FUNDAMENTOS DE LA SEGURIDAD DE DATOS DE PAGO

Contraseñas seguras

¿CUÁL ES EL RIESGO?

81%

sobre las vulnerabilidades relacionadas con hackeos a través de contraseñas robadas o débiles

(Informe de investigación de Verizon sobre vulnerabilidad de datos de 2017)

El uso de contraseñas débiles y predeterminadas es una de las causas principales de compromiso de datos de las empresas.

Las contraseñas son esenciales para la seguridad de la computadora y los datos de pago. Para que sean eficaces, deben ser seguras y actualizarse con frecuencia.

Con frecuencia, el equipo computacional y software listos para usar (incluyendo las terminales de pago) vienen con contraseñas predeterminadas por el proveedor o preestablecidas como "contraseña" o "administrador", que son muy conocidas y los delincuentes sacan provecho de ello con facilidad.

Contraseñas predeterminadas normales que DEBEN cambiarse:

[ninguno]	guest
[nombre del producto/ proveedor]	manager
1234 o 4321	pass
access	password
admin	root
anonymous	as
database	secret
	sysadmin
	user

PRÁCTICAS RECOMENDADAS PARA LAS CONTRASEÑAS

Para minimizar el riesgo de compromiso, los negocios deben cambiar las contraseñas predeterminadas por el proveedor por unas más seguras y nunca compartirlas: cada empleado debe tener su propia ID y contraseña de inicio de sesión.

Cambie sus contraseñas con frecuencia

Trate su contraseñas como si fueran cepillos de dientes. No permita que nadie más las use y cámbielas cada tres meses.

No comparta sus contraseñas

Insista para que cada empleado tenga su propia ID y contraseña de inicio de sesión: ¡nunca las comparta!

Cómo dificultar que adivinen su contraseña

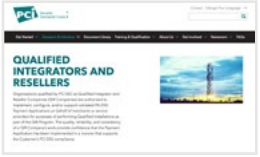
Las contraseñas más comunes son "contraseña", "contraseña1" y "123456". Los hackers introducen contraseñas que se adivinan con facilidad, porque la mitad de la gente las utiliza. Una contraseña segura tiene siete o más caracteres y una combinación de letras mayúsculas y minúsculas, números y símbolos (como !@#$&*). Una fase que integra números y símbolos puede ser una contraseña segura: la clave es elegir una frase con un significado especial para usted de forma que la recuerde con facilidad, como su pasatiempo favorito, por ejemplo (como ¡Am0pesc4rtruch4s!).

RECURSOS

Visite **pcissc.org/Merchants** donde encontrará más recursos

Los vendedores y proveedores de servicios pueden ayudar a las empresas para que identifiquen las contraseñas predeterminadas y que las cambien.

La Guía de pagos seguros Guía de pagos seguros proporciona a las empresas la información básica para protegerse contra el robo de datos de pago.



La lista de integradores calificados de PCI y revendedores (QIR) es un recurso que las empresas pueden aprovechar para encontrar instaladores de servicios de pago que hayan recibido capacitación del PCI Security Standards Council sobre contraseñas seguras y otros fundamentos de seguridad de datos de pago.

Vea este video rápido animado para conocer la manera en que las empresas pueden minimizar las posibilidades de una vulnerabilidad a sus datos cambiando contraseñas predeterminadas del proveedor por unas más seguras y nunca compartir las contraseñas.

PCI Security Standards Council