

● OFERTAS FALSAS. ● PHISHING ● SPAMMING ● APLICACIONES FRAUDULENTAS.

PRINCIPALES ESTAFAS



Ofertas falsas. Te ofrecen descuentos de ensueño para que des click en el enlace y así redirigirte a páginas web falsas o instalar malwares (programas dañinos).

Phishing o suplantación de identidad de marcas reconocidas para obtener la información de tus tarjetas.

Spamming o envío masivo de mensajes no solicitados con ofertas o cupones de todo tipo.

Aplicaciones fraudulentas. Los ciberdelincuentes crean aplicaciones falsas para robar tus datos bancarios o infectar tu celular con malwares.



¿CÓMO PROTEGERTE?

Analiza los correos que te lleguen. Si una oferta llamó tu atención ve a la página oficial de la marca en tu navegador y búscala.

Comprueba que el dominio de la página web sea el correcto y no uno parecido.

Inspecciona la página en búsqueda de la información legal (términos y condiciones, política de privacidad, política de cambios y devoluciones). Desconfía si no la tiene.

Toma en cuenta las opiniones de otros usuarios sobre el portal web antes de comprar.

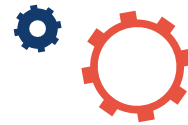
Verifica los precios. No es normal que los montos sean demasiado bajos o todos iguales.

Al momento de pagar comprueba que el link empiece por "https" y tenga certificado de seguridad y sello de confianza.

Asegúrate de que acepten diferentes tipos de pago.

Utiliza una sola tarjeta para pagar, así puedes minimizar riesgos. Procura que tenga protección contra fraudes.

¿QUÉ HACER SI TE VULNERAN?



Comunícalo al Departamento de Investigación de Crímenes de Alta Tecnología (DICAT).

Informa a tu banco que fuiste víctima de estafa.

