particularmente las de tus cuentas más confidenciales y, sobre todo, cámbialas si recibes un correo legítimo y verificado (no phishing) diciéndote que la cuenta de determinado servicio ha sido comprometida.

Utilizar frases enteras: imagina varias contraseñas juntas en una misma "frase"- es un ejemplo de práctica segura de contraseñas. Aquí van unos ejemplos:

NoALaMineriaEnAmericaLatina

AbortoSiAbortoNoEsoLoDecidoYo

NosotrxsNoCruzamosFronterasEllasNosCruzanANosotrxs

7. Propón a las participantes dedicar varios minutos a crear algunos ejemplos de contraseñas robustas. Recuérdales que tengan en cuenta la importancia de la confidencialidad de la información que están resguardando a la hora de escoger la longitud y complejidad de sus contraseñas - quizás quieran utilizar contraseñas más robustas para sus cuentas más importantes y unas menos complejas (pero aún seguras) para sus cuentas sin tanta relevancia.

Referencias

- https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras
- https://securityinabox.org/es/guide/passwords