TALLER: TIPOS DE FRAUDES. (NUEVOS Y NO TAN NUEVOS)

Objetivo: Conocer los fraudes más comunes en España, identificar señales de alerta y aprender a protegerse.

1. Introducción

- Objetivo: Explicar que el taller busca informar sobre los fraudes más frecuentes en España y cómo prevenirlos.

- Importancia: Destacar el aumento de los fraudes en la era digital y la necesidad de estar informados.

2. Fraudes tradicionales

Breve descripción de los fraudes clásicos que siguen vigentes:

-Vishing (Voice Phishing). Estafas telefónicas: Llamadas falsas de supuestos técnicos de bancos, operadoras o servicios públicos.

- Phishing por correo electrónico: Emails falsos que imitan a entidades bancarias o empresas para robar datos.

- Timos inmobiliarios: Ofertas falsas de alquileres o ventas de propiedades.

- Estafas nigerianas: Ofertas de grandes sumas de dinero a cambio de un adelanto.

- Estafas piramidales: ForunFilatelico y Afinsa como gran ejemplo. Se paga a inversores antiguos con el dinero de nuevos.

-Fraudes con tarjetas de crédito Skimming: Clonación de tarjetas mediante dispositivos en cajeros automáticos. Compras no autorizadas: Datos de tarjeta robados en filtraciones de datos.

- Esquemas Ponzi. Promesas de inversiones con altos retornos.

3. Fraudes digitales y nuevos métodos

Descripción de los fraudes más recientes y cómo operan:

- Smishing:Mensajes de texto (SMS) con enlaces maliciosos o solicitudes de datos personales.

- Fraudes en redes sociales: Cuentas falsas que ofrecen productos, servicios o inversiones fraudulentas.

- Estafas en plataformas de compra-venta: Vendedores falsos en Wallapop, Milanuncios, etc.

- Criptoestafas:Ofertas de inversión en criptomonedas con rendimientos irreales.

- NFT falsos: Venta de activos digitales sin valor real.

- Suplantación de identidad: Robo de datos para acceder a cuentas bancarias o realizar compras online. .DeepfakeScams

- Uso de inteligencia artificial para falsificar rostros y voces.

- Falsos empleos y teletrabajo. Anuncios de trabajo falsos que piden pagos por adelantado o roban datos personales.

- SIM Swapping (Intercambio de SIM) Los estafadores clonan tu tarjeta SIM para acceder a tus cuentas bancarias y redes sociales.

4. Cómo protegerse.

Consejos prácticos para evitar ser víctima de fraudes:

- Verificar siempre la fuente: No confiar en llamadas, correos o mensajes no solicitados.

- No compartir datos personales: Bancos y empresas nunca piden contraseñas o datos sensibles por teléfono o email.

- Usar contraseñas seguras y autenticación en dos pasos.

- Desconfiar de ofertas demasiado buenas para ser verdad.

- Reportar fraudes: Contactar con la policía (Grupo de Delitos Telemáticos) o la Oficina de Seguridad del Internauta (OSI).