

Sé escéptico ante correos electrónicos, mensajes o sitios web sospechosos. No hagas clic en enlaces ni proporciones información personal a menos que estés seguro de la legitimidad.



Phishing

No permitas acceso remoto a tu computadora a menos que estés seguro de la autenticidad del soporte técnico. No llames a teléfonos proporcionados en ventanas emergentes o mensajes no solicitados.



Fraude de soporte técnico

Mantén actualizado tu software de seguridad, realiza copias de seguridad regularmente y sé cauteloso al abrir archivos adjuntos o hacer clic en enlaces en correos electrónicos.



Ransomware

Desconfía de premios que no has solicitado y verifica la autenticidad de las loterías antes de proporcionar información personal o realizar pagos.



Estafas de lotería en línea

SUS AHORROS

Es importante estar informado y ser consciente de las tácticas utilizadas por los estafadores en línea. Además de estas precauciones específicas, es fundamental mantener actualizado tu software de seguridad, utilizar contraseñas fuertes y educar a otros sobre las amenazas cibernéticas

Estafas de inversión en línea



Investiga cuidadosamente antes de invertir en cualquier oportunidad. Desconfía de las ofertas que parecen demasiado buenas para ser verdad

Estafas de romance en línea



Sé cauteloso al entablar relaciones en línea y nunca envíes dinero a alguien que no hayas conocido en persona. Verifica la autenticidad de la persona antes de compartir información personal

Fraude de tarjetas de crédito en línea



Utiliza sitios web seguros para realizar transacciones, revisa regularmente tus estados de cuenta y reporta cualquier actividad sospechosa de inmediato

Suplantación de identidad (pharming)



Usa software de seguridad, mantén actualizado tu sistema operativo y navega por sitios web seguros. Verifica siempre la URL del sitio antes de ingresar información confidencial