CIBERCONSEJOS

AUTENTICACIÓN DE DOS FACTORES (2FA)

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Autenticación de dos factores (2FA)

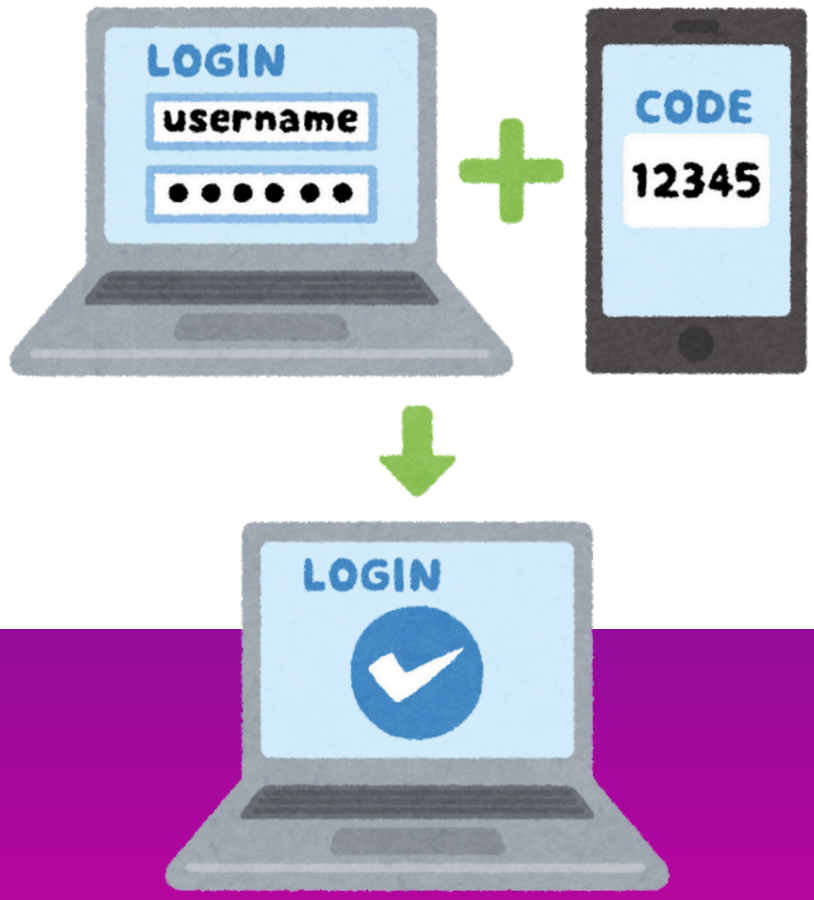
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

La autentificación de dos o más factores (2FA) es una medida de seguridad que exige una forma adicional de identificación para acceder a una cuenta, la que se suma a la tradicional contraseña.

Al activar la autenticación de dos factores (2FA), mejoras significativamente la seguridad de tus cuentas en línea.

Existen muchas formas de implementar un 2FA.

Por ejemplo, un código enviado por SMS o a una app a un celular ya registrado por el usuario, un token, una tarjeta de combinaciones o datos biométricos como la huella.



2FA en WhatsApp

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- En WhatsApp ve a "Configuración" (o "Ajustes").
- Selecciona "Cuenta".
- Toca "Verificación en dos pasos".
- Presiona "Activar".
- Ingresa un código PIN de seis dígitos que será requerido cada vez que registres tu número de teléfono con WhatsApp.
- Introduce una dirección de correo electrónico para recuperar tu cuenta en caso de olvidar el PIN.
- Confirma el correo electrónico.

2FA en Instagram (también sirve para Facebook)

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- En Instagram ve a tu perfil y toca las tres líneas horizontales en la esquina superior derecha.
- Selecciona "Centro de cuentas" y ve a "Contraseña y seguridad".
- Haz clic en "Autenticación en dos pasos".
- Ahí te aparecerán todas las cuentas que tienes en Meta, empresa matriz de Facebook e Instagram.
- Selecciona la cuenta de Instagram.
- Elige el método de seguridad: "Mensaje de texto" o una "Aplicación de autenticación".
- Sigue las instrucciones en pantalla para completar el proceso.

2FA en TikTok

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- En TikTok ve a tu perfil.
- Toca las tres líneas horizontales en la esquina superior derecha para acceder a "Ajustes y privacidad".
- Selecciona "Seguridad y permisos".
- Haz clic en "Verificación en dos pasos".
- Elige el método de verificación: "Teléfono", "Correo electrónico", “Aplicación de autenticación” o "Contraseña".
- Presiona el botón “Activar” y luego sigue las instrucciones para completar la configuración.

2FA en Gmail

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- Abre tu cuenta de Google y ve a "Seguridad".
- En "Iniciar sesión en Google", selecciona "Verificación en dos pasos".
- Haz clic en "Continuar".
- Verifica que eres tú, ingresando
- la contraseña de Google o a
- través de face ID en iPhone.
- Agrega tu número de teléfono y elige si deseas recibir los códigos de verificación por mensaje de texto o llamada.
- También puedes agregar llaves de seguridad, códigos de respaldo y app de autenticación.