¿MANEJO DE CONTRASEÑAS SEGURAS?

Las contraseñas son las llaves que dan acceso a nuestros servicios y por ende a nuestra información personal por lo que si alguien las consigue puede comprometer nuestra privacidad, pudiendo entre otras cosas: publicar en nuestro nombre en redes sociales, leer y contestar a correos electrónicos haciéndose pasar por nosotros, acceder a nuestra banca online, etc.

En el control de accesos el nombre de usuario nos identifica y la contraseña nos autentica (con ella se comprueba que somos quienes decimos ser). Todo sistema de autenticación de usuarios se basa en la utilización de uno, o varios, de los siguientes factores:

¿Qué técnicas utilizan los ciberdelincuentes para ataques de contraseñas? Esta situación trae como consecuencia que ataques cibernéticos de diversos tipos tomen lugar. Algunas de las técnicas más utilizadas por ciber-atacantes son:

Ataques de fuerza bruta Los atacantes prueban millones de combinaciones de contraseñas básicas (en cuestión de segundos) hasta que dan con la indicada y logran acceder a los medios internos de una compañía.

Ataques por diccionario A diferencia del ataque por fuerza bruta, el atacante trata de adivinar las contraseñas con base en palabras de un diccionario en cualquier idioma.

Los ataques del tipo Pass-the-Hash (PtH) A través de este método, un hacker es capaz de violar el Single Sign On (SS0) por medio de los protocolos NTLM, Kerberos y de otros protocolos de autenticación. Estos ataques son más comunes en dispositivos Windows.

Ataques del tipo Pass-the-Ticket (PtT) y Golden Ticket Este tipo de ataques son una variación del PtT y consisten en el robo de la cuenta krbtgt en un controlador de dominio que codifica los tickets que garantizan tickets (TGT).

Ataques a contraseñas con Ingeniería Social. - Son mejor conocidos como phishing y spear phishing, e implican engañar a las personas para que revelen informaciones que pueden utilizarse para conseguir acceso.

Siete malos hábitos al generar una contraseña

1. La clave más recurrente entre los usuarios en Internet es 123456, evite usar claves que sean este o cualquier otro conjunto de números consecutivos.
2. tener una misma clave para todo hará que el ciberdelincuente tenga acceso a todos sus sistemas e información personal más fácilmente.
3. El número telefónico, la cédula de identidad, su nombre o su fecha de nacimiento no son buenas alternativas para una clave.
4. Tener dos o tres claves y cambiarles el orden para usarlas en diferentes plataformas deja expuesta su seguridad.

5. No compartir con nadie el nombre de usuario y contraseña, nunca envíe estos datos por medios digitales, como WhatsApp, Facebook Messenger o correo electrónico, es mejor hacerlo vía telefónica. Luego de esto es aconsejable cambiar las contraseñas.
6. Es recomendable cambiar la clave mínima una vez al año, de hecho, varios sistemas ya lo exigen y obligan al usuario a renovar su contraseña cada 6 o 12 meses.
7. No es recomendable guardar las contraseñas en los gestores que ofrecen los navegadores (por ejemplo, Google Chrome) porque es entregar estos códigos secretos a empresas tecnológicas que han sido cuestionadas por el manejo que les dan a los datos de sus usuarios.

CONSEJOS PARA MANEJAR TUS CONTRASEÑA

1. Cambia de contraseñas periódicamente Cambiar nuestras contraseñas siempre será una buena práctica, en caso de que alguna de las que usamos sea capturada por un tercero, el hecho de cambiarlas con regularidad hará que la que fue comprometida sea inservible a quién la capturó.
2. Combinaciones alfanuméricas. - Utilizar combinaciones de letras, números, mayúsculas, minúsculas, símbolos, etc., es la mejor elección.
3. Procura que la longitud sea mayor. - En el caso del uso de contraseñas, esto es más que real. Entre más larga, compleja y combinada sea tu contraseña, más robusta y fuerte será.
4. No uses palabras en otros idiomas o reversibles. - Muchos ataques de fuerza bruta se adaptan para convertirse en ataques de diccionario, es decir, que con el objetivo de tratar de hacer más corto el tiempo de adivinar una contraseña y con base en estadísticas, atacantes informáticos suelen cargar diccionarios con palabras ya existentes
5. Usar frases para recordar la contraseña. - Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc.

Referencia: Boletín No. 8 -Ciberseguridad Ministerio de Telecomunicaciones y de la Sociedad de la Información