Liberty Seguros

¿Sabes qué es el Phishing?

Es un ataque realizado por ciberdelincuentes, para obtener información personal y/o financiera y engañar a sus víctimas.

Descubre cómo identificar y evitar el Pishing:

La técnica más común es mediante el envío de correos electrónicos o mensajes que suplantan a una organización o persona de confianza de la víctima.

¿A quién va dirigido el Phishing?

Cualquier persona puede ser victima de un ataque cibernético.

Tipos de Phishing

- **Phishing de correo electrónico**
- **Phishing de software malintencionado**
- **Phishing de objetivo definido**
- **Phishing de altos cargos**
- **Phishing por SMS (smishing)**
- **Phishing por voz (vishing)**

¿Como identificar el Phishing?

https://

Comprueba la dirección de correo del remitente antes de abrir el mensaje.

Mantén actualizado tu software y el sistema operativo de tu dispositivo.

No compartas información personal, contraseñas o claves bancarias con desconocidos.

No hagas clic en enlaces desconocidos o sopechosos.

¿Qué hacer en caso de sufrir un ataque de phishing?

- **Modificar la contraseña** de acceso del servicio suplantado y cualquier otro servicio en el que se utilicen las mismas credenciales.
- **Contactar a la entidad suplantada** para que esté informada y que adopte las medidas necesarias para proteger la información de sus clientes.

Ciberamenzas más comunes

El **factor humano**, es la variable más importante de las amenazas actuales, ya que por su comportamiento digital, forma de trabajar, el sitio donde hacen clic, un like, que páginas visitan, tienen una alta probabilidad de ser víctima de la ciberdelincuencia a través de los siguientes ciberataques:

- **Pishing**
- Malware
- Ramsomware
- Extorsión sexual (sextorsion)
- Minería ilícita de criptomonedas
- Suplantación de identidad
- Delitos en línea contra menores (Grooming)