ALERTA TÉCNICA

MICITT-DGD-DRII-AT-019-2020

Estafadores que están usando el nombre de la Organización Mundial de la Salud (OMS) para robar dinero y datos y Advertencias para el consumidor y consejos de ciberseguridad ante el COVID-19

Se les comunica a los Directores (as) /Jefes (as) de Tecnologías de Información y a los (as) enlaces de Ciberseguridad, para que tomen las medidas necesarias para advertir y prevenir sobre Cibercriminales que están usando el nombre de la Organización Mundial de la Salud (OMS) para robar dinero y datos delicados.

Es fundamental verificar la autenticidad de quien les contacta antes de responder, esto porque se están haciendo pasar por la OMS.

El método que están utilizando es el "Phishing", por lo que los cibercriminales están enviando emails maliciosos que parecen provenir de la organización, en estos emails se pide a la gente que de información delicada, como sus nombres de usuario o contraseñas, o se le pide a la gente que haga clic en un enlace o documento adjunto malicioso. Por medio de estas acciones los criminales pueden instalar malware o robar información delicada.

Debemos de tener cuidado con los cibercriminales, ya que estos utilizan email, sitios web, llamadas de teléfono, mensajes de texto e incluso mensajes por fax para sus estafas, aprovechando en este momento el miedo y el pánico de la población ante la pandemia de coronavirus COVIT-19.

La Federal Communications Comission (FCC) de los Estados Unidos ha recibido informes de campañas de mensajes de texto fraudulentos y llamadas automáticas de estafa acerca del COVIT-19 que ofrecen kits gratuitos de pruebas en el hogar, promueven curas falsas, venden seguros de salud y se aprovechan de los temores relacionados con el virus.

Los estafadores también están utilizando llamadas automáticas para dirigirse a los consumidores durante esta emergencia nacional.

La FCC ha recibido informes de llamadas automáticas que pretenden ofrecer kits de prueba de virus gratuitos, en un esfuerzo por recopilar información personal de los consumidores. Otras llamadas automáticas son la comercialización de curas falsas y la solicitud de pago por teléfono.

Recomendaciones

1. Verifica que la dirección de correo electrónico del remitente sea oficial:

   Hay que asegurarse de que la dirección electrónica contiene las siglas “who.int” después de la @.

2. Revisa el enlace antes de hacer clic:

   Asegúrate de que el enlace comienza con “https://www.who.int”, en el caso de la OMS.

3. Tenga cuidado cuando brinde sus datos personales:

   Es importante preguntarse para qué quiere alguien su información y si esto es apropiado. No hay razón para que alguien necesite su nombre de usuario o contraseña para acceder a información pública.

4. No se apresure ni se sienta bajo presión ante una solicitud de información:

Los cibercriminales utilizan emergencias, como el Covid-19, para que la gente tome decisiones rápidas. Tómese su tiempo cuando alguien le pida información personal para analizar si realmente es necesario brindarla. Tenga cuidado si está siendo presionado para compartir información o realizar un pago de inmediato.

5. Tenga instalado un antivirus y un antimalware en sus equipos para prevenir infecciones y descarga de malware.

6. Si es víctima de una estafa informática puede comunicarse a la línea confidencial del Organismo de Investigación Judicial 800-8000645

7. No responda llamadas o mensajes de texto de números desconocidos, o cualquier otro que parezca sospechoso.

8. Nunca comparta su información personal o financiera por correo electrónico, mensajes de texto o por teléfono.

9. Los estafadores a menudo falsifican números de teléfono para engañarlo para que responda. Recuerde que las agencias gubernamentales nunca lo llamarán para pedirle información personal o dinero.

10. No haga clic en ningún enlace en un mensaje de texto. Si un amigo le envía un mensaje de texto con un enlace sospechoso que parece fuera de lugar, llámelo para asegurarse de que no haya sido hackeado

11. Utilice fuentes oficiales para informarse, desconfíe de cadenas de mensajes que se desconoce la fuente oficial de la información brindada

Referencias

https://www.who.int/about/communications/cyber-security

https://www.fcc.gov/covid-scams

https://www.bbc.com/mundo/noticias-52009138

https://www.rcnradio.com/tecnologia/cuidado-la-estafa-que-suplanta-la-oms-para-pedir-donaciones-por-el-covid-19

En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr

MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2020.03.25 15:35:15 -06'00'

ROBERTO PAULO LEMAITRE PICADO (FIRMA)

Firmado digitalmente por ROBERTO PAULO LEMAITRE PICADO (FIRMA)
Fecha: 2020.03.25 15:44:32 -06'00'

Jorge Mora Flores
Director de Gobernanza Digital

Roberto Lemaitre Picado
Coordinador CSIRT-CR