Ten cuidado con las páginas webs falsas. Utiliza webs que confies, en especial aquellas en las que hagas transacciones, como los sitios de comercio electrónico. Un elemento clave para tener en cuenta es un certificado de seguridad o SSL. Es decir, presta atención a que las URL empiecen con "https" en lugar de "http" (la "s" significa "seguro") y que tengan el ícono de candado en la barra de direcciones.

Presta especial atención a los falsos correos que simulan ser tu banco y en los que te piden datos confidenciales y claves de seguridad para realizar operaciones. Nunca lo hagas: recuerda que las claves son personales y no tienes obligación alguna de facilitarlas. En la duda es mejor que hables con tu banco y confirmes el origen de esos correos.

PROTEGETE DE LA CIBERDELINCUENCIA

Lucentum
Federación Provincial de Asociaciones de Amas de Casa, Consumidores y Usuarios de Alicante "Lucentum"

Subvencionado por:
GENERALITAT VALENCIANA
Conselleria de Innovación, Industria, Comercio y Turismo

CIBERDELINCUENCIA

CIBERDELINCUENCIA

Las personas consumidoras pueden enfrentarse a situaciones de estafas en su actividad en el ámbito financiero, sobre todo a raíz de la influencia de las nuevas tecnologías.

Es importante que sepamos identificar las principales estafas financieras que podemos sufrir y que aprendamos a prevenirlas. Fraude del Técnico Informático, Phishing, , Smishing, Vishing... Son técnicas utilizadas para acceder a nuestros datos, suplantar nuestra identidad e infectar nuestros dispositivos.

TÉCNICAS DE CIBERDELINCUENTES

PHISING

Utiliza correos electrónicos y enlaces fraudulentos.

SMISHING

utiliza mensajes de texto o mensajes por WhatsApp.

VISHING

Son llamadas fraudulentas, utilizando argumentos para engañar.

FRAUDE DEL TÉCNICO INFORMÁTICO

Persona que te llama, supuestamente de alguna conocida empresa, alertándote de que tienes un problema en tu ordenador, móvil u otro dispositivo .

NORMAS BÁSICAS PARA PREVENIR LA CIBERDELINCUENCIA

Crea contraseñas complejas (combinaciones de números y letras, mayúsculas y minúsculas...), cámbialas con regularidad, instala un antivirus y actualiza tus dispositivos.

Si recibes correos electrónicos en los que solicitan información personal o confidencial, no los respondas, descargues ni ejecutes los ficheros asociados.

Usa una conexión a internet segura. No es recomendable utilizar redes Wi-Fi públicas, pero si te conectas a internet en un lugar público utilizando estas redes, evita realizar transacciones personales (como operaciones bancarias o compras en línea) en las que se utilicen datos confidenciales.