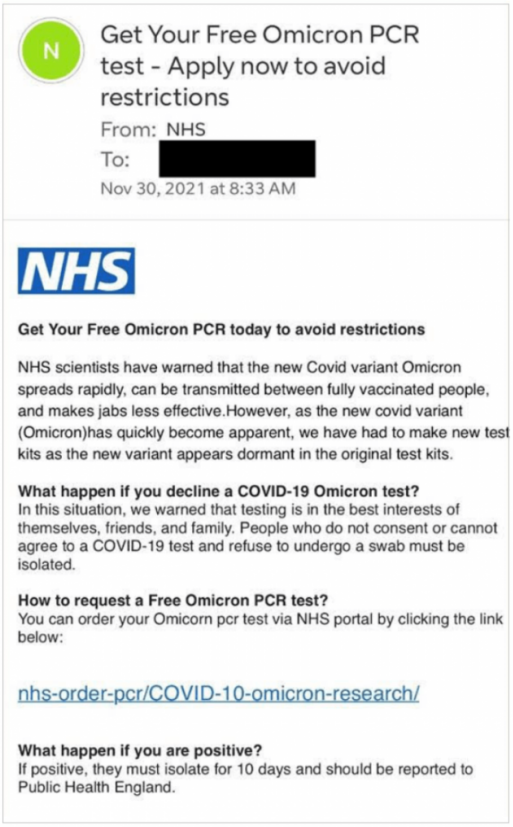
Estafadores aprovechan la preocupación por Omicron para una campaña de phishing

En un correo electrónico al que accedió este organismo, los cibercriminales se hacen pasar por el Servicio Nacional de Salud (NHS), que es el proveedor nacional de atención médica del Reino Unido, y ofrecen a las potenciales víctimas la oportunidad de obtener una "prueba PCR de Omicron gratuita" utilizando como pretexto que esto las ayudará a evitar las restricciones recientemente introducidas por el gobierno británico. El correo electrónico también afirma engañosamente que la nueva variante no es detectable por los kits de prueba utilizados para las anteriores variantes del COVID-19 y que se ha desarrollado un nuevo kit de prueba para ese propósito.



Fuente de la imagen: conversation.which.co.uk

"Existen diferentes versiones del correo electrónico que están circulando; por ejemplo, una contiene un enlace, mientras que en otra se accede al sitio mediante un botón. En cualquier escenario, el usuario es redirigido a un sitio web falso que suplanta la identidad del NHS y se solicita que complete un formulario ingresando su nombre completo, fecha de nacimiento, dirección, número de teléfono móvil y dirección de correo electrónico. Básicamente toda la información que un estafador necesitaría para llevar a cabo un caso bastante convincente de robo de identidad y fraude con el potencial de dejar las finanzas de la víctima en ruinas" señala Cecilia Pastorino, Especialista en Seguridad Informática del Laboratorio de Investigación de ESET

Latinoamérica.

Si bien en el correo se anuncia el test como gratuito, el sitio web solicita una tarifa de 1.24 libras, que equivale a unos 1.64 dólares. Además, como medida de prevención, incluye la opción de ingresar el apellido de soltera de su madre para utilizar como pregunta de seguridad; un enfoque que en realidad todavía se utiliza para ayudar a los usuarios a proteger sus cuentas online. En caso de que las víctimas sean engañadas y completen el formulario, han proporcionado efectivamente a los estafadores un plan para cometer robo de identidad y fraude. La organización Which? ha informado del sitio web al Centro Nacional de Seguridad Cibernética del Reino Unido.

Los actores maliciosos suelen cambiar la temática de sus estafas según cuáles sean los temas del momento para intentar obtener datos confidenciales de las personas y su dinero, por lo que no es una sorpresa que estén aprovechando las últimas noticias sobre la crisis del COVID-19.

ESET acercó algunas recomendaciones para evitar ser víctima de estafas similares:

- Si recibió un correo electrónico que dice ser de una organización oficial, consulte el sitio web de la entidad y comuníquese con ellos utilizando la información de contacto oficial para averiguar si realmente enviaron ese mensaje.
- No haga clic en enlaces ni descargue archivos que recibió en un correo electrónico no solicitado de una fuente que no conoce y que no puede verificar de forma independiente.
- Active la autenticación en dos pasos (2FA) al menos en las cuentas online más importantes e instale un software de seguridad de varias capas, que tenga buena reputación y que cuente con protección antiphishing.

“Además de llevar adelante una amplia variedad de estafas relacionadas con la vacuna COVID-19, los delincuentes también han apuntado a varias compañías farmacéuticas y organizaciones gubernamentales involucradas en el proceso de desarrollo, aprobación y distribución de vacunas. Por ejemplo, han comprometido un laboratorio de investigación de la Universidad de Oxford que realiza investigaciones sobre formas de combatir el virus y documentos robados de la Agencia Europea de Medicamentos, por nombrar solo algunas campañas e incidentes en los últimos casi dos años”, concluye Cecilia Pastorino, Especialista en Seguridad Informática del Laboratorio de Investigación de ESET Latinoamérica.