Si piensas en las contraseñas que usas, ¿crees que serían fáciles de hackear? Según varios estudios, muchos de los usuarios de internet en casa o en el trabajo no usamos contraseñas suficientemente seguras.

Esto se convierte en una oportunidad para los hackers, que cada vez usan técnicas más sofisticadas y pueden descifrar contraseñas más fácilmente. Tan solo en 2021, los ciberataques aumentaron un 150%, y se espera que en 2022 sigan creciendo.

Las malas prácticas de los usuarios sumado a la mayor habilidad de los hackers, hacen que los hackeos sean un negocio cada vez más rentable y que los ciudadanos y las compañías deban aprender a proteger sus contraseñas.

Malas prácticas de los usuarios al crear contraseñas

Los datos no dejan lugar a dudas: solemos poner contraseñas fáciles de recordar, independientemente de su facilidad para ser hackeadas. Además, es común en muchos usuarios usar la misma contraseña para varias cuentas.

Nordpass ha elaborado un informe sobre las contraseñas más usadas y los resultados son sorprendentes. La contraseña más usada mundialmente se ha llegado a usar hasta 103.170.552 veces. Y no solo eso, si no que esta contraseña es simplemente: 123456. Como usuarios de internet, deberíamos tomar consciencia de la importancia de la ciberseguridad y proteger mejor nuestras contraseñas.

Phishing: el principal método para hackear los correos electrónicos

El phishing es la manera más usada por los hackers para intentar conseguir las contraseñas de los correos electrónicos. Al acceder al correo electrónico, los hackers son capaces de sacar multitud de información. Podrían acceder a los datos de nuestra cuenta bancaria, nuestras compras online o nuestras suscripciones, como las de las plataformas de streaming.

Además, recordemos que muchos usuarios repiten sus contraseñas, por lo que si descifran la contraseña del correo electrónico podrían también acceder a otras plataformas online.

¿Cómo funciona el phishing?

La técnica del phishing consiste en crear un mail haciendo ver que proviene de una fuente fiable. En ellos, se incluye alguna llamada a la acción, como por ejemplo, consulte aquí su pedido u obtenga más información. Si el usuario hace click, le llevará a un enlace malicioso y el hacker podrá intentar descifrar su contraseña.

¿Cuáles son los correos de phishing más comunes?

Los hackers cada vez sofistican más sus métodos de phishing y sus mails son más creativos. Sin embargo, sí que podemos identificar tres tipos de correos electrónicos de phishing bastante comunes:

- Verificación de cuenta: se hacen pasar por una empresa en la cual el usuario tenga una cuenta, como por ejemplo Amazon, y avisan de que debe entrar al enlace para verificar su cuenta. Además, suelen decir que si no se entra en el enlace se desactivará la cuenta, de esta manera presionan al usuario.
- Spear phishing: esto suele ocurrir en las empresas, los hackers se hacen pasar por un compañero replicando su mail y envían un enlace malicioso a alguien interno de la compañía.
- Envío de factura falsa: otra técnica frecuentemente utilizada es la de hacerse pasar por una compañía de internet que vende online. Suelen enviar un correo electrónico con un enlace malicioso para consultar la supuesta factura, así consiguen obtener los datos del usuario hackeado.

3 métodos para crear contraseñas seguras

Lo mejor que podemos hacer para evitar estos hackeos es establecer contraseñas que sean

difíciles de descifrar. Para ello, los expertos recomiendan usar un mínimo de 10 caracteres constituidos por mayúsculas, minúsculas, números y caracteres especiales. Cada contraseña debe ser usada sólo para una cuenta y ser cambiada cada mes.

Teniendo en cuenta estos criterios, puede parecer que crear contraseñas seguras es complicado. Por eso, te contamos 3 métodos para que crees contraseñas fáciles de recordar y difíciles de descifrar

1. Acorta palabras: puedes crear una frase y eliminar las primeras o últimas letras para crear combinaciones que sean seguras. Por ejemplo: de la frase me gusta viajar en avión o en coche, podríamos eliminar las dos primeras letras de cada palabra y resultaría en : sta ajar ión che.
2. Cambia las vocales. Para este método, recomendamos usar frases sin sentido, para así añadirle dificultad a ser descifradas. Podríamos usar: un ordenador está flotando en una ciudad y cambiar todas las «o» por «a» y las «u» por «i». El resultado final sería: in ardenadar esta flatanda en una ciidad.
3. Usar los códigos de países para crear combinaciones. Si usas los códigos ISO de los países, podrás crear combinaciones que sean fáciles de recordar. Por ejemplo, si usas México, Reino Unido, Francia, Alemania, Japón puedes crear la siguiente contraseña: mex gbr fra deu jpn

Recuerda que con el resultado creado con todos estos métodos, luego deberás añadirle mayúsculas, números y caracteres especiales para que sean aún más seguras.

Fuente: https://holahorro.mx/blog/ciberatques-contrasenas-seguras/