Seguridad en sus Contraseñas

Últimos Consejos para la Seguridad de sus Contraseñas

Las contraseñas! las claves de la vida moderna. Parece que no podemos ir a ninguna parte ni hacer nada en estos tiempos sin una contraseña. En nuestros trabajos necesitamos una contraseña, nuestros autos requieren contraseñas, inclusive nuestro compañero fiel “el celular” también podría necesitar de una contraseña. El tener una contraseña única es tentador para tener “llave maestra” que facilite nuestras vidas, si bien el hecho de generar una contraseña puede ser muy fácil, pero sin duda alguna no es muy seguro y corremos el riesgo de poner en peligro nuestra informacion personal si alguien utiliza nuestra “llave maestra”

Esto nos trae a la mente el tipito castillo antiguo con un anillo gigante repleto con las llaves de todas las habitaciones. No sería una gran carga para llevar a todas partes? No sería mejor tener una llave maestra que abra todas las habitaciones?, Si, sí, pero una vez la llave maestra sea robada todo el castillo quedaría abierto.

Usted lo ha escuchado una y otra vez…”Utilice una contraseña segura”. Pero las contraseñas seguras son difíciles de recordar y no hay nada más frustrante que quedar bloqueado por su cuenta por haber escrito una contraseña incorrecta 5 veces. Todos sabemos crear una mejor contraseña que por ejemplo: “contraseña1” (no?). Pero el problema es mucho más importante que eso.

Elegir una contraseña segura

En estos días un determinado software le dirá, a medida que escribe una contraseña, lo fuerte que es. Incluso le puede dar

una luz indicadora de color rojo-amarillo-verde. Esto es especialmente cierto con el software que tiene que ver con el acceso a los elementos importantes de su negocio, al igual que su servidor de alojamiento web. Asegúrese de llegar a la contraseña más diversa que pueda crear. Cuando una página web o el software crea una contraseña para usted y aparece esto: «% Y6tff rJ», no lo cambie a nombre de su hijo. Siempre incluya números, letras minúsculas / mayúsculas y símbolos en la contraseña. Trate de hacer que su contraseña sea de al menos 8 caracteres de longitud. Si tu mamá puede adivinar la contraseña, también puede hacerlo un hacker. Evite los nombres o palabras del diccionario como por ejemplo "12345".

Recordar una contraseña segura

Como podríamos recordar una contraseña como «¿P89 # r76b», Utilice un mantenimiento de contraseñas para llevar un registro de sus contraseñas para usted. "Guardianes de Contraseña" le permitirán el acceso a todas las contraseñas al conocer sólo una contraseña. (Aha! Hay una llave maestra!) Asegúrese de realizar copias de seguridad del mantenimiento de contraseñas para que no se pierda la información importante. En una emergencia, usted puede elegir la opción «Contraseña olvidada» en la mayoría de los programas y aplicaciones basadas en web.

Protección de su contraseña

– Vamos a empezar con lo básico. Nunca escriba su contraseña en una hoja de papel. Nunca guarde su contraseña en un archivo llamado Passwords.docx. Si usted tiene que dar su contraseña a un compañero de trabajo, amigo o técnico de computadoras, asegúrese de cambiar pronto después de que haya terminado. Nunca ponga una etiqueta con su contraseña en la parte inferior del teclado. Incluso los más brillantes pueden accidentalmente anunciara su contraseña. Las estafas de phishing se crean específicamente para ayudarle a entregar su contraseña. Si algo le parece raro, como hacer clic en un

enlace en Twitter, y luego Twitter le pide que vuelva a entrar, y luego cerró la ventana, podría ser una estafa. Si usted ha tenido un incidente con su contraseña, cámbiela inmediatamente. Las empresas comprometidas recientemente incluyen Yahoo!, Battle.net y LinkedIn. Es una buena idea cambiar las contraseñas de sus cuentas cada pocos meses de todos modos.

Diversificación en las contraseñas

– Digamos que tienes una contraseña complicada realmente grande como «B7YYm $ 0T4» y la está usando como su contraseña de Twitter, contraseña bancaria, contraseña de equipo y para todo lo demás imaginable. Esta es una mala idea. Si un hacker acceda a su Twitter, puede ir y tener acceso a cualquier otra entidad que hace negocios en línea. Usar la misma contraseña también puede poner su empresa en riesgo.

«Siempre es una buena estrategia utilizar contraseñas diferentes para sus cuentas personales y su identidad corporativa. Además de las estrategias mnemotécnicas para recordar contraseñas y la creación de contraseñas seguras, las aplicaciones que utilizan como KeePass o directorio central de contraseña puede ser de gran ayuda si usted tiene demasiadas contraseñas de manejar. Usar la misma contraseña para su cuenta de la empresa como sus cuentas personales sólo pone su organización en riesgo «-. Ray F., Vicepresidente de Seguridad en Redes para HostDime

Con la erupción de los intentos de hacking de las principales entidades en línea recientemente, una contraseña segura es más importante que nunca. Mantener tu contraseña protegida y diversificado es tan importante como el cerrojo de su puerta.