Errores a corregir en el Día Mundial de la Contraseña

Todos los días deberíamos aplicar prácticas de seguridad férreas en internet que eviten la acción de los ciberdelincuentes. Pero hoy más que nunca, en pleno 4 de mayo con la celebración del **Día Mundial de las Contraseñas**, los expertos del sector nos hacen reflexionar.

"Hay dos malos hábitos relacionado con el uso de contraseñas que todos debemos mejorar", determina Eduard Meelhuysen, director de la firma de seguridad Bitglass en EMEA.

"En primer lugar, muchas personas utilizan la misma contraseña en las cuentas de trabajo y en sus aplicaciones personales tales como los bancos y las redes sociales", apunta Meelhuysen. "Usar la misma contraseña es sin duda una mala idea, ya que una intrusión en cualquiera de estos sitios puede tener un efecto dominó en todos los demás inicios de sesión". Este representante de Bitglass añade que "el uso de las mismas contraseñas o incluso similares en el trabajo puede agregar un multiplicador a ese efecto dominó, poniendo toda una red de la empresa en riesgo". Por eso, **"debemos crear contraseñas únicas** para las cuentas, especialmente aquellas relacionadas con el trabajo".

¿Cuál es el segundo aspecto a mejorar? La composición de la propia contraseña, que no tiene que contener datos personales que se puedan adivinar con facilidad y que debe combinar diferentes caracteres, letras, números y signos.

"Los hackers son conocidos por utilizar algo llamado 'brute-force attack'", esto es, un ataque de fuerza bruta o "programa informático que utilizan para comprobar sistemáticamente muchas combinaciones de palabras y números comunes, de modo que pueden adivinar una contraseña", explica Eduard Meelhuysen. "Esto significa que **cuanto más corta y más simple sea una contraseña, más fácil será acceder** a tus cuentas usando esta tecnología. Mediante el uso de una contraseña más larga y más compleja, podemos ponérselo exponencialmente más difícil a los hackers".

En este sentido, **"si una contraseña tarda demasiado en ser descifrada, los hackers simplemente pasarán al siguiente lote"**, indica este experto.

A nivel corporativo, Bitglass también advierte de que "el número de violaciones de datos a gran escala y el hecho de que los usuarios reutilizan regularmente contraseñas es un problema real para las empresas hoy en día". Esto es así porque **"las contraseñas estáticas no puede proporcionar una protección corporativa efectiva"**, dice Anurag Kahol, CTO de Bitglass. Esto estaría animando a las organizaciones a aprovechar la autenticación de tipo dinámico y a analizar en busca de comportamientos sospechosos.

"Es esencial que este enfoque de la autenticación del usuario también puede extenderse a todas las aplicaciones en la nube", recomienda el directivo de **Bitglass**. "Por ejemplo, si un usuario inicia sesión en Office 365 desde el Reino Unido y entonces poco después inicia sesión en Salesforce desde Alemania, debería ser marcado como una actividad anómala" y pedir de nuevo que ese

usuario autentique su identidad.