Shigra DIGITAL

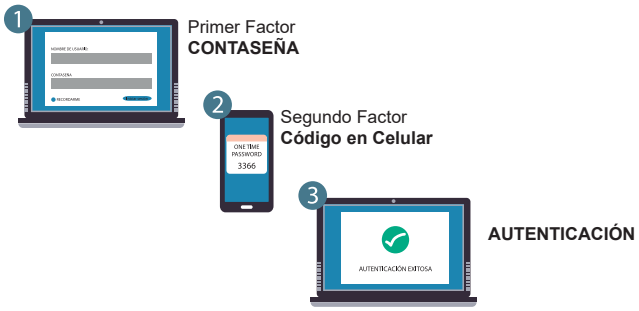
¡Usemos verificación en dos pasos (2AF)!

Los datos y la información que generamos en el uso diario de la Internet, representan el activo digital más preciado para los gobiernos, las empresas prestadoras de servicios de telecomunicación, empresas de marketing y redes sociales, incluso a los crakers (delincuentes cibernéticos), o también para aquellas exparejas que desean extorsionarnos.

Una de las primeras formas de proteger la privacidad de nuestras cuentas de comunicación electrónica es la técnica conocida como autenticación de doble factor o paso. (2AF)

Se trata de una técnica de seguridad que permite proteger nuestras comunicaciones electrónicas, como las cuentas de correo electrónico, cuentas de redes sociales, o accesos a sistemas informáticos especializados.
Son un escalón más en el proceso de la seguridad digital, que proveen una seguridad extra en el acceso autorizado a la información de tipo sensible y personal o corporativo.
Es importante que este tipo de autenticación puede activarse en cualquier dispositivo tecnológico como un celular, una Tablet, una computadora, etc.

El siguiente esquema muestra el funcionamiento de la doble autenticación:



Los factores de la doble autenticación en forma fácil de recordar y entender, pueden ser:

- Algo que sé (conocimiento),
- Algo que tengo (posesión),
- Algo que soy (inherente),

Es decir, algo que el usuario conoce como su contraseña; algo que el usuario posee como una llave YubiKey; algo que es único en el usuario, como su huella dactilar, iris ocular, voz humana.
Es común escuchar el término mitigación; muy relacionado con el hecho de prevenir antes que lamentar un hackeo de nuestras cuentas de comunicación electrónicas.

HUAIRA
creative commons

Créditos: Fundación Huaira 2020. Shigra Digital.
https://www.huaira.org/ShigraDigital

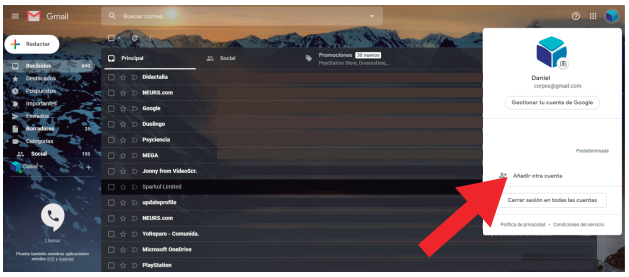
Doble autenticación en aplicaciones de uso diario.

La tecnología cada día avanza a pasos agigantados, y muchas veces nos abruma la cantidad de ataques que se denuncian por diversos medios noticiosos. Por ello es importante que la activemos en nuestras cuentas de comunicaciones electrónicas de uso diario.

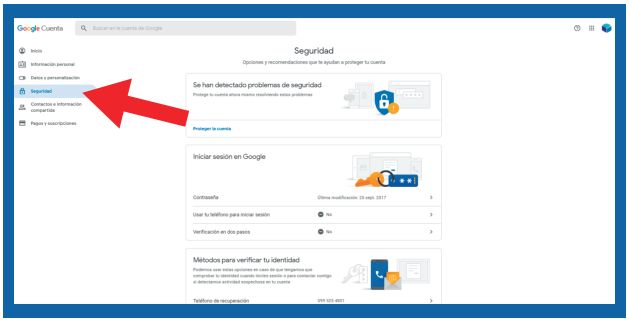
Veamos cómo se lo activa en:

1. Correo electrónico de Gmail.

Ingresas a tu cuenta de Gmail; luego das click en tu foto de perfil (avatar) y eliges la opción Gestionar tu cuenta de google:

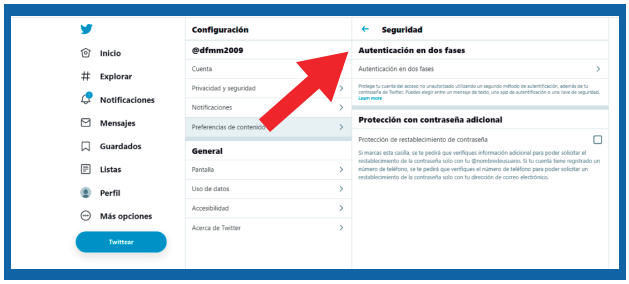


En la siguiente pantalla que se visualiza debes revisar cada opción que te ofrecen los diferentes menús del apartado seguridad y privacidad.



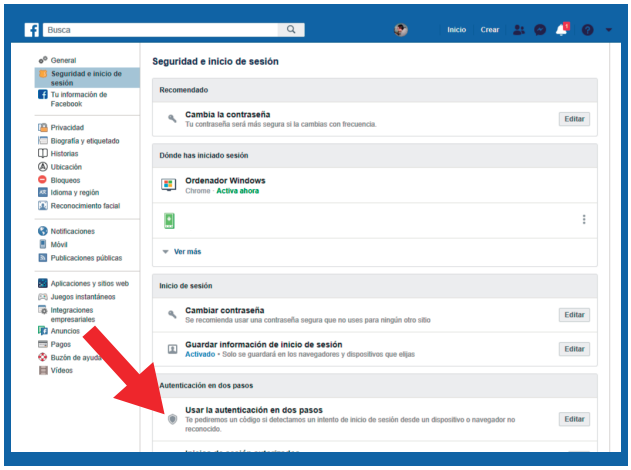
2. Red social Twitter.

Ingresas a tu cuenta de Twitter; luego das click en la opción más opciones después en configuración. Una vez en ese menú elijes la opción cuenta, después la opción seguridad y finalmente la opción autenticación en dos fases.



3. Red social Facebook.

Ingresas a tu cuenta de Facebook; luego das click en la lista desplegable superior derecha, luego eliges la opción configuración, finalmente das click en sección seguridad e inicio de sesión y configuras la opción usar autenticación en dos pasos.



Esta misma técnica se puede utilizar en otras aplicaciones de comunicación de tipo cifrada como Whatsapp, Telegram, wire o signal; serán aprendidas en los siguientes apartados.

Suscríbete a Shigra Digital en nuestro canal de Telegram

@ShigraDigital

¡No olvides que puedes imprimir tu propia ShigraDigital y compartirla libremente!

-Puedes contactarnos en:
shigradigital@huaira.org