“ PROTEGE TUS DATOS BANCARIOS” #Acompaña(DAS) desde casa

Durante estos días, pasamos más tiempo en internet y esto está siendo aprovechado por los ciber-delincuentes para realizar estafas electrónicas y obtener información privada de los usuarios. Te mandamos una serie de recomendaciones y consejos para evitar estos fraudes. Ahora más que nunca es fundamental no confiar tus datos a nadie ni por teléfono ni por correo electrónico si no es por los canales digitales oficiales del banco. Las entidades bancarias nunca van a pedirte las contraseñas, número de tarjeta, CVV o el PIN, por teléfono, mail, SMS o redes sociales. Si crees que has podido sufrir un posible fraude, cada entidad bancaria suele tener un canal de contacto para comunicarlo, búscalo en su página web.

¿Cómo evitar este tipo de estafas?

Email:

- No abras archivos adjuntos, ni hagas clic en enlaces web de correos sospechosos sobre el Coronavirus.

- Navega solo por páginas web que incluyan al inicio de la URL https:// y no http://

- El contenido suele mostrar fallos ortográficos o un lenguaje extraño más propio de una máquina.

- Las apariencias engañan, los atacantes suelen crear emails y páginas con un aspecto muy similar a la oficial.

SMS:

- No hagas clic en el enlace o número de teléfono de un mensaje del que no tengas seguridad.
- No respondas al mensaje.

Llamada telefónica:

- No facilites datos.

- Sospecha ante acciones que te soliciten que no sean habituales y trata de verificarlas por otra vía alternativa, correo, llamada, etc.

- Y recuerda:
  - Facilita datos SOLO a través de los canales oficiales de tu entidad bancaria como de organismos oficiales.

- No descargues información sobre Covid-19 de webs desconocidas o que recibas por email o WhatsApp, podrían infectarte con malware en tu ordenador o móvil.

  - No compartas información no contrastada con fuentes oficiales, así contribuyes a no difundir bulos.
  - No instales apps no oficiales para conocer el alcance internacional del Covid-19, podrían robarte información del móvil.