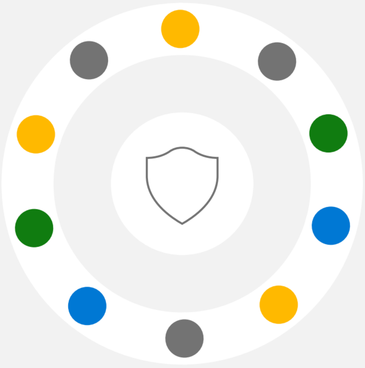
10 reglas fáciles para asegurar tus datos personales y proteger tus dispositivos



#METAS

Nunca tener que reemplazar todas tus identificaciones, tarjetas de crédito y documentos oficiales después que de que tu identidad haya sido robada por ciberdelincuentes.

Aquí hay 10 reglas fáciles para mantener tu correo electrónico, cuentas y dispositivos más seguros y evitar el robo de identidad.

1 **Sólo comparte información personal en tiempo real, preferiblemente en persona o por teléfono. Ten cuidado con lo que compartes en redes sociales.**

Comparte información personal en persona o por teléfono. Si es absolutamente necesario enviar información personal por correo electrónico, utiliza las herramientas de cifrado de Microsoft Outlook. Protégete de los hackers de redes sociales. Antes de publicar en redes sociales, piensa en la información que se puede obtener de ellas.

2 **Se escéptico con los mensajes que contienen enlaces a sitios web, especialmente los que piden información personal**.

Busca un número de teléfono en el sitio web oficial del remitente y llámalo directamente para confirmar que el mensaje es legítimo.

3 **Estar atento a los mensajes con archivos adjuntos.**

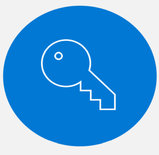
Nunca abras archivos adjuntos inesperados, incluso si parecen provenir de personas u organizaciones en las que confías. Si te preocupa que el mensaje pueda ser importante, llama al remitente para verificarlo.

4 **Olvídate de las contraseñas y utiliza una aplicación de autenticación para una mayor seguridad**.

No pueden robar tu contraseña si no usas una. En cambio, activa la opción sin contraseña para que tu cuenta de Microsoft inicie sesión con tu teléfono o Windows Hello.

5 **Si debes usar contraseñas, hazlas seguras y únicas con un administrador de contraseñas**.

Las contraseñas seguras tienen al menos 14 caracteres y símbolos aleatorios. Usa Microsoft Edge para recordar contraseñas y administrar cambios de contraseña.

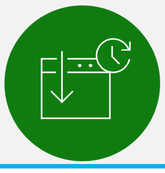


6 **Habilita la función de bloqueo en todos tus dispositivos móviles**.

Utiliza un PIN, huella digital o reconocimiento facial para desbloquear su dispositivo.

7 **Instala las actualizaciones de software inmediatamente.**

Muchas actualizaciones de aplicaciones y sistemas operativos son soluciones de seguridad para problemas actuales, así que instálalas de inmediato.



8 **Asegúrate de que todas las aplicaciones de tu dispositivo sean legítimas**.

Solo instala aplicaciones de la tienda oficial para tu dispositivo.

9 **Usa Windows 11 y activa Tamper Protection para proteger tu configuración de seguridad. .**

Utiliza siempre la última versión de Windows. Tamper Protection bloquea cambios no autorizados en tu configuración de seguridad.

.

10 **Mantén tu navegador actualizado, navega en modo incógnito y habilita el bloqueador de ventanas emergentes**.

Instala las actualizaciones del navegador y del sistema operativo de inmediato para mantener los últimos estándares de seguridad.

Para obtener más información sobre cómo mantener su correo electrónico, cuentas y dispositivos seguros, vaya a https://support.microsoft.com/security.

Obtenga las últimas noticias de seguridad de Microsoft, vaya a https://www.microsoft.com/en-us/securitynow.