LastPass

Los 4 principales riesgos de ciberseguridad

RIESGO 1 Ataques basados en contraseñas

Qué es: los hackers utilizan credenciales robadas para acceder a la red de una empresa, conseguir privilegios de administrador o apropiarse de cuentas de empleados.

El **80%** de los robos de datos vinculados a hackeos tiene su origen en contraseñas poco seguras y robadas.[1]

El año 2022 marcó un nuevo récord en el coste medio de los robos de datos, que se situó en **4,45 millones de USD**

RIESGO 2 Malware

Qué es: software malicioso instalado secretamente en un dispositivo para permitir a los hackers acceder a datos o cuentas.

de las pymes han sufrido ataques de malware.[1]

de las organizaciones han sido víctimas de la difusión de malware entre empleados.[3]

RIESGO 3 Phishing

Qué es: el intento de robar credenciales u otra información de valor engañando a los usuarios para que entren en aplicaciones o sitios web maliciosos.

En 2022 se denunciaron **más de 255 millones** de ataques de phishing.[1]

Una empresa de 10.000 empleados pierde de promedio **65.343 horas** cada año por ataques de phishing.[3]

RIESGO 4 Ransomware

Qué es: malware que roba y cifra los datos de una víctima y pide una recompensa para su restitución.

de las pymes ha sufrido ataques de ransomware.

de las pequeñas empresas víctimas de ransomware paga los rescates exigidos.[3]

LastPass puede ayudarle a evitar los ciberataques más habituales.

Más información

Fuentes:

(1) https://www.verizon.com/business/en-gb/resources/2022-data-breachinvestigations-report-dbir.pdf

(2) https://www.swktech.com/costs-of-a-cyber-attack-for-smbs/

(3) https://www.comparitech.com/antivirus/malware-statistics-facts/