DECÁLOGO DE CIBERSEGURIDAD

Pensar dos veces

No responder a ninguna comunicación sospechosa

Comprobar el remitente

Desconfiar de los números desconocidos y correos extraños

No fiarse de apariencias

El uso de nombres o logos oficiales no es una garantía de seguridad

Actuar con serenidad

Suelen solicitar una acción urgente, con alguna advertencia si no la realizamos

Analizar el objetivo del mensaje

En general, ninguna compañía u organismo solicita información personal por estos canales

Analizar el asunto

Muchos fraudes utilizarán un asunto llamativo, que nos obligue a tomar decisiones rápidas

Comprobar los enlaces

Es preferible acceder a una web tecleando la dirección en el navegador, no a través de un enlace

Analizar el archivo adjunto

Debemos analizarlos con un antivirus y las apps deben descargarse siempre desde los mercados oficiales

Maximizar las cautelas

Si sospechamos, no debemos seguir sus indicaciones, ni facilitar información personal

Examinar la redacción

A veces los mensajes tienen errores ortográficos y gramaticales, lo que debe hacernos sospechar

El mejor consejo es que comuniques con tu entidad bancaria o entidad de referencia a través de sus canales oficiales

AEB ceca unacc