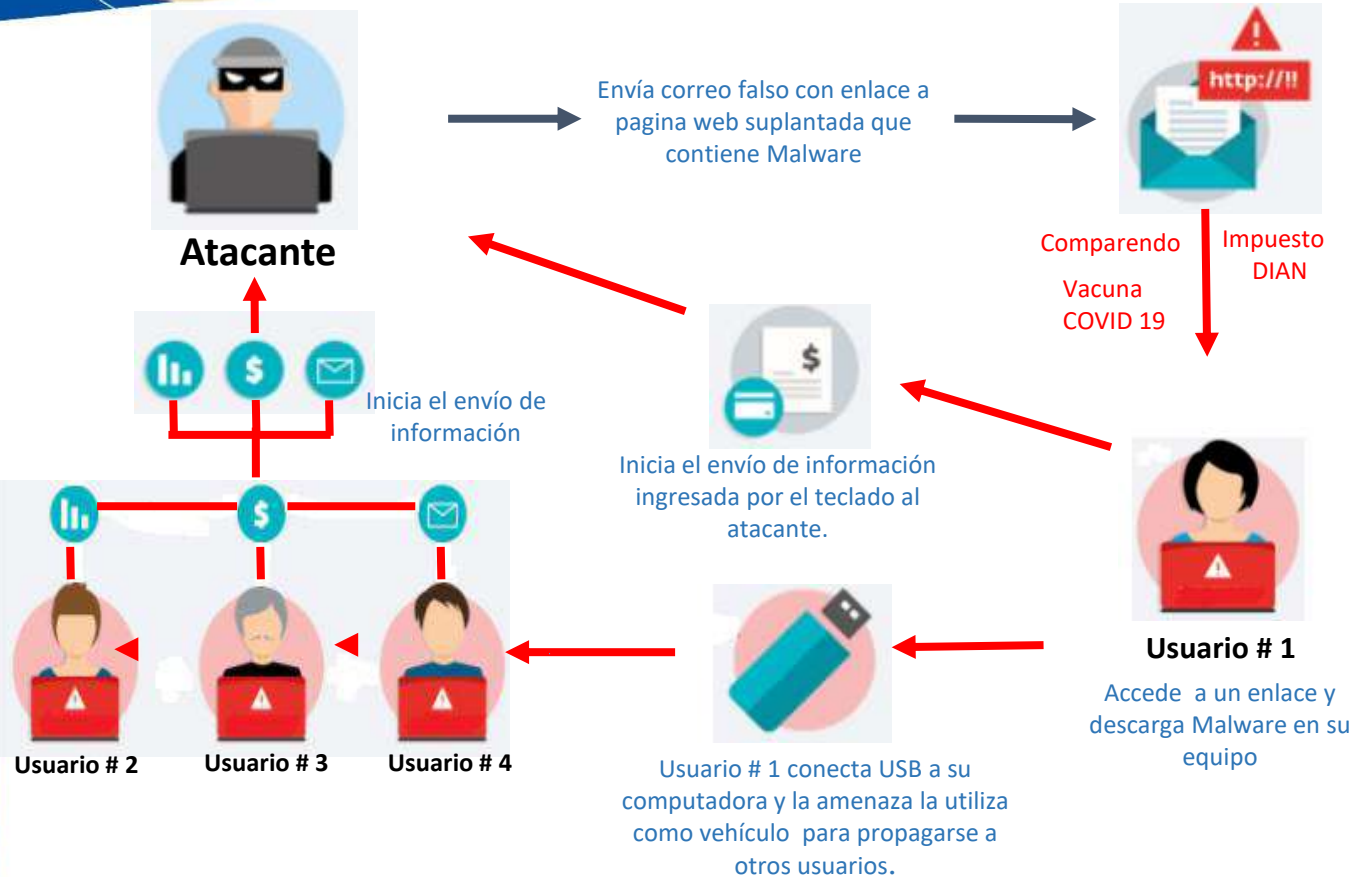


BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA



¡ENTERATE! Como funciona un KEYLOGGER



Evite ser víctima de un ataque con Keylogger (*Envío de información ingresada por teclado al delincuente*)

- No abra correos de dudosa reputación ni descargue documentos adjuntos.
- Acceda a los sitios web desde el navegador ingresando la URL de forma manual y no desde un correo electrónico.
- Cerciórese de tener un antivirus Instalado y actualizado.
- No utilice memorias USB para compartir archivos, utilice medios digitales.
- Si recibe un correo sospechoso, repórtelo a Seguridad Informática.



**Universidad
de Santander**

Personería Jur. 810 de 12/03/96 Min.Educación **UDES**



BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

¡ALERTA! SEGUNDA CAMPAÑA MALICIOSA a través de correo electrónico Vacunación Covid 19

Mediante segunda campaña maliciosa sobre vacunación contra COVID 19, ciberdelincuentes pretenden robar información personal y/o financiera; en el correo falso se envía un mensaje indicando agendamiento para vacunación en el Plan Nacional de Vacunación.

La recomendación es tener en cuenta información solo de sitios oficiales, si recibe este tipo de mensajes, no descargue archivos adjuntos por que puede descargando virus en su equipo sin darse cuenta, por que se realiza de forma transparente para el usuario, elimine el mensaje de inmediato e informe de su recepción al Área de Seguridad Informática.



Tomado y adaptado de: <http://www.colcert.gov.co/>



**Universidad
de Santander**
Personería Jur. 810 de 12/03/96 Min.Educación **UDES**



BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

¡ALERTA! Phishing Falsa Campaña emergencia sanitaria

From: hacienda vijes-valle.gov.co <hacienda@vijes-valle.gov.co>
Sent: Tuesday, April 13, 2021 9:38 AM
Subject: --Importante- emergencia sanitaria requerimiento

-Importante-

Abril 13

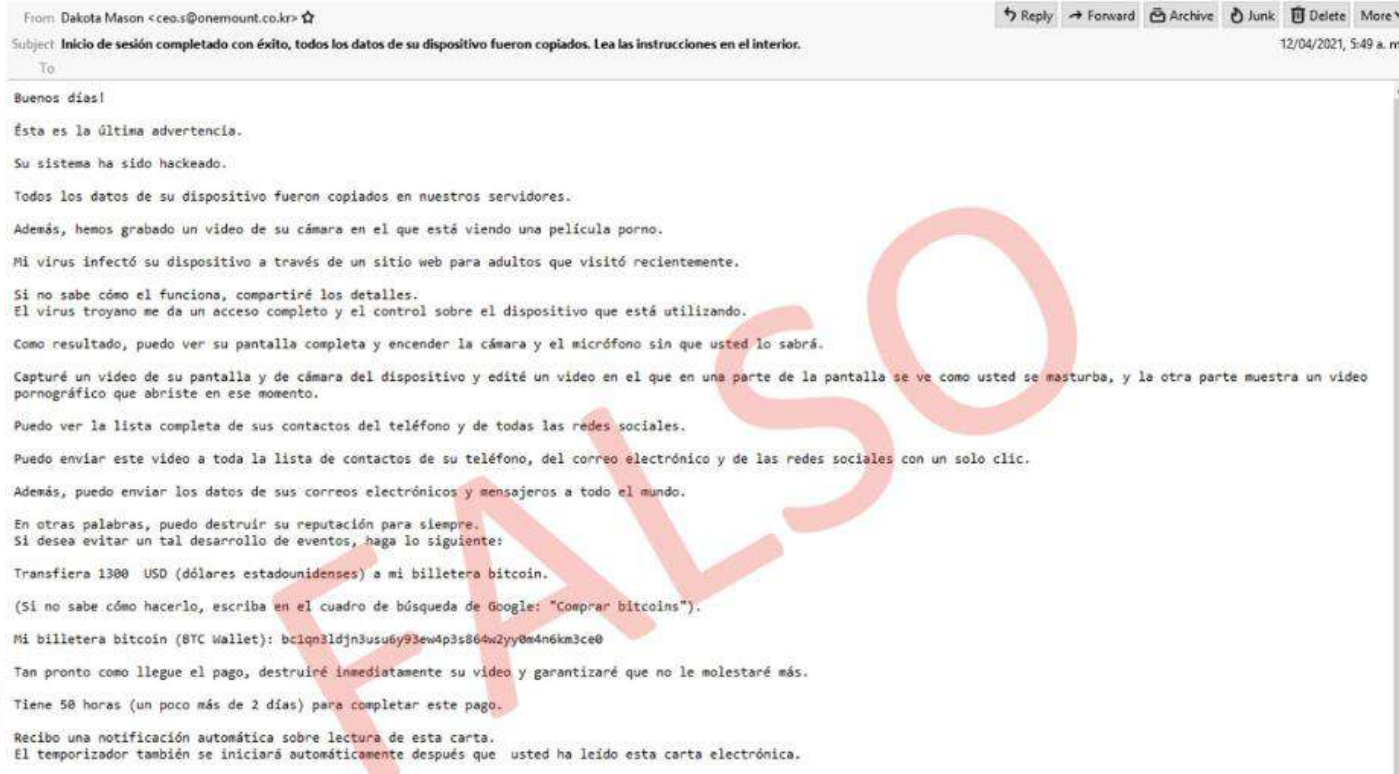
Informamos y requerimos información.

La idea es informar lo que está pasando y lo que pasara con la economía en los próximos días en el país por el motivo del Covid.-19 y el nuevo pico que está en proceso.

Está circulando en la red un correo electrónico con asunto **"Importante emergencia sanitaria requerimiento"** el cual contiene link con Malware y permite a los ciberdelincuentes tomar control del equipo y robar datos personales y financieros. La recomendación es informar a Seguridad Informática y eliminar de inmediato el mensaje.

BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

¡ALERTA! Correo fraudulento



Falso correo electrónico con el asunto: **"Inicio de sesión completado con éxito, todos los datos de su dispositivo fueron copiados..."** está siendo enviado para extorsionar a las personas indicando un supuesto ¡sistema hackeado!. El mensaje es falso, la recomendación es informar a Seguridad Informática y eliminar de inmediato el mensaje.

Tomado y adaptado de: <http://www.colcert.gov.co/>



**Universidad
de Santander**
Personería Jur. 810 de 12/03/96 Min.Educación **UDES**



BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

¡ALERTA! Falsa campaña por WhatsApp

Falsa Noticia circula a través de la aplicación de mensajería WhatsApp en la cual se informa sobre un supuesto bono de ayuda por parte del Gobierno Nacional. Elimine el mensaje y no lo comparta ;cuide sus datos personales!

Hola, acabo de hacer la solicitud para el bono de \$500,000 Pesos, y me aprobaron. Te lo estoy mandando a ti para que también puedas obtener los beneficios. La solicitud es RAPIDA haciendo clic aquí... ➡ <http://bit.ly/solicitarbono>

