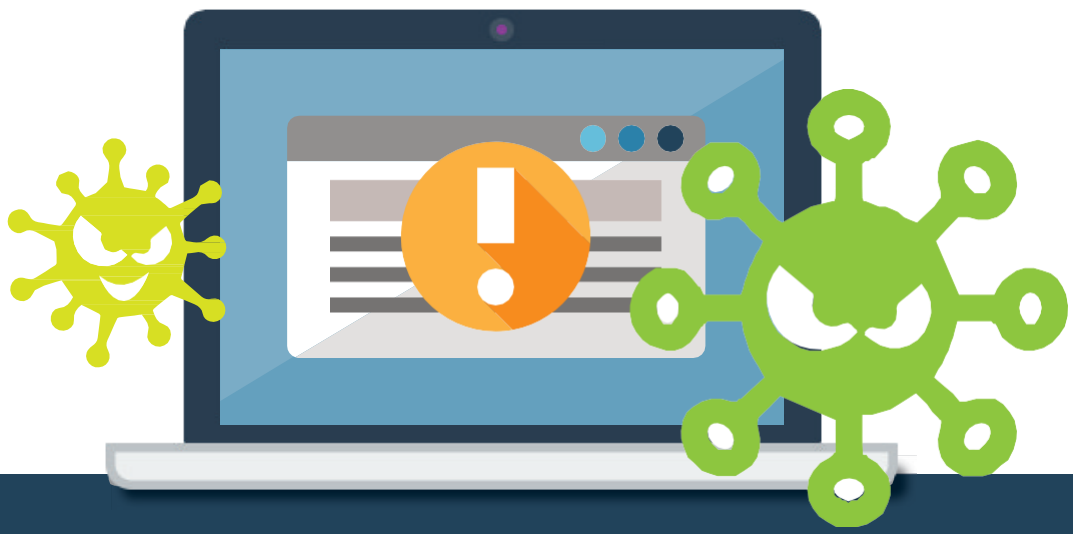
⚠ CORONAVIRUS ALERTA DE ESTAFA ⚠



¡Cuidado con estas estafas!

Después que ocurren fenomenos globales, desastres naturales, o pandemias como COVID-19, a menudo hay un aumento oportunista de la actividad criminal en internet.

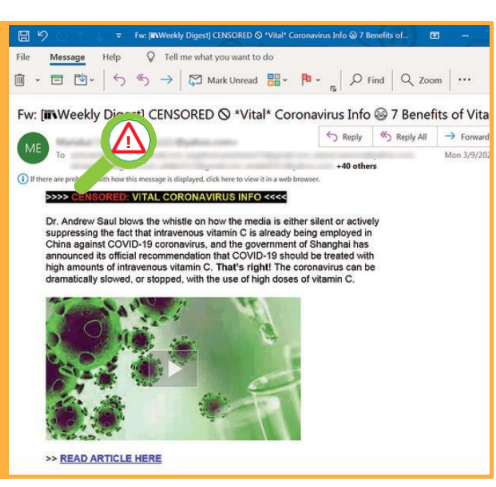
Los malos se están aprovechando de su miedo y envían todo tipo de estafas relacionadas con el Coronavirus (COVID-19).

A continuación se presentan algunos ejemplos de los tipos de estafas que deben tener en cuenta:

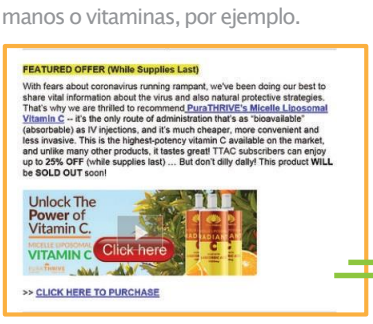
SITIOS WEB MALICIOSOS

Sitios Web Maliciosos... Con el propósito de infectar su dispositivo con malware. Tenga cuidado con sitios como **Coronavirus(.)com** o **Corona-virus-Map(.)com**. Desde enero se han registrado miles de sitios web que contienen la palabra 'corona' y muchos de ellos son sospechosos. Algunos de estos sitios web distribuyen malware.

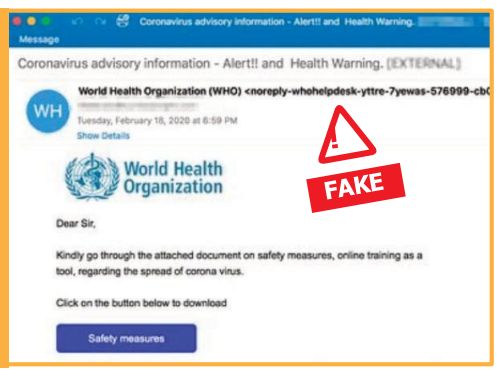
CORREOS SPAM



Correos electrónicos no deseados ... Tratando de captar su curiosidad usando frases de temáticas capciosas como "censuras", para tratar de vender información (videos pagos) o productos que ahora tienen una gran demanda como máscaras, desinfectantes de manos o vitaminas, por ejemplo.

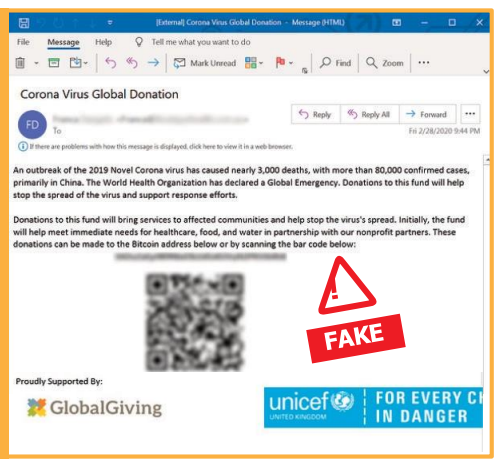


ESTAFAS DE PHISHING



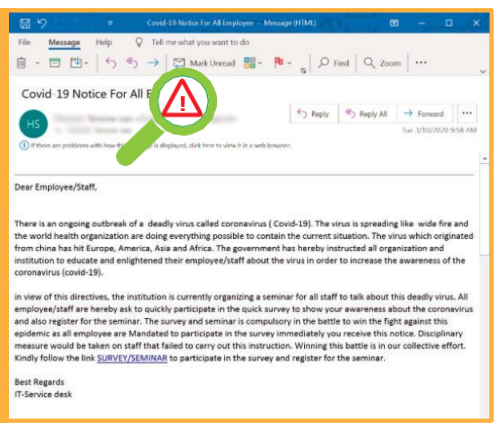
Estafas de Phishing ...que parecen provenir de organizaciones como los CDC (Centros para el Control de Enfermedades) o la OMS (Organización Mundial de la Salud). Los estafadores han creado correos electrónicos que parecen provenir de estas Fuentes, pero en realidad contienen enlaces maliciosos de phishing o archivos adjuntos peligrosos. También hay correos electrónicos que afirman tener una lista "nueva" o "actualizada" de casos de Coronavirus en su sector. Estos correos electrónicos contienen enlaces peligrosos.

FALSAS CARIDADES



Falsas caridades ...correos electrónicos y sitios web que solicitan donaciones de caridad para estudios, médicos o victimas que han sido afectados por el Coronavirus COVID-19. Los estafadores a menudo crean correos electrónicos de caridad falsos después de desastres globales o pandemias como el brote de COVID-19.

COMUNICACIONES FALSAS DE RH O IT



Comunicación interna falsa de recursos humanos o TI ...como encuestas de coronavirus que se hacen pasar por su departamento de recursos humanos o de TI. El objetivo aquí es robar su nombre de usuario y contraseña.

Para accede al 'documento' o 'encuesta', el destinatario debe proporcionar sus credenciales de Office365 en un sitio falso, lo que compromete su cuenta de Office 365.

¡Sé Cauteloso! Protégete de estafas como esta:

- Nunca haga click en enlaces o abra archivos adjuntos de un correo electrónico que no esperaba.
- Si recibe un correo electrónico sospechoso que parece provenir de una organización oficial como la OMS o de la Secretaria de Salud, **reporte el correo electrónico** a su equipo de Seguridad para verificarlo.
- Si desea hacer una donación de caridad, vaya al sitio web de caridad de su elección para enviar su pago. **Escriba la dirección web de la organización benéfica en su navegador** en lugar de hacer click en los enlaces de correos electrónicos u otros mensajes.

KnowBe4
Human error. Conquered.