

Recomendaciones para crear contraseñas robustas

2011-11-01

Recomendaciones para crear contraseñas robustas

Conforme crece la cantidad de información que docentes y estudiantes almacenan en Internet, se vuelve crítico el diseño de estrategias para proteger sus cuentas en los servicios en línea a los que acceden regularmente. La primera de estas consiste en generar contraseñas robustas; encuentre aquí una serie de recomendaciones y reglas sencillas para hacerlo y mantener a salvo sus cuentas en línea de todo tipo de delincuentes.

Conforme crece la cantidad de información que docentes y estudiantes almacenan en Internet, se vuelve crítico el diseño de estrategias para proteger sus cuentas en los servicios en línea a los que acceden regularmente. La primera de estas consiste en generar contraseñas robustas; encuentre aquí una serie de recomendaciones y reglas sencillas para hacerlo y mantener a salvo sus cuentas en línea de todo tipo de delincuentes.

-

RECOMENDACIONES PARA CREAR CONTRASEÑAS ROBUSTAS

imagen

En las noticias de farándula, cada vez se denuncian con mayor frecuencia, casos en los que personajes del mundo del espectáculo son víctimas del robo de sus cuentas de correo o de redes sociales. Estos casos, desafortunadamente, solo son la visible punta de un enorme “iceberg” que incluye cientos de miles de personas que a diario son víctimas de ciberataques a lo largo y ancho del planeta; solo que, por no tratarse de personalidades, los medios de comunicación no los registran.

Y es que el riesgo de convertirse en víctimas de delitos en línea es bastante más grande de lo que el común de las personas puede imaginar. Por lo tanto, es tarea de Instituciones Educativas y docentes, formar a los estudiantes en distintos temas relacionados con Ciudadanía Digital; entre los cuales, uno de los más importantes es el relacionado con la seguridad en ambientes virtuales. Como educadores debemos asegurarnos que los estudiantes comprenden la importancia tanto de proteger su propia privacidad como de respetar la de los demás y que están en capacidad de realizar acciones efectivas en este sentido.

Conforme crece la cantidad de información que ellos almacenan en Internet, se vuelve crítico el diseño de una estrategia para proteger sus cuentas en los diferentes servicios en línea a los que acceden regularmente (correo electrónico, redes sociales, sistemas de almacenamiento de archivos, videos, fotografías, etc). La primera acción y la más efectiva para lograrlo consiste en generar contraseñas robustas que impidan el acceso no autorizado a sus cuentas.

Aunque esta recomendación suena supremamente lógica, la mayoría de las personas la pasan por alto ya que no se sienten cómodas creando contraseñas robustas que pueden ser complicadas de imaginar y, en muchos casos, difíciles de recordar. A continuación ofrecemos una serie de recomendaciones y reglas sencillas que contribuyen a mantener a salvo, de todo tipo de delincuentes, las cuentas en línea [1]:

TAMAÑO: Las contraseñas largas son difíciles de descifrar. Aunque no hay una regla fija en cuanto al tamaño, procure crear claves tan largas como lo permita el servicio en línea en el que estas se utilizarán. Algunos sitios exigen a sus usuarios contraseñas con un tamaño mínimo de 10 caracteres; sin embargo, otros no establecen al respecto ninguna restricción y las personas por lo regular toman el camino fácil y crean contraseñas muy cortas (4 a 6 caracteres).

[John Pozadzides](#), experto en estándares de Internet, resume en la siguiente tabla el tiempo que tarda un computador actual en probar todas las combinaciones posibles en función de la cantidad de caracteres que tiene una contraseña:

<http://www.linkedin.com/in/johnpozadzides>

VARIEDAD: Mezclar letras, números y símbolos hace que las contraseñas sean más seguras (ju@N_ru1fO). Cuando un sitio no permita el uso de símbolos (% , & , \$; # , etc), una buena práctica consiste en combinar números, letras mayúsculas y minúsculas (juaNru1fO, JUANru1fo, etc). Varios sitios ofrecen herramientas para determinar qué tan robusta es una contraseña. Uno de ellos es <https://www.grc.com/haystack.htm> “[How Big is your Haystack?](https://www.grc.com/haystack.htm)”:

<https://www.grc.com/haystack.htm>

También Microsoft ofrece un [comprobador de contraseñas](#) que no recopila ni trasmite información:

<https://www.microsoft.com/es-es/security/online-privacy/password-checker.aspx>

PATRONES: Utilizar un patrón del teclado facilita recordar una contraseña; por ejemplo, una V empezando con el número tres: 3eDCft6; o una W: 3eDCft6yHNJi9. Otra forma consiste en cambiar una letra por un número y completar 12 caracteres con símbolos; por ejemplo: Fau5to%%%%%%%%%, Rut3ador!!!!!!!!!!!!, G4to****, etc.

INFORMACIÓN PERSONAL: No es buena idea incluir en las contraseñas información personal identificable (nombre de la persona o de un familiar, nomenclatura de la calle, nombre de la mascota, modelo de carro, fecha de nacimiento, etc). En lugar de esto, utilice el título de una canción o de un libro, una frase literaria o el nombre de un autor. Por ejemplo, “ElBluesDelEsclavo”, “ComoAguaParaChoco1ate”, “LaLit3ratura3sM3ntirBi3nLaV3rdad”, “Ju4n_C4rlos_Onetti”, etc.

PALABRAS COMUNES: No es buena idea utilizar palabras comunes, pues los delincuentes a menudo ingresan de forma automática las palabras de un diccionario para intentar descubrir una clave. Sin embargo, se pueden usar palabras comunes, pero deletreándolas al revés o mezclando mayúsculas y minúsculas con números. Por

ejemplo:

Ana María à “a1raManA” mayúsculas iniciales y se cambia la i por un 1.

- LuMaJu0Ma à Luisa, Mary, Juan y 0 Mascotas = miembros de la familia.
- RobDlaHug72 à Roberto, Diana, Hugo y 72 (resultado de la suma de edades).

ACRÓNIMOS: Uno de los métodos más utilizados para crear contraseñas robustas fáciles de recordar es mediante acrónimos. Por ejemplo, una frase célebre como “A Caballo Regalado No Se Le Mira El Diente” puede convertirse en la siguiente contraseña “ACRNSLMED”. Para complejizarla se pueden sustituir algunas letras por símbolos y números (A por @ y 3 por E): “@CRNSLM3D”. Adicionalmente, le intercalamos mayúsculas y minúsculas: “@CrNsLm3d”.

Otros ejemplos:

- Mis Dos Hermanos y Una Hermana à M2hy1H@@@@
- Mi cumpleaños es el 9 de abril à Mcee9dA%%%%%%%%

DIFERENTES CUENTAS: No aconsejan los expertos utilizar la misma contraseña en varios servicios en línea. Sin embargo, resulta poco práctico y, dependiendo del número de cuentas, inviable, crear una contraseña para cada una. Una opción puede consistir en crear una única contraseña robusta y a esta agregarle un símbolo más la inicial del servicio en la que se utilizará. Por ejemplo:

- Gmail à @CrNsLm3d%g
- Hotmail à @CrNsLm3d%h
- Wordpress à @CrNsLm3d%w

- Blogger à @CrNsLm3d%b
- Facebook à @CrNsLm3d%f

GUARDARLAS EN SITIO SEGURO: Todas las recomendaciones apuntan a que las contraseñas no deben escribirse en ninguna parte; lo ideal es guardarlas en la memoria. No obstante, esto puede no resultar práctico. Si decide escribir las contraseñas en algún lugar, guarde la anotación lejos del computador y en un lugar en el que otras personas no lo puedan encontrar fácilmente. En todo caso, nunca comparta sus contraseñas con otras personas y evite a toda costa guardarlas en un archivo de texto del teléfono celular (móvil).

Una técnica para generar contraseñas cortas pero robustas es la propuesta por [Labnol](http://www.labnol.org/software/write-passwords-safely-on-paper/12972/) que se basa en una tabla de códigos como la siguiente, la cual se puede imprimir y tener siempre a mano:

<http://www.labnol.org/software/write-passwords-safely-on-paper/12972/>

Por ejemplo, una palabra sencilla de recordar como “cosa” equivaldría a “T9OeTyJ8”:

- Primera letra c = T9
- Segunda letra o = Oe
- Tercera letra s = Ty
- Cuarta letra a = J8

Si se desea que la contraseña sea más robusta, podemos agregar al final de este código otra palabra fácil de recordar como por ejemplo “cOIOMbia” =
T9OeTyJ8cOIOMbia

Recuerde que usted puede crear fácilmente con una Hoja de Cálculo su propia tabla de códigos. Descargue un archivo XLS para realizar esta tarea haciendo [clic aquí](#).

CÁMBIELAS A MENUDO: Una buena práctica consiste en cambiar las contraseñas cada 2 o 3 meses. Esto es particularmente importante para las cuentas financieras o de sitios de comercio en línea en las que se graba el número de la tarjeta de crédito.

NO UTILICE LA MISMA CONTRASEÑA PARA TODO: Nunca se debe utilizar la misma contraseña para diferentes cuentas (correo, redes sociales, cuenta bancaria, etc). Una vez que alguien descubre una contraseña, puede probarla con diferentes cuentas.

Con el fin de hacer más práctico atender este punto, se puede usar una tabla como la incluida en la sección “Guardarlas en sitio seguro” de este mismo documento y utilizar los cinco primeros caracteres de los sitios para los cuales debemos crear contraseñas. A las contraseñas resultantes, se les puede agregar una palabra como “cOIOMbia” y quedarían las siguientes claves:

- Gmail = FsX4PwRwO3cOIOMbia
- Hotmail = FsOeG1M5MqcOIOMbia
- Wordpress = UjOeTyD9HycOIOMbia
- Facebook = WnFoSaÑtMqcOIOMbia
- Twitter = JnHnFhZpQncOIOMbia

RECORDAR CONTRASEÑAS: La mayoría de los sitios ofrecen un sistema para ayudarle a recordar su contraseña y para ello le hacen una pregunta que se supone que solo el dueño de la cuenta puede responder. La mayoría de esas preguntas se basan en información pública como nombre de la mamá, nombre de la mascota, equipo de fútbol, etc. Una buena idea consiste en utilizar una respuesta falsa, pero que usted recuerde fácilmente (el nombre de la mamá de un amigo o el nombre del equipo de fútbol rival, etc).

INGENIERÍA SOCIAL: Cada vez es más frecuente que los delincuentes no se molesten en utilizar recursos técnicos para robar una contraseña. La llamada ingeniería social se sustenta en el principio que dice que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, los delincuentes utilizan el teléfono o Internet para engañar a los usuarios, fingiendo ser, por ejemplo, un empleado de algún banco, un amigo, un compañero de estudio, un técnico o un familiar y en su lugar, proceden a engañar al usuario para que sea él mismo quien voluntariamente suministre al delincuente la clave.

NOTAS DEL EDITOR:

[1] La mayoría de las recomendaciones están basadas en las que plantea Nancy Muir en el documento

http://www.dell.com/downloads/global/solutions/public/white_papers/guide_to_teaching_cyber_saf

"[Guide to Teaching Cyber Safety to the Digital Generation](#)"; documento publicado por Wiley Publishing Inc, con el auspicio de las compañías Dell y Microsoft.

CRÉDITOS:

Documento elaborado por Eduteka con información proveniente de las siguientes fuentes:

- [Aprenda a proteger sus cuentas en Internet](#); Iván Luzardo, Revista Enter (2011).
- [Educación del carácter en la era digital](#), Jason Ohler (2011).
- [Ciudadanía Digital](#); Mike S. Ribble, Gerald D. Bailey & Tweed W. Ross, Revista Leading & Learning with Technology, números 1 y 2 del Volumen 32 (2004).
- [Creación de contraseñas robustas](#); Red Hat (2005).
- <http://www.seguridad.unam.mx/descarga.dsc?arch=1366> ¿Cómo crear contraseñas seguras?; Departamento de Seguridad en Computo/UNAM-CERT.

- [Ingeniería Social](#); Wikipedia (2011).
- [How Strong Are Your Passwords?](#); Noemi Twigg, Forever Geek (2010).
- [Contraseñas fáciles de recordar pero robustas](#); Fausto Cepeda, Hacking (2011).
- [Compruebe su contraseña](#); Microsoft (2011).
- [Keep Your Passwords Safe on a Piece of Paper](#) (2010).
- [Contraseñas, cuestión de conciencia](#); Jorge Alejandro Mieres, Seguridad Digital (2007).

*Publicación de este documento en EDUTEKA: Noviembre 01 de 2011.

Última modificación de este documento: Noviembre 01 de 2011.*