RECOMENDACIONES PARA RECONOCER UN ATAQUE DE PHISING.

La situación de alerta generada por el Coronavirus a nivel mundial es un caldo de cultivo peligroso para ataques de Phishing (Técnicas que buscan engañar a sus víctimas haciéndose pasar por una organización o persona de confianza para que acabe realizando acciones que no deberían) a través de servicios de mensajería instantánea, correo electrónico u otros medios. Los ciberdelincuentes siempre tratan de explotar situaciones de miedo y la situación que se está viviendo en la actualidad no es una excepción, según aseguran desde la Agencia Española de Protección de Datos (AEPD).

Los ciberdelincuentes tratarán de suplantar organizaciones legítimas con información relevante sobre el Coronavirus como el Ministerio de Sanidad, una Consejería de Sanidad de una Comunidad Autónoma, Fuerzas y Cuerpos de Seguridad del Estado, Organizaciones Internacionales, simulando prestar ayuda y consejo o incluso fingiendo ser la Empresa en la que el Trabajador presta sus servicios. Podrán hacerlo a través de mensajería instantánea como WhatsApp, Telegram o, también a través de correos electrónicos. En la mayoría de los casos pedirán que se abra un archivo con urgencia o, se siga un enlace de Internet para obtener la información.

Si se sigue el enlace, se descarga y ejecuta un archivo adjunto, puede que se trate de algún tipo de Malware que permita a los ciberdelincuentes tomar el control del dispositivo, acceder tanto a la información como a los datos personales e incluso cifrar esos datos.

Los enlaces de Internet incluidos en estos mensajes o correos electrónicos también pueden enlazar a Páginas Web que suplantan la identidad de otras organizaciones para robar credenciales de acceso a un servicio u otra información personal, por ejemplo, el número de la seguridad social, los datos bancarios para el pago de un test de Coronavirus, etcétera.

TENER PRESENTE:

1. Especial precaución al abrir documentos y archivos adjuntos sobre el Coronavirus. Previamente deben ser analizados.
2. Mantenerse informado mediante fuentes oficiales y confiables, acudiendo directamente a Páginas Web de las instituciones o medios de comunicación, nunca a través de un enlace proporcionado en un mensaje o en un correo electrónico.
3. Verificar la dirección de correo electrónico remitente del mensaje y también el enlace a la Página Web al que remite el mensaje. A veces, resulta obvio que la dirección web no es legítima, pero otras veces los ciberdelincuentes son capaces de crear enlaces que se parecen mucho a las direcciones legítimas.
4. Tener cuidado con las solicitudes de datos personales a través de Páginas Web a las que se ha llegado siguiendo un enlace contenido en un mensaje o correo electrónico. Mejor acceder directamente a la Página Web de esa organización.
5. Fijarse bien en el contenido del mensaje, sospechar de mensajes con faltas de ortografía, errores gramaticales y saludos genéricos sin aportar ningún dato como “Estimado ciudadano” o “Estimado paciente”.
6. Sospechar mucho más si además el contenido del mensaje urge a realizar cualquier tipo de acción cuanto antes, con una urgencia injustificada.
7. Ante una situación de riesgo es más importante que nunca guardar la tranquilidad y reflexionar antes de actuar o tomar decisiones precipitadas. En este sentido, más que nunca, tener precaución frente a este tipo de prácticas y aprender a distinguir entre Páginas Web fiables y no fiables, así como mensajes con información segura e insegura. No se debe interactuar con contenidos multimedia recibidos a través de correos electrónicos sospechosos, siendo muy precavidos ante correos electrónicos de Bancos, de Correos, de Google, etcétera.