Ciberseguridad

ETITC

Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

Boletín Informativo No. 01 de 2023

Campaña de Ingeniería Social

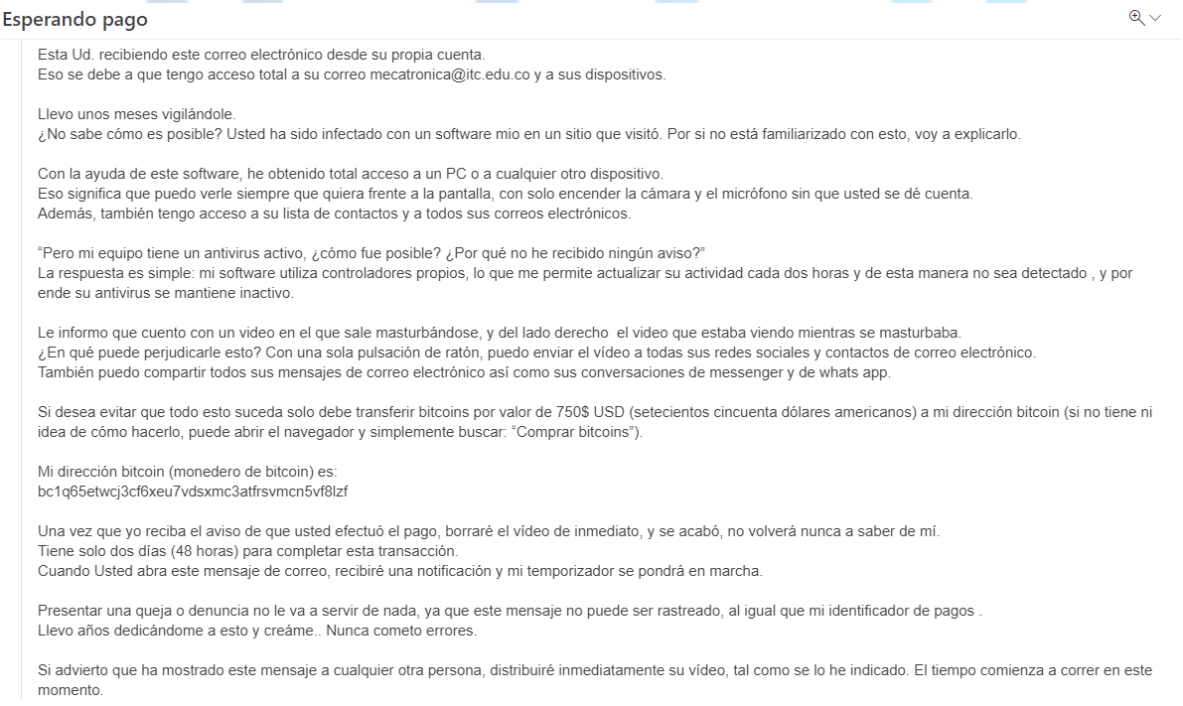
11 de enero de 2023

¿HAS RECIBIDO UN CORREO INSTITUCIONAL DESDE TU MISMA CUENTA, CHANTAJEÁNDOTE?

Desde la semana anterior se ha detectado una campaña de sextorsión bajo la técnica de "MAIL SPOOFING", donde los ciberdelincuentes suplantaron las direcciones de correos institucionales de nuestro dominio @itc.edu.co, con el fin de engañarlos y hacerles creer que han conseguido instalar malware y/o troyano en su dispositivo y que puede ver observarlo(a) todo el tiempo.

A través de está extorsión incita a sus víctimas a abonar una cantidad de dinero a una cuenta monedero de BITCOIN, a cambio de no divulgar información íntima o privada que supuestamente ha encontrado en el dispositivo o cuenta institucional.

A continuación, anexo screenshots sobre el mensaje recibido:



Esperando pago

Esta Ud. recibiendo este correo electrónico desde su propia cuenta.
Eso se debe a que tengo acceso total a su correo mecatronica@itc.edu.co y a sus dispositivos.

Llevo unos meses vigilándole.
¿No sabe cómo es posible? Usted ha sido infectado con un software mio en un sitio que visitó. Por si no está familiarizado con esto, voy a explicarlo.

Con la ayuda de este software, he obtenido total acceso a un PC o a cualquier otro dispositivo.
Eso significa que puedo verle siempre que quiera frente a la pantalla, con solo encender la cámara y el micrófono sin que usted se dé cuenta.
Además, también tengo acceso a su lista de contactos y a todos sus correos electrónicos.

"Pero mi equipo tiene un antivirus activo, ¿cómo fue posible? ¿Por qué no he recibido ningún aviso?"
La respuesta es simple: mi software utiliza controladores propios, lo que me permite actualizar su actividad cada dos horas y de esta manera no sea detectado , y por ende su antivirus se mantiene inactivo.

Le informo que cuento con un video en el que sale masturbándose, y del lado derecho el video que estaba viendo mientras se masturbaba.
¿En qué puede perjudicarle esto? Con una sola pulsación de ratón, puedo enviar el vídeo a todas sus redes sociales y contactos de correo electrónico.
También puedo compartir todos sus mensajes de correo electrónico así como sus conversaciones de messenger y de whats app.

Si desea evitar que todo esto suceda solo debe transferir bitcoins por valor de 750$ USD (setecientos cincuenta dólares americanos) a mi dirección bitcoin (si no tiene ni idea de cómo hacerlo, puede abrir el navegador y simplemente buscar: "Comprar bitcoins").

Mi dirección bitcoin (monedero de bitcoin) es:
bc1q65etwcj3cf6xeu7vdsxmc3atfrsvmcn5vf8lzf

Una vez que yo reciba el aviso de que usted efectuó el pago, borraré el vídeo de inmediato, y se acabó, no volverá nunca a saber de mí.
Tiene solo dos días (48 horas) para completar esta transacción.
Cuando Usted abra este mensaje de correo, recibiré una notificación y mi temporizador se pondrá en marcha.

Presentar una queja o denuncia no le va a servir de nada, ya que este mensaje no puede ser rastreado, al igual que mi identificador de pagos .
Llevo años dedicándome a esto y creáme.. Nunca cometo errores.

Si advierto que ha mostrado este mensaje a cualquier otra persona, distribuiré inmediatamente su vídeo, tal como se lo he indicado. El tiempo comienza a correr en este momento.

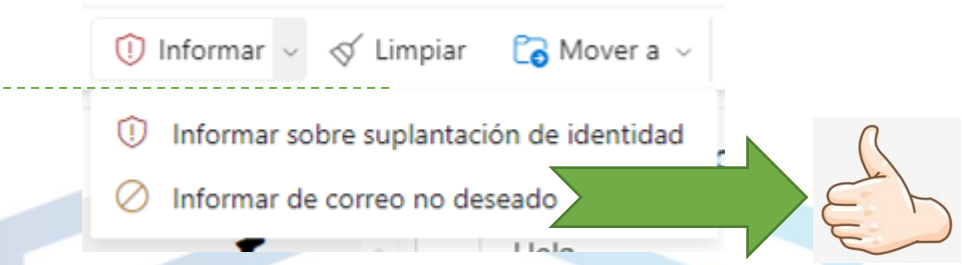
¿AQUÍ TE CONTAMOS QUE HACER EN CASO DE RECIBIRLO?

Paso 1. Reportarlo al correo de Mesa de Servicios (mesadeayuda@itc.edu.co)

Si no tienes la certeza de que algo sea cierto o no conoces el remitente, sugiero que no lo reenvíes y adopta una postura crítica, incluso ante información que confirme tus creencias antes de compartirla. Frecuentemente, las noticias que parecen inverosímiles suelen ser falsas.

Si no tienes la certeza de que algo sea cierto o no conoces el remitente, sugiero que no lo reenvíes y adopta una postura crítica, incluso ante información que confirme tus creencias antes de compartirla. Frecuentemente, las noticias que parecen inverosímiles suelen ser falsas.

Paso 2. Marca el mensaje como: “Informar de correo no deseado”



RECOMENDACIONES

1. Activa la doble autenticación de su correo institucional.
2. Cambia frecuentemente su contraseña incluyendo como mínimo 8 caracteres incluyendo letras mayúsculas, minúsculas, símbolos especiales y números.
3. No abrir ningún enlace web – URL.
4. No descargar archivos adjuntos de este correo sospechoso.
5. Verificar las direcciones de correo electrónico de quién remite antes de iniciar cualquier acción en el mismo.
6. Bloquear inmediatamente el remitente del correo electrónico.
7. Participa en los talleres de sensibilización del Sistema de Gestión de Seguridad de la Información programados desde Talento Humano.

Finalmente, deseamos conocer su percepción, expectativas y necesidades del Sistema de Gestión de Seguridad de la Información para la vigencia 2023, has clic aquí: https://forms.office.com/r/JyPf1pYdAa

Cordialmente,

Ing. Sandra J. Guerrero G.
Gestión de Seguridad de la Información
seguridaddigital@itc.edu.co
seguridaddigital