C12/CONV/2025 – Recomendaciones para evitar ataques de pishing y smishing

Binaura (Grupo Monlex), consultora en tecnología, seguridad y protección de datos colaboradora de CAEB alerta sobre los **factores psicológicos que aprovechan los ciberdelincuentes en ataques de phishing y smishing.**

Estos fraudes manipulan emociones y provocan respuestas rápidas:

- Autoridad: suplantan a jefes o entidades oficiales.
- Miedo a perder algo: amenazan con bloqueos o sanciones.
- Urgencia: fuerzan a actuar sin pensar.
- Ego/vanidad: halagos o falsas recompensas.
- Automatismos: mensajes tipo “no se ha podido entregar su paquete, pulse aquí”.

Casos recientes

El INCIBE ha detectado:

- Suplantación de la Agencia Tributariamediante correos y SMS con enlaces fraudulentos.
- Falsos SMS de entidades bancarias que piden llamar a números controlados por los atacantes.
- Mensajes de entrega de paquetes que invitan a pagar pequeñas tasas para liberar un envío inexistente.

Recomendaciones

- Verificar siempre remitente y dirección web antes de hacer clic.
- Desconfiar de mensajes que generen urgencia o miedo.
- No compartir datos personales ni bancarios por email o SMS.
- Usar autenticación multifactor en accesos críticos.
- Establecer un canal interno para reportar intentos de fraude.

Más información y consultas : info@binauramonlex.com