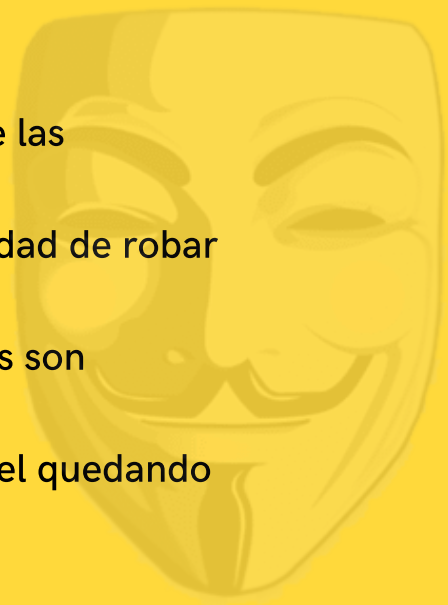
DOBLE FACTOR DE AUTENTICACION

Los ciberdelincuentes buscan nuestras contraseñas para poder acceder a nuestros servicios, robarnos datos, extorsionarnos, etc. Pueden conseguir las contraseñas de muchas formas.

Además de autenticarnos con una contraseña o con PIN, es decir con "algo que sé", también podemos hacerlo con "algo que tengo" (un token USB o una tarjeta de coordenadas) o con "algo que soy" (la huella, el iris, la voz o el rostro) o bien con varios de estos elementos o factores. Algunos bancos llevan haciendo esto desde hace tiempo. Es lo que se llama autenticación de doble (o triple) factor.

Con la doble autenticación se mitigan en gran medida los ataques cibernéticos como:

- Intentando adivinarlas por fuerza bruta.
- Engañándonos con técnicas de ingeniería social para que se las entreguemos (phishing).
- Infectándonos por malware también que tiene la funcionalidad de robar contraseñas.
- Aprovechando agujeros de seguridad, si nuestros servidores son vulnerables o tienen fallos de configuración.
- Por malas prácticas del usuario como apuntarlas en un papel quedando a la vista de alguien con malas intenciones.



RECOMENDACIONES:

- Siguiendo un principio de proporcionalidad, se recomienda utilizar siempre doble factor en los servicios que sean críticos, como la administración de sistemas, las cuentas del banco o la gestión de la tienda online.

- Para acceder a los aplicativos de la empresa se recomienda el uso de la doble autenticación, perder la contraseña de acceso puede parar nuestra actividad o nos ocasione importantes problemas de otro tipo como de imagen, legales o contractuales.

- Si los servicios que utilizamos no lo permiten, y como paso intermedio, podemos utilizar un gestor de contraseñas (gratuito o de pago) que soporte doble factor.

- En el caso de las redes sociales activar el doble factor de autenticación, si lo ofrecen.

- También podemos contratar con una empresa de seguridad, la integración de la autenticación de doble factor para el acceso a nuestros dispositivos, servicios y aplicaciones o para los servicios que ofrecemos a nuestros clientes si consideramos que el acceso a los mismos debe protegerse por todos los medios.

CSIRT
EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

E-Mail: info@cert.pa
Phone: +507 520-2378
Web: https://cert.pa
Twitter: @CSIRTPanama