EL CORONAVIRUS EN LA WEB

La tecnología de los antivirus ha detectado alrededor del mundo, archivos relacionados al **coronavirus**; una enfermedad viral que está presente en los titulares de medios de comunicación de todo el mundo debido a su peligrosa naturaleza.

Y esto ha sido aprovechado por los ***ciberdelincuentes***. Circula un supuesto video que contiene información para prevenir la enfermedad, y en realidad son **archivos maliciosos** disfrazados como **pdf**, **mp4**, **docx**, que contienen **troyanos** hasta **gusanos** capaces de **destruir, bloquear, modificar o copiar datos**, así como interferir en el funcionamiento de computadores o redes empresariales.

A medida que el **miedo** crece alrededor del mundo por este virus, es muy probable que esta tendencia crezca. A medida que la gente siga preocupada por su salud, se seguirá propagando más **malware oculto** en documentos falsos sobre el coronavirus.

Es por ello que para evitar ser víctima de estas trampas se recomiendan las siguientes medidas:

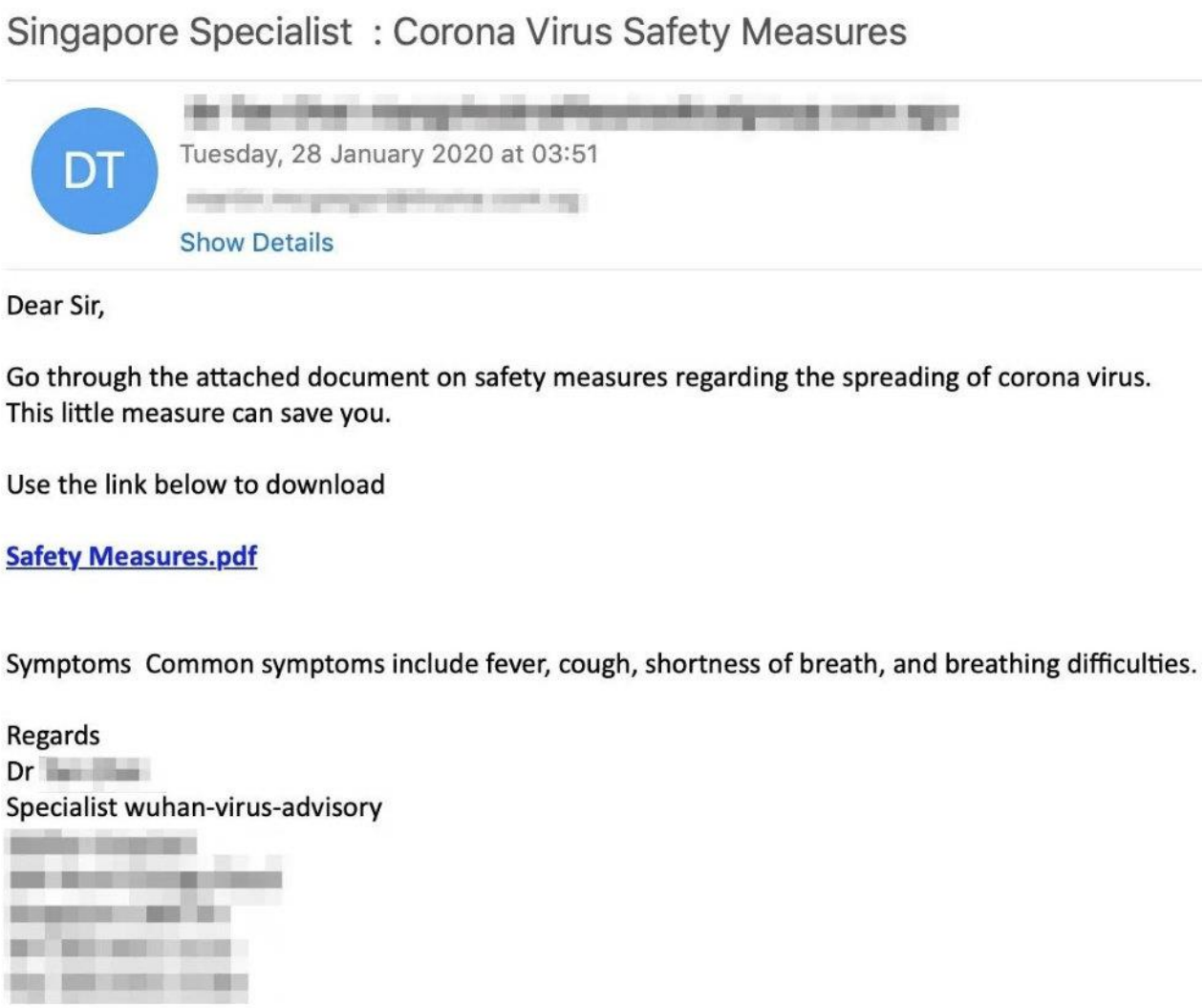
1. **Evita** los enlaces **sospechosos** que prometen contenido exclusivo. Remítase a las fuentes **oficiales** para obtener información confiable y legitima

2. Fíjese en la **extensión de los archivos descargados**. Los documentos y archivos de video no deben tener formato .**exe** o **lnk**.

3. Si necesitas información acerca del virus, **realiza una búsqueda común** en el navegador**, no confíes** en archivos enviados a través de un correo electrónico y que se relacionen al coronavirus.

4. **Se cuidadoso** en la navegación por internet, con la popularidad que tiene este tema puede utilizarse en cualquier tipo de trampa. Ten cuidado con el contenido que se relacione al **“Coronavirus”**.

A continuación, un ejemplo de envío de correo malicioso, con un **supuesto** **PDF** que contiene información acerca de la enfermedad.



Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

Safety Measures.pdf

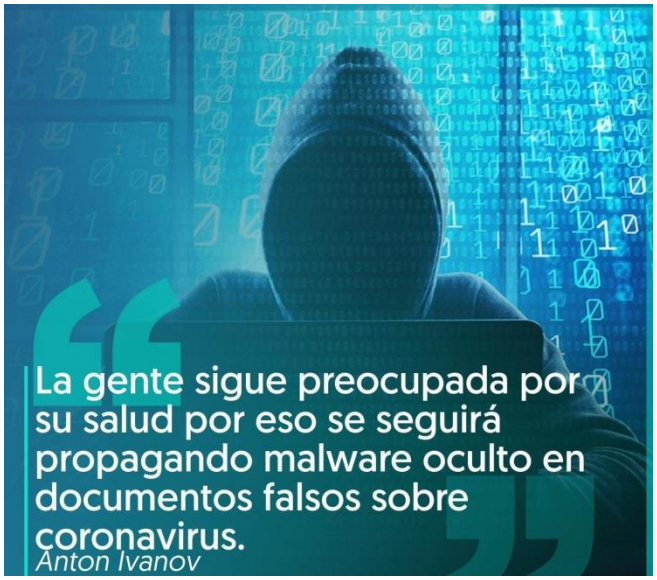
Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

CONTINÚA EL PHISHING CON TEMÁTICA DE CORONAVIRUS

Los ciberatacantes siguen aprovechando el coronavirus para ataques de **phishing**.

La Organización Mundial de la Salud (OMS) ha advertido a los usuarios de Internet que tengan **cuidado con los ataques de phishing con temática de coronavirus** que *«suplantan a las organizaciones»* con el **objetivo de robar información** y **difundir malware.** Recientemente se ha tenido constancia de una serie de campañas de **phishing** que utilizan técnicas de **ingeniería social** para aprovechar los temores globales de la amenaza de coronavirus con el fin de **engañar** a los usuarios y lanzar con éxito ataques cibernéticos.



Estos ataques muestran hasta donde son capaces de llegar los crackers cuando intentan sortear las ciberdefensas, pero los ataques de phishing en sí mismos no son nada nuevo. Según una investigación**, el 60%** de las organizaciones mencionan los **ataques externos como el phishing**, como uno de los **mayores riesgos de seguridad** a los que se enfrenta actualmente una organización, por delante de otras técnicas populares como el **ransomware**. Esto se debe a que los ciberatacantes **siguen buscando** el camino de menor resistencia. Los correos electrónicos de phishing bien diseñados**, especialmente aquellos que juegan con los miedos de las personas**, a menudo funcionan. Los atacantes suelen utilizar estas tácticas para establecerse dentro de las organizaciones para luego acceder a credenciales privilegiadas, aquellas que otorgan control sobre datos confidenciales o **sistemas críticos**.

El estudio revela que el **50%** de las organizaciones **no puede evitar** que los **piratas informáticos** se infiltren en su negocio cada vez que lo intentan, y consideran necesario **limitar los lugares a los que pueden acceder**. Para salvaguardar la continuidad del negocio, las empresas deben 1) **Administrar proactivamente** los privilegios, 2) **limitar el acceso** a la información a quienes lo requieran y 3) **aislar** las áreas comprometidas de inmediato, en caso de un **ataque**.

Es inevitable que un empleado caiga en la trampa de un ciberdelincuente, **no importa lo preparado que esté**. Pero un empleado **informado** será capaz de **detectar** alguna de estas trampas y **evitar que su empresa se vea comprometida**.

Las trampas por coronavirus CONTINUAN, no abras contenido con esta temática.

EJEMPLOS DE CORREOS FALSOS CON INFORMACIÓN DE CORONAVIRUS