GOVERTIS Advisory Services

PHISHING EN TIEMPOS DE PANDEMIA

El PHISHING es la técnica de ingeniería social para obtener información confidencial de los usuarios de forma fraudulenta.
Algunos de los más habituales:

SPEAR PHISHING
Método de ataque personalizado en una persona u organización

PHISHING REDIRECTOR
Método de ataque basado en campañas masivas

SMISHING (SMS)
Método de ataque por medio de mensajes de texto

VISHING
Método de ataque por medio de una llamada telefónica

¿CÓMO PROTEGERSE CONTRA EL PHISHING?

- Si el mensaje te pide hacer una acción extraña: ignóralo y bórralo.
- Evita abrir archivos adjuntos si desconoces al remitente o no se espera el documento.
- Protege tu contraseña. No almacenes la contraseña en los navegadores.
- Verifica las credenciales SSL del sitio de destino.
- Instala el programa antivirus y mantenlo actualizado.
- Comunica el incidente a tu responsable (DPD, CISO...)
- Comprueba el dominio del correo remitente y que su nombre coincida con su cuenta de correo electrónico.
- Mantener actualizado el navegador, el sistema operativo y demás software.
- Evita el uso de medios extraíbles.
- Evita usar redes públicas.