El phishing se aprovecha del COVID-19

- Phishing es el término informático de engaño a una víctima para hacerse pasar por una persona, empresa o servicio de confianza y manipularla.
- Se manifiesta principalmente a través de servicios de mensajería instántanea, email y otros medios.

El constante deseo por mantenerse al tanto de los últimos acontecimientos en relación con el COVID-19, podría conllevar a que la población baje la guardia en la protección de sus dispositivos y enlaces web a los que accede, lo que podría aumentar la exposición a riesgos informáticos como el phishing.

Así se desprende de un informe realizado por la Agencia Española de Protección de Datos, en la cual se cita que los servicios de mensajería instantánea, correo electrónico y otros medios, serían de los más aprovechados por los ciberdelincuentes.

En ese sentido, la Agencia de Protección de Datos de los Habitantes (PRODHAB), ha decidido sumarse a esta campaña, solicitando precaución a la población para que únicamente se informen a través de los medios oficiales que para sus efectos ha autorizado el Gobierno, como el Ministerio de Salud o la Comisión Nacional de Emergencias.

“Si bien no tenemos reportes de que en Costa Rica se hayan presentado casos de este tipo por el momento, el modus operandi en otros países es que los ciberdelicuentes suplantan organizaciones legítimas simulando prestar ayuda o consejo, y una vez obtienen la confianza de la persona, solicitan que se abra un archivo con urgencia o que siga un enlace de Internet para obtener cierta información”, explicó Elizabeth Mora, Directora Nacional de PRODHAB.

La medida de prevención que gira la PRODHAB incluye no accesar estos enlaces desconocidos, y no descargar archivos o ejecutar programas en los celulares o computadoras. Ya que, al hacerlo, los ciberdelincuentes pueden tomar control del dispositivo, acceder a la información personal e incluso cifrarla para su propio beneficio.

“En momentos donde la mayoría estamos dirigiendo nuestros esfuerzos a evitar la transferencia del llamado coronavirus, hay quienes están tratando de aprovecharse de la situación, por lo que no podemos descuidar nuestros datos”, finalizó la Jerarca.

5 RECOMENDACIONES para no ser víctima de phishing

- Manténgase informado solo a través de fuentes oficiales y confiables, acudiendo directamente a sus webs o redes sociales oficiales.
- Verifique la dirección de correo electrónico del remitente y el enlace web al que lo intentan dirigir. En ocasiones, es muy evidente que la dirección web no es legítima.
- Si recibe una solicitud de enlace y en ella le demandan brindar sus datos personales, desconfíe y comuníquese directamente con la institución y verifique su petición.
- Revise el contenido del mensaje, sospeche de mensajes con faltas de ortografía, errores gramaticales y saludos genéricos.
- Si considera que sus datos están siendo vulnerados, infórmelo a la PRODHAB a través del teléfono 2234-0189. O comuníquese con la sección de Delitos Informáticos del OIJ al 2295-3127 o mediante la línea gratuita 800-8000-OIJ (645).

DIRECCIÓN NACIONAL
UNIDAD DE DIVULGACIÓN
Agencia de Protección de Datos de los Habitantes PRODHAB