REPUNTAN LOS CASOS DE PHISHING QUE USAN COVID19 COMO GANCHO

No es la primera vez que se utiliza este tipo de correos con el fin de robar datos personales y bancarios. Por este motivo la concienciación y la información son esenciales.

Recomendaciones:

1.- Comprobar siempre la autenticidad del remitente y si tenemos dudas:

- No seguir enlaces sospechosos.
- No abrir correos de usuarios desconocidos.
- Precaución al seguir enlaces en correos aunque sean de contactos conocidos.
- Atención al descargar ficheros adjuntos de correos aunque sean de contactos conocidos.

2.- Y si hemos picado en un enlace malicioso **¿Qué puedo hacer?**

- Cambiar rápidamente las credenciales en caso de que las hayamos introducido en la página fraudulenta.
- Comunicarlo a nuestros contactos para prevenir que ellos también pudieran caer.
- Recabar y documentar toda la información posible sobre el engaño.
- Denunciarlo ante los Cuerpos y Fuerzas de seguridad del Estado.
- Colaborar con la Oficina de Seguridad del Internauta (OSI) incidencias@certsi.es

Y recuerda que tienes a tu disposición los servicios jurídicos de Tyrius www.tyrius.org

#YoMeQuedoEnCasa #EstoPasará

C/ Conde Montornés 20-1, 46003 Valencia
tel.: 963515993 · fax: 963942231
tyrius@tyrius.org
www.tyrius.org