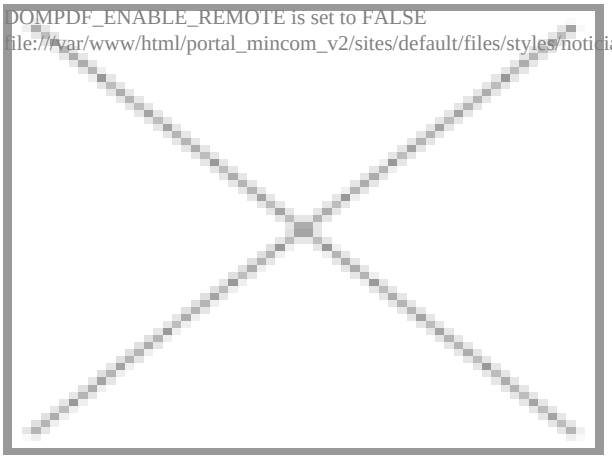

Source:
Diario TI

Las contraseñas son vestigios de los primeros días de la era de la información. Son controles superficiales que no hacen más que crear la ilusión de seguridad – hasta que ocurre un ataque que la elimine-. Las contraseñas cortas son fáciles de recordar y fáciles de descifrar; las contraseñas largas son más difíciles de recordar, pero sólo un poco más difíciles de desarticular, sobre todo con el poder de la informática que se maneja hoy en día y las herramientas de cracking especializadas.

Sin embargo, muchas organizaciones todavía almacenan passwords de empleados y clientes en algún documento, lo que significa que si el archivo es robado, en realidad no importa cuantos caracteres especiales se utilizaron. Se dice que son más seguras las contraseñas más largas y las frases con letras mayúsculas y minúsculas, números y caracteres especiales. Y se podría argumentar que esto es cierto, pero también se podría argumentar que son sólo un poco mejores, y que esta ligera diferencia se está convirtiendo en algo totalmente irrelevante. El volumen, la velocidad, la variedad y el vigor de los atacantes maliciosos; como ciberdelincuentes con actividades lucrativas, activistas con motivos políticos, y los estados-naciones con su interminable suministro de herramientas, malware y técnicas, hacen que tratar de proteger las contraseñas sea una responsabilidad abrumadora para cualquier organización.

Sería como tener un guardia de seguridad en un banco tratando de detener un ejército invasor con nada más que un par de sacos de arena y un revólver.

Parece que con los avances tecnológicos, descubrimos mayores fallos en cuanto a la protección de nuestra información y lo hacemos de manera más lenta.

Existen algunas buenas prácticas que podemos utilizar para mantener nuestras cuentas seguras:

1) Autenticación robusta

Utiliza soluciones de autenticación más robustas que aprovechen las capacidades de tu Smartphone (la aplicación Google Authenticator para Gmail es una buena recomendación), impresiones biométricas y de

reconocimiento de voz/ facial.

2) Permite la comunicación entre dispositivos

Cuando eso no es posible, utiliza una herramienta de gestión de contraseñas que se sincronice entre todos tus dispositivos. Ésta creará contraseñas únicas, y diferentes que nunca necesitarás recordar y serán fáciles de cambiar con frecuencia para casi todos tus sitios favoritos.

3) Cuidado con el phishing

Si recibes un correo electrónico de una “empresa” o persona que te pide que alteres tu cuenta, nunca hagas clic en el enlace. Hay una buena probabilidad de que sea una especie de ataque de phishing. Si la URL del enlace parece que podría ser legítima, pero no estás seguro, navega directamente al sitio para confirmar su validez.

Desafortunadamente, demasiadas personas simplemente ignoran los signos de un ataque o el ser víctimas de una estafa o robo de datos. Incluso sin ninguna acción por parte del usuario final, y utilizando aparentes contraseñas “fuertes”, la información de la persona puede ser robada.

Las empresas que detecten alguna vulnerabilidad o ataque a sus cuentas deberán resetear sus passwords en automático, avisar a los usuarios por qué se realizó este cambio de contraseñas e idealmente utilizar herramientas de seguridad más robustas en el futuro.

Links
[1] http://diarioti.com/adios-a-la-era-de-las-contrasenas/92548