Múltiple **F**actor de **A**utenticación (**MFA**)

El **M**últiple **F**actor de **A**utenticación (**MFA**) es un método de seguridad que requiere que los usuarios proporcionen más de una forma de verificación para acceder a una cuenta o sistema. En lugar de depender únicamente de una contraseña como única medida de seguridad, **MFA** agrega una o más capas adicionales de autenticación para confirmar la identidad del usuario.

Los factores de autenticación típicos son tres:

- **Algo que sabes, o que Conoces**: Este factor implica el uso de información que solo el usuario debe conocer, como una contraseña, un PIN (número de identificación personal) o respuestas a preguntas de seguridad. Por ejemplo, cuando una aplicación desea validar por segunda vez, te envía un código a tu teléfono

- **Algo que tienes, o que posees**: Este factor implica la posesión de un dispositivo o medio físico que solo el usuario debe tener acceso, como un teléfono móvil, una tarjeta inteligente, una llave de seguridad o una tarjeta de acceso. Por ejemplo, el token que te genera la aplicación bancaria instalada en el celular.

- **Algo que eres, lo que es Inherente a la persona**: Este factor se basa en características físicas o de comportamiento únicas del usuario, como la huella dactilar, el reconocimiento facial, el escaneo de iris o la voz.

La idea principal es que, para acceder a una cuenta o sistema protegido con **MFA**, el usuario debe proporcionar al menos dos de estos factores (o incluso los tres, en caso de MFA de tres factores) para demostrar su identidad. Esto añade una capa adicional de seguridad, ya que los atacantes tendrían que sortear varios desafíos de autenticación en lugar de solo uno (como en el caso de usar solo una contraseña).

El MFA se utiliza ampliamente para proteger cuentas en línea, servicios en línea de Bancos, aplicaciones empresariales y otros sistemas que almacenan información sensible. Al implementar MFA, los usuarios pueden tener mayor tranquilidad sabiendo que sus cuentas están mejor protegidas contra ataques de fuerza bruta, robos de contraseñas y otros intentos de acceso no autorizado. Algunas aplicaciones solicitan “Activar la verificación de dos pasos” generando la activación del segundo factor de autenticación.

A modo de ejemplo…

La autenticación es como abrir una puerta con una llave. La llave es tu contraseña. Sin embargo, en lugar de depender solo de una llave (contraseña) para proteger esa puerta (tu cuenta), utilizas más de una cerradura en la misma puerta. Eso es la **a**utenticación de **m**últiples **f**actores (**MFA**).

…un poco más en detalle…

1. **La Contraseña es el Primer factor**: Es como la primera línea de defensa para abrir la

puerta. Proporcionas tu contraseña, que es una combinación de números, letras y/o caracteres especiales, para verificar que eres el usuario autorizado.

2. **El Segundo factor** o Segunda línea de defensa, imagina que, después de insertar la contraseña en la cerradura, necesitas utilizar una llave adicional (segundo factor) para abrir completamente la puerta. Este segundo factor puede ser algo que solo tú posees, como un código enviado a tu teléfono móvil, una huella digital o una llave física.

3. **El Tercer factor** o Tercera línea de defensa: Algunos sistemas avanzados pueden tener incluso un tercer factor de autenticación. Es como si, después de usar la contraseña y la llave, también tuvieras que decir una palabra específica (como una frase secreta) para finalmente acceder al lugar protegido.

La idea principal es que cada factor adicional es agregar una capa de seguridad y protección. Incluso si alguien descubre tu contraseña, no podrá acceder a tu cuenta sin el segundo (y posiblemente tercer) factor de autenticación. Esto hace que sea mucho más difícil para los ciberdelincuente o personas malintencionadas obtener acceso no autorizado a tus cuentas y datos personales.

En resumen, el **M**ultiple **F**actor de **Autenticación** es como tener una puerta con múltiples cerraduras, y cada cerradura requiere su propia llave única para abrirla. Esta combinación de factores de autenticación mejora significativamente la seguridad y protege tus cuentas digitales de manera más efectiva que solo depender de una contraseña.

Recuerde…..el equipo de seguridad está para ayudarle. Puede escribirnos a **protege@unq.edu.ar** y le asistiremos de inmediato.
Proteger la información y la seguridad de la universidad es nuestra prioridad.

¡Gracias por su colaboración y precaución!