MONEY MULING

Public awareness and prevention

More than 90% of money mule transactions are linked to cybercrime. The illegally obtained money often comes from phishing, malware attacks, online auction fraud, e-commerce fraud, business e-mail compromise (bec) and CEO fraud, romance scams and holiday fraud (booking fraud) and many others.

WHAT IS MONEY MULING?

- A money mule is a person who transfers illegally obtained money between different payment accounts, very often in different countries, on behalf of others.
- Money mules are also recruited by criminals to receive money into their bank account, in order to withdraw the money and in most cases wire it overseas, receiving a commission payment in return for the provided services.
- Even if money mules are not involved in the crimes which generate the money (cybercrime, payment and on-line fraud, drugs and human trafficking, etc.), they are acting illegally by laundering the proceeds of crime, helping criminal syndicates move funds easily around the world and remain anonymous.
- If you are caught acting as a money mule, even if done so unwittingly, you can face a prison sentence, fine or community service, and the prospect of never again being able to secure a mortgage or open a bank account.
MONEY MULING

The mule is a person who transfers illegally obtained money between different payment accounts, very often in different countries, while earning a commission payment.

Criminals recruit victims using different methods:
- Direct contact in person or through email
- Social media (i.e. Facebook posts on closed groups)
- Instant messaging apps
- Online posting
- Seemingly legitimate job adverts (i.e. "money transfer agents")

They can even copy a genuine company's website and have a similar web address to make the scam seem authentic.

The most targeted profiles are:
- Newcomers to a country
- The unemployed, students and people in economic distress
- Men (more likely than women) particularly those aged 18-34
HOW TO PROTECT ONESELF?

If an opportunity sounds too good to be true, it probably is.
Be very cautious of unsolicited emails or approaches over social media promising opportunities to make easy money.
Verify any company that makes you a job offer and check their contact details (address, landline phone number, email address and website) are correct and whether they are registered in your country.
Be especially wary of job offers from people or companies overseas as it will be harder for you to find out if they really are legitimate.
Never give your bank account or any other personal details to anyone unless you know and trust them.
Look for the common warning signs as above explained, and do some research before agreeing to participate.

WHAT TO DO?
If you have received e-mails of this type do not respond to them and do not click on any links they contain. Inform the police instead.
If after reading this flyer you believe that you are participating in a money mule scheme, stop transferring money immediately and notify your bank, the service you used to conduct the transaction, and law enforcement.

HOW ARE MONEY MULES RECRUITED?

As new technologies and trends emerge, organised crime groups develop new systems to defraud people:

- seemingly legitimate job adverts (e.g.: ‘money transfer agents’)
- seemingly legitimate online posts
- direct approach in person or through email
- social media (i.e. Facebook posts on closed groups)
- messages sent through instant messaging apps (e.g.: Whatsapp, Viber)

WHO ARE THE MOST TARGETED INDIVIDUALS?

- Newcomers to the country (often targeted soon after arrival) as well as the unemployed, students and people in economic distress are the most susceptible to the crime.
- Men are more likely than women to be targeted to become a mule, as are those aged 18-34 years compared to people aged 55+.

WHAT ARE THE WARNING SIGNS?

The following characteristics do not necessarily indicate a money mule solicitation, but they are commonly used in those solicitations:

- Money mule adverts or offers may copy a genuine company’s website and have a similar web address to make the scam seem authentic.
- If done by email, the writing is often awkward and includes poor sentence structure with grammatical and spelling mistakes. The email address associated with the offer uses a web-based service (Gmail, Yahoo!, Windows Live Hotmail, etc.) instead of an organisation-based domain.
- These adverts will normally state that they are an overseas company seeking ‘local/national representatives’ or ‘agents’ to act on their behalf for a period of time, sometimes to avoid high transaction charges or local taxes.
- The position involves transferring money or goods.
- The specific job duties are not described.
- The position does not list education or experience requirements.
- All interactions and transactions will be done online. The offer promises significant earning potential for little effort.
- The nature of the work that the company will claim to be involved in can vary, but the specifics of the job being advertised invariably mean using your bank account to move money.

WHAT TO DO?

If you have received e-mails of this type do not respond to them and do not click on any links they contain. Inform the police instead.
If after reading this flyer you believe that you are participating in a money mule scheme, stop transferring money immediately and notify your bank, the service you used to conduct the transaction, and law enforcement.
Download the Money Mule poster and flyer in your language (PDF)

Poster


Flyer
