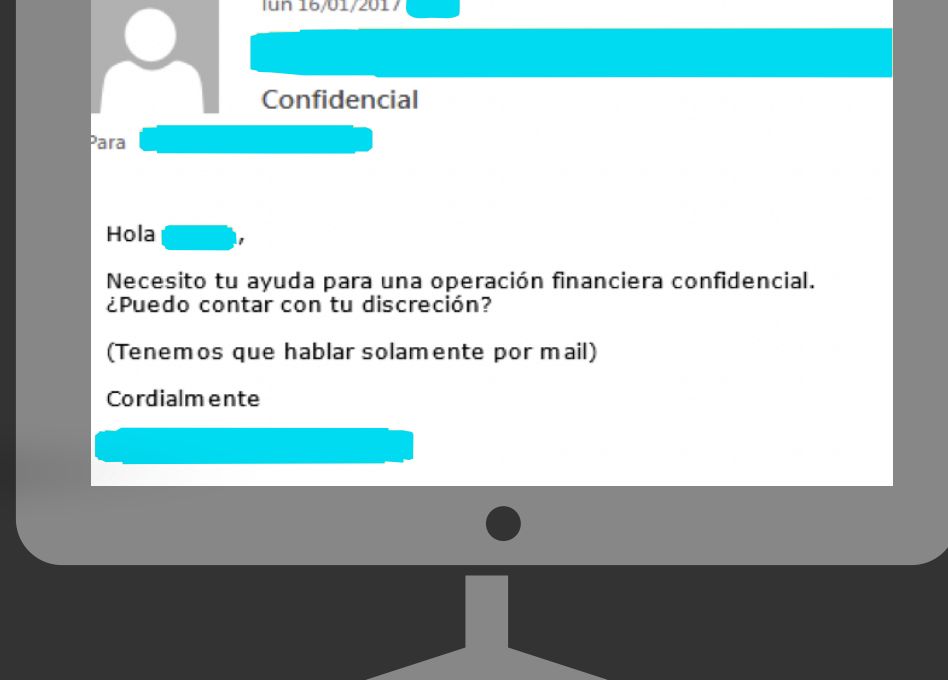


CIBERATAQUES DIRIGIDOS

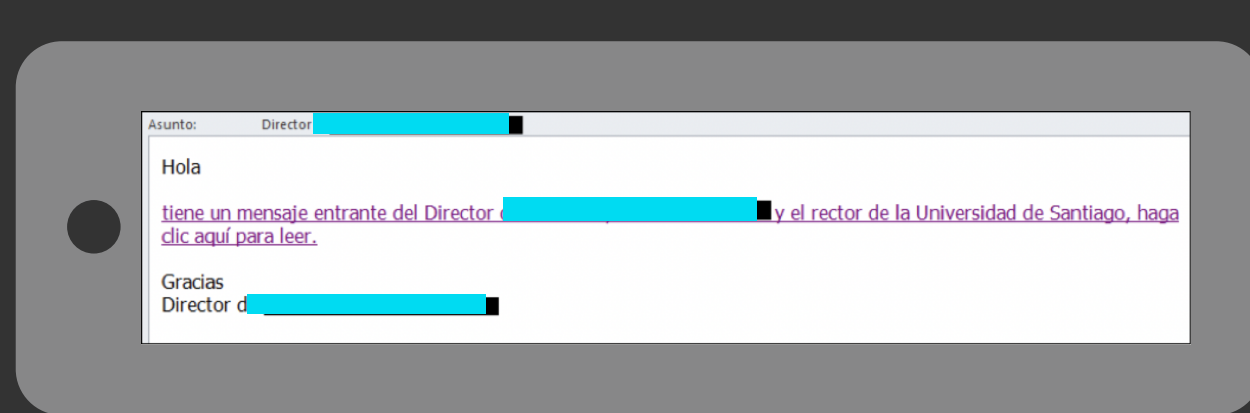


Suplantar la identidad de forma pública o dentro de las organizaciones es bastante recurrente por parte de los cibercriminales. Las consecuencias de estos ataques son difíciles de cuantificar, muchas veces porque las personas afectadas se enteran muy tarde de la estafa o porque se rehúsan a compartir públicamente que fueron víctimas. En qué consisten estos ataques y cómo prevenir, ¡te contamos a continuación!

ATAQUE AL CEO El cibercriminal se aprovecha de un error en un mando medio de la organización para explotar la confianza y así obtener réditos, por lo general, económicos. Un ataque de este tipo puede iniciar con un correo electrónico proveniente del presidente o gerente general de una compañía, como, por ejemplo:



ATAQUE SPEAR PHISHING El objetivo es obtener credenciales de ingreso, información confidencial o esparcir malware en una entidad determinada. El spear phishing es más difícil de detectar, ya que el atacante realizó una investigación previa sobre la víctima, por lo tanto, el mensaje no le parecerá extraño a la víctima, y al igual que en el ataque al CEO, se hará pasar por un conocido o una persona con autoridad.



ATAQUE SUPLANTACIÓN DE LA IMAGEN PÚBLICA

El uso de la imagen de personas, marcas o instituciones es muy recurrente. Los cibercriminales explotan la imagen de una figura para persuadir a otras de imitarlo. A partir de ello, arma una trama capaz de lograr que las personas realicen depósitos en bitcoins.



¿QUÉ ES LA CRIPTOMONEDA? Es un tipo de moneda digital que está basado en código informático. Funcionan de forma autónoma y difieren significativamente de las monedas tradicionales. La utilidad de las bitcoins para los cibercriminales es muy alta. Las criptomonedas proporcionan una forma sencilla para que los delincuentes exijan el pago y proporcionan un método para blanquear el producto de los delitos informáticos.

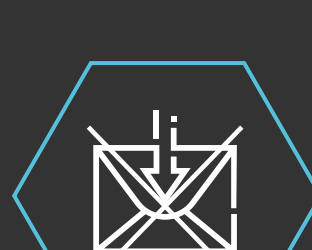


¿CÓMO PREVENIR?



REVISA el correo del remitente. Los atacantes usan una pequeña variante del correo para parecer creíble o también hackean cuentas.

CONFIRMA la información que recibes, llamando a la persona o al CEO de la empresa.



NUNCA RESPONDAS este tipo de correos y duda si te solicitan pagos en criptomonedas.

NO DESCARGUES archivos o abras enlaces de dudosa procedencia, pueden contener malware.



LIMITA la información que compartes en redes sociales, especialmente para los CEOs.