Medidas de Ciberseguridad en tiempo de COVID-19

Recomendaciones

Mientras dure la situación de alerta como consecuencia de la crisis sanitaria derivada de los contagios por Coronavirus o COVID-19, se esta observando a nivel mundial actos perpetrados por ciberdelincuentes que aprovechan esta situación para lanzar ataques de phishing y de todo tipo para sacar provecho.

El modus operandi de estos ciberdelicuentes es siempre muy similar. Perpetran campañas que tratan de suplantar a organizaciones legítimas con información relevante sobre el COVID-19, como lo son el Ministerio de Sanidad, una Consejería de Sanidad de una Comunidad Autónoma, Fuerzas del Orden, Organizaciones Internacionales, etc., simulando prestar ayuda y consejo, o incluso fingiendo ser una empresa para la que se trabaja, un cliente o un proveedor.

Estas campañas se hacen a través de mensajería instantánea como WhatsApp o Telegram y también a través de emails. En la mayoría de los casos se suele solicitar que se abra un archivo con urgencia o se siga un enlace de internet para obtener la información. Al seguir el enlace y descargar el contenido, se ejecuta un archivo adjunto. En estas situaciones se trata de algún tipo de malware que permite a los ciberdelincuentes tomar el control de su dispositivo, acceder a la información y datos personales e incluso cifrar esos datos.

Los enlaces de internet incluidos en estos mensajes o correos electrónicos también le pueden llevar a páginas web que suplantan la identidad de otras organizaciones para robar las credenciales de acceso a un servicio u otra información personal, por ejemplo, números de la seguridad social, datos bancarios para el pago de un test de coronavirus, etc.

Para evitar estas situaciones os queremos sugerir una serie de medidas de prevención. En concreto:

- **Manténgase informado mediante fuentes oficiales y confiables**, acudiendo directamente a las webs de las instituciones o medios de comunicación, nunca a través de un enlace proporcionado en un mensaje o en un email.

CORREO ELECTRÓNICO
sec.general@oiss.org

Calle Velázquez 105,1
28006 – MADRID
TEL.: 91 561 17 47

Recomendaciones

- **Verifique la dirección de correo electrónico remitente del mensaje** y también el enlace web al que te 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.

- **Tenga cuidado con las solicitudes de datos personales** a través de webs a las que haya llegado siguiendo un enlace contenido en un mensaje o correo electrónico. Mejor acceda directamente a la web de esa organización.

- **Fíjese bien en el contenido del mensaje**, sospeche de mensajes con faltas de ortografía, errores gramaticales y saludos genéricos sin aportar ningún dato de usted como “Estimado ciudadano” o “Estimado paciente”.

- **Sospeche mucho más** si además el contenido del mensaje le urge a realizar cualquier tipo de acción cuanto antes, con una urgencia injustificada.

- Ante una situación de riesgo es más importante que nunca guardar la **tranquilidad y reflexionar antes de actuar** o tomar decisiones precipitadas.

Esperamos haberle ayudado con esta información. Cautela y mucho ánimo de cara a superar esta situación.

Leynet abogados & consultores

CORREO ELECTRÓNICO
sec.general@oiss.org

Calle Velázquez 105,1
28006 – MADRID
TEL.: 91 561 17 47