¡ALERTA, CIBERFRAUDE!

¿Qué es una estafa de mulas de dinero?
Consejos para estar seguro en Internet

BOLETíN N° 17

Enero - Marzo 2024

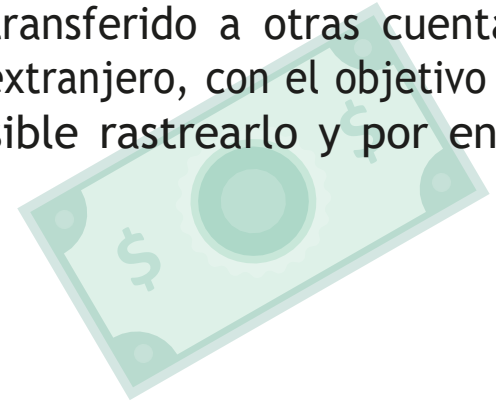
Universidad de Santander
UDES
VIGILADA MINEDUCACIÓN | SNIES 2832
ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN

Estafa de mulas de dinero

El ciberfraude se incrementa; cada día los ciberdelincuentes buscan nuevas vías para saltarse los controles de las entidades financieras y ejecutar delitos intentando esquivar responsabilidades. A veces la forma de "esquivar" radica precisamente en cargarle el delito a otro.

¿Qué es una cuenta mula?

Una mula financiera o "cuenta mula" es una figura intermediaria que es usada para recibir dinero obtenido de forma fraudulenta (generalmente a través de phishing, malware, etc.) que posteriormente es transferido a otras cuentas, generalmente en el extranjero, con el objetivo de que sea casi imposible rastrearlo y por ende recuperarlo.



¿Cómo se capta una cuenta mula?

Uno de los ganchos más utilizados consiste en las falsas ofertas de trabajo; prometen sumas cuantiosas de dinero, con esfuerzo mínimo y apenas conocimiento.

Estas ofertas suelen postearse en webs o redes sociales cuyo propósito no es precisamente el perfil laboral, tales como Facebook, Instagram, etc.

El dinero fácil busca aprovecharse de personas vulnerables con el objetivo de utilizar su situación de necesidad para enriquecerse.

Otras vías

Prestamistas que "por error" transfieren una cantidad de dinero superior al pactado y solicitan enviarlo a una cuenta distinta.

Falsos romances online que requieren enviar una transferencia a un familiar o amigo y no pueden ejecutarlo desde sus cuentas personales… la lista es larga, el propósito es el mismo, hacerte llegar una cantidad de dinero, para que la remitas a una segunda cuenta y actúes como "mulero".

Fuente: https://uniblog.unicajabanco.es/cuentas-mula-di-no-al-ciberfraude

Tips para protegernos de las estafas de mulas

- Cuidado con la publicidad en la que te ofrecen sumas de dinero muy altas, sin salir de casa, sin ningún tipo de conocimiento o condiciones previas, por lo general este tipo de anuncios buscan aprovecharse de las necesidades o ambiciones.
- Si estás aplicando a un empleo, verifica las direcciones de correo desde las que te contactan, investiga a la empresa en Internet y cerciórate de que, en efecto, es una empresa legítima.
- Si recibes una transferencia que no estabas esperando, infórmalo a tu oficina antes de devolverlo con las condiciones que indique el remitente, este supuesto error puede ser una estrategia para blanquear dinero.
- Si un familiar o amigo te solicita transferir dinero usando tu cuenta, y decides hacerlo cerciórate de que no sea una operativa fraudulenta.
- Cuida tus datos personales y tus documentos de identificación, no los envíes nunca a desconocidos.
- Si sospechas que puedes estar siendo utilizado como cuenta mula, denúncialo en tu banco y a las autoridades pertinentes.

Fuente: https://uniblog.unicajabanco.es/cuentas-mula-di-no-al-ciberfraude

Consejos para estar seguro en Internet

Haz una buena gestión de tus contraseñas

Las contraseñas están diseñadas para proteger las cuentas que tenemos en diferentes portales, tiendas o productos por suscripción.

Deben ser seguras, evitando que sean fáciles de relacionar con el usuario, evitar fechas de cumpleaños, nombres, apellidos, placas de vehículos, números de documentos de identidad o de teléfonos.

Evitar utilizar la misma contraseña en todos los sitios (cuentas de correo, servicios de streaming, tiendas virtuales y demás sitios gratuitos o de suscripción). Es importante tener una contraseña para cada sitio y cambiarla de forma periódica.

Una buena forma de crear contraseñas seguras es mediante alguna de las muchas páginas que pueden generar estos contenidos de forma aleatorio incluyendo números, letras mayúsculas y minúsculas y caracteres especiales. Eso sí, deberás guardarla en algún gestor de contraseñas o, también, en una agenda física.

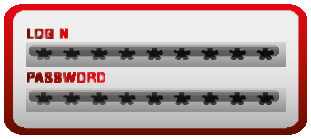
Activa la autenticación de dos factores (2FA) para añadir una capa adicional de seguridad contra esquemas de ataque comunes como el phishing, la ingeniería social y los ataques de fuerza bruta para el robo de contraseñas.

Fuente: https://www.microcad.es/ciberseguridad/consejos-seguridad-informatica/

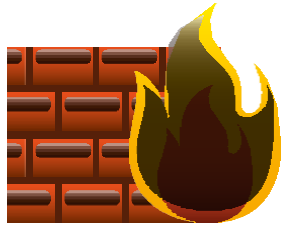
Consejos para estar seguro en Internet

Actualiza siempre el software básico

Mantener actualizado el sistema operativo es importante ya que la mayoría de las actualizaciones suelen ser parches realizados para cubrir problemas técnicos o brechas de seguridad informática.



Los malware se actualizan constantemente no podemos dejar atrás el sistema operativo de nuestros equipos ni la base de datos o versiones de los antivirus.



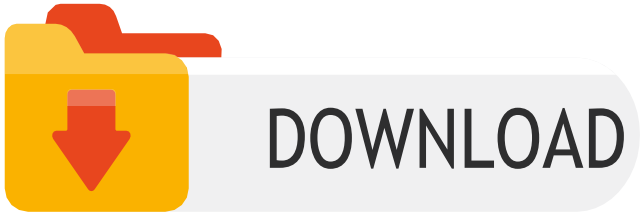
Solamente con mantener actualizados nuestros equipos, aplicaciones y antivirus estaremos reduciendo el riesgo de programas malintencionados que buscan hacerse a nuestros datos u ocasionar daños y mal funcionamiento alsistema operativo de nuestros equipos.

Fuente: https://www.microcad.es/ciberseguridad/consejos-seguridad-informatica/

Consejos para estar seguro en Internet

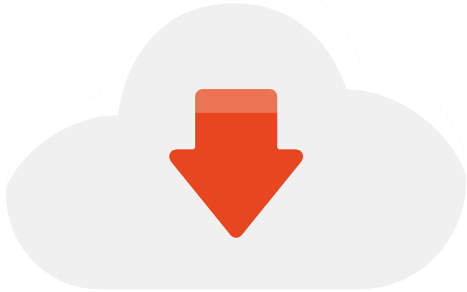
Cuidado con las descargas y adjuntos

Cuando se está navegando por algunos sitios web abundan los anuncios, ofertas, promociones y contenido llamativo; mediante ventanas emergentes o enlaces directos a descargas de ejecutables buscan ser abiertos por los usuarios, en ocasiones se disfrazan de utilidades como compresores, lectores de documentos e incluso como antivirus; de esta manera son instalados y terminan perjudicando nuestros equipos.



Con los adjuntos de correos electrónico hay que tener especial cuidado, ya que pueden verse comprometidos o pueden tener malware que al ser ejecutados afectan el normal comportamiento de los equipos de cómputo o dispositivos móviles.

Las descargas que se dan dentro de las páginas web y los adjuntos de los correos electrónicos siempre son llamativos y suelen despertar el interés de los usuarios mostrándose como aplicaciones que facilitan la realización de tareas o notificaciones de entidades públicas/privadas que quieren brindar información de reportes, infracciones, estados de procesos judiciales.



Fuente: https://www.microcad.es/ciberseguridad/consejos-seguridad-informatica/

CONTÁCTANOS

Si presentas dudas o detectas alguna situación sospechosa puedes comunicarte con el subproceso de seguridad informática UDES:

Bucaramanga

seguridadinformatica@udes.edu.co
Teléfono (607) 6516500 ext. 1005-1001

Valledupar

lortiz@valledupar.udes.edu.co
Teléfono: (605) 5730073 ext. 129

Cúcuta

wpena@udes.edu.co
Teléfono: (607) 5748717 ext. 4196