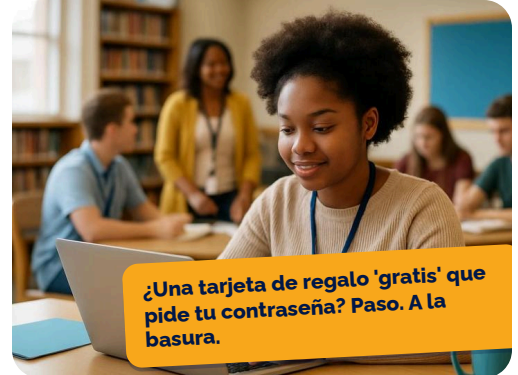


EDICIÓN TEMPORADA DE SORTEOS

¿Gratis y urgente? Es carnada.

Los sorteos falsos, el saldo 'gratis' para el teléfono y las apps imitadoras buscan una sola cosa: tu usuario, tus datos personales o un pago con la tarjeta de tu familia. Aparecen en anuncios, ventanas emergentes y mensajes que parecen oficiales.



¿Una tarjeta de regalo 'gratis' que pide tu contraseña? Paso. A la basura.



Apps solo de la tienda oficial

Descarga apps solo de la tienda oficial de tu dispositivo o de la lista aprobada por tu escuela. Revisa el nombre del desarrollador y las reseñas. Una 'versión premium gratis' de un enlace raro es como entra el malware.



Revisa quién publica de verdad

Las cuentas de sorteos falsos copian logos y fotos reales. Fíjate en la antigüedad de la cuenta y en lo que ha publicado. Un sorteo real no te cobra el envío ni te pide la contraseña para ganar.



Nada de tarjetas familiares para cosas 'gratis'

Si un premio gratis pide un número de tarjeta, un cargo pequeño o tu contraseña, no es gratis. Pregúntale a tu mamá, papá o tutor antes de escribir datos de una tarjeta, siempre.



Detecta la estafa



Ventana emergente

External

Ventana emergente en un sitio de trucos para juegos <free-gift-rewards.example/claim>

FELICIDADES: eres el ganador de hoy

Felicidades. Eres el visitante número 1,000,000 de hoy y ganaste una tarjeta de regalo de \$500 para tu tienda de juegos favorita. Para reclamarla, instala nuestra app Rewards Helper y escribe un número de tarjeta para pagar \$1.99 de envío. Tu premio vence en 02:59 y luego pasa al siguiente visitante. Si cierras esta ventana, pierdes tu lugar.

Descubre la estafa: ¿cuántas señales de alerta encuentras?

Señales de alerta que encontré: ○ ○ ○ ○ ○

Busca: sorpresa, urgencia, secreto, un método de pago inusual, un remitente o enlace que no puedes confirmar.

DATO CURIOSO

Georgia, esto va con nosotros: en el Informe de Delitos en Internet 2025 del FBI, Georgia ocupó el primer lugar del país en dinero perdido por víctimas de 17 años o menos, más de \$3 millones.

Fuente: FBI IC3 2025 Internet Crime Report



Tu acción de 60 segundos

Revisa las apps de tu teléfono y borra las que no usas o que no recuerdas haber instalado.



¿A quién le aviso?

Nombre / ext. _____

Canal para reportar _____



Escanea para una lección de 2 minutos sobre pantallas falsas de inicio de sesión

Gratis, sin iniciar sesión · k12cyberforward.com/learn

- RESPUESTA**
- Cinco señales: 'visitante un millón', un premio demasiado bueno, una app para instalar, una tarjeta para el 'envío' y una cuenta regresiva. Lo inteligente: cierra la pestaña sin tocar nada dentro de la ventana, no instalas nada y avísale a un adulto si ya escribiste datos de una tarjeta.
- Las ventanas de 'visitante un millón' son estafa desde hace décadas.
 - Un premio enorme por no hacer nada es demasiado bueno para ser verdad.
 - Una app que viene de una ventana emergente puede ser malware.
 - La tarjeta para el 'envío' es para robar el número.
 - El reloj en cuenta regresiva es presión falsa.