Microsoft Security

12 consejos para proteger tus datos y dispositivos conectados a Internet

Aquí tienes 12 consejos para mantener tu correo electrónico, tus cuentas y tus dispositivos, incluidos los que están conectados a la red de tu organización, mejor protegidos de los ciberataques:

1

No te fíes de los mensajes con enlaces, especialmente aquellos que solicitan información personal

Los enlaces y sitios web falsos pueden ser muy convincentes. En lugar de confiar en los enlaces, busca un número de teléfono en el sitio web oficial del remitente para que puedas llamar directamente y confirmar que el mensaje es legítimo.

2

Presta especial atención a los mensajes con archivos adjuntos

Nunca abras archivos adjuntos inesperados aunque parezcan provenir de personas u organizaciones en las que confías. Si crees que el mensaje puede ser importante, llama al remitente para que lo verifique.

3

Comparte información personal solo en tiempo real

Siempre conviene compartir la información personal en persona o por teléfono. Si no tienes más remedio que enviar información personal por correo electrónico, usa las herramientas de cifrado de Microsoft Outlook.

4

Renuncia a las contraseñas y usa una aplicación de autenticación para reforzar la seguridad

Si no tienes contraseña, no te la pueden robar. Activa la autenticación sin contraseña de tu cuenta Microsoft para iniciar sesión con tu teléfono o Windows Hello.

5

Si tienes que usar contraseñas, asegúrate de que sean seguras y únicas con un administrador de contraseñas

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

6

Habilita la función de bloqueo en todos tus dispositivos móviles

Exige un PIN, una huella dactilar o el reconocimiento facial para desbloquear tu dispositivo.

7

Instala las actualizaciones de software inmediatamente

Muchas actualizaciones de aplicaciones, navegadores y sistemas operativos contienen correcciones de seguridad para los problemas actualmente activos, así que instálalas inmediatamente para mantener los estándares de seguridad más recientes.

8

Asegúrate de que todas las aplicaciones de tu dispositivo sean legítimas

Instala solo las aplicaciones desde la tienda de aplicaciones oficial de tu dispositivo.

9

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

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

10

Reduce la superficie de ataque

Elimina las conexiones a internet innecesarias, restringe los puertos abiertos y utiliza herramientas de exploración para comprobar si tu entorno digital contiene puntos débiles, para que puedas tomar medidas y mitigar los riesgos.

11

Usa tus herramientas de análisis de firmware

Comprueba si tu entorno de trabajo contiene puntos débiles para que puedas tomar medidas y mitigar los riesgos.

12

No transfieras archivos que contengan definiciones del sistema

Enviar definiciones del sistema a través de canales inseguros o a empleados no esenciales puede permitir ataques a tu entorno digital que corrompan tus procesos y hagan que tu entorno sea vulnerable.

Explora más temas de concienciación sobre ciberseguridad y oportunidades de formación en https://aka.ms/cybersecurity-awareness.

Microsoft Security