US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Understanding and Protecting Yourself Against Money Mule Schemes

Matthew DeSantis, Chad Dougherty, Mindi McDowell

Money Mules Are Used to Commit Fraud

"Money mules" are people who are used to transport and launder stolen money or some kind of merchandise. Criminals may even recruit money mules to use stolen credit card information. Individuals being used as money mules may be willing participants; however, many money mules are not aware that they are being used to commit fraud. The individuals being used as money mules are not the only victims; the larger scheme is designed to extract money from an organization or from other people.

Schemes May Seem Like Legitimate Opportunities

The most common money mule solicitations are disguised as "work from home" opportunities. These advertisements often target unsuspecting people who are interested in the convenience and flexibility of these types of jobs. Because there are companies that legitimately offer opportunities to work from home, users may not recognize malicious offers. Criminals often try to make the offer seem as legitimate as possible and may use the following approaches:

- carefully crafting the wording so that an email does not appear to be spam and is not caught by spam filters
- linking to fake but professionally designed websites that appear to belong to recognized companies or that promote a company that does not even exist
- posting some of these jobs on legitimate websites, including websites specifically for job seekers

Typical Process

After an individual agrees to be a money mule, the schemes tend to follow a similar process[1]:

1. The "company" collects information from the "employee." The information may include personal data such as the individual's Social Security number and bank account

[1] Bank Safe Online offers an illustration of this process (http://www.banksafeonline.org.uk/moneymule_explained.html).

information. The company may also ask the employee to sign a seemingly official contract.

2. The company (or the employee, under the direction of the company) creates a financial account[2] that the employee can use to collect and transfer funds.
3. The employee receives funds or some type of merchandise.
4. The employee is instructed to transfer the funds (usually keeping some percentage) to some other financial account or to deliver the merchandise to some third party. This financial account or third party is associated with the criminal. Often, the company will instruct the employee to use wire transfers for the funds, and there may be another money mule on the other end of the transfer with instructions to cash those funds.

Through this process, the criminal receives the stolen money or merchandise while hiding his or her involvement.

Typically, a criminal will only use a money mule once. After the money mule performs his or her role in the transaction, the criminal usually dissolves the relationship completely and recruits someone else for the next scheme.

Consequences Can Be Severe

If caught and prosecuted, the criminal faces the most severe consequences. However, the other parties involved in the scheme may also face serious consequences.

Money Mule

The following are potential consequences for money mules:

- **Inaccessible bank accounts** – During an investigation, law enforcement officials may freeze a money mule's bank accounts. Being unable to access funds may create a significant financial burden. These activities may also have a long-term impact on credit scores.
- **Prosecution** – Money mules may be prosecuted for their participation in these schemes.
- **Accountability for charges** – In some cases, money mules are found personally responsible for repaying the losses suffered by the other victims.[3]
- **Vulnerability of personal information** – As described in the typical process, criminals often collect personal information from the money mules. It is possible that the criminals may use this information for other malicious purposes.

[2] These accounts are typically established at a bank or through a service such as PayPal.

[3] "'Money Mules' Help Haul Cyber Criminals' Loot" (http://www.washingtonpost.com/wp-dyn/content/story/2008/01/25/ST2008012501460.html)

Targeted Individuals

If the fraud is designed to extract money from individuals, those individuals could experience the following consequences:

- **Financial loss** – An individual may pay for undelivered goods or have money deducted directly from one of his or her financial or credit card accounts. Depending on the forum used for the transaction and whether the scheme is identified, the individual may be able to recover at least a portion of these losses.
- **Significant hassle to resolve issues** – Identifying and reporting the fraud may require numerous steps, and the process could take a long time.

Targeted Organizations

If the fraud is designed to extract money from an organization, it may affect both the organization and its customers or constituents.

- **Financial loss** – A criminal may be able to siphon significant amounts of money from an organization's financial accounts before the activity raises suspicions.
- **Compromise of sensitive data** – If a criminal can access customer data, such as credit card information, he or she may be able to steal that information and use money mules to abuse the customers' financial or credit card accounts.
- **Damage to reputation** – If an organization experiences fraud, they may lose the trust and loyalty of their customers or partners.
- **Significant hassle to resolve issues** – Identifying and reporting the fraud may require numerous steps, and the process could take a long time.
- **Potential for future compromises** – If a criminal uses malicious code to access information on an organization's computer, he or she may hide additional malicious code that would allow the criminal to regain access in the future. If an organization does not locate and remove this code, it may be susceptible to another compromise.

Take Steps to Protect Yourself

Avoid Becoming a Money Mule

If an opportunity sounds too good to be true, it probably is. Look for common warning signs, and do some research before agreeing to participate. If you believe that you are participating in a money mule scheme, stop transferring money and merchandise immediately and notify the appropriate authorities. These authorities may include your bank, the service you used to conduct the transaction, and law enforcement.

Warning Signs

The following characteristics do not necessarily indicate a money mule solicitation, but they are commonly used in those solicitations[4].

- The position involves transferring money or goods.
- The specific job duties are not described.
- The company is located in another country.
- 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 writing is awkward and includes poor sentence structure.
- The email address associated with the offer uses a web-based service (Gmail, Yahoo!, Windows Live Hotmail, etc.) instead of an organization-based domain.

Research Strategies

- Perform online searches using information from the offer:
    - the subject line of the email
    - the company supposedly offering the position
    - the person who signed the message or the name of the contact person mentioned in the offer

  Look for indications that the offer might be a scam. If an online search does not produce any results, that may also be suspicious.
- Check the Better Business Bureau website[5].

Avoid Becoming a Victim

Individuals and organizations can both take precautions that minimize their risks.

Individuals

- Try to investigate the person or company before doing business with them.
- When transferring money, use a method that protects the transaction. For example, many banks, credit cards, and services such as PayPal may offer fraud protection.
- Monitor the transactions, including checking for withdrawals from your bank account and tracking an order.
- If you notice any problems, immediately contact the appropriate authorities. Depending on the circumstances, these authorities may include your bank, the service you used to conduct the transaction, and law enforcement.

---

[4] See the F-Secure Weblog for an example (http://www.f-secure.com/weblog/archives/archive-012007.html#00001084).

[5] http://www.bbb.org/

Organizations

Criminals typically use stealthy methods to access an organization's data or finances. These methods may include using malicious code, such as a virus, to gain administrative access to a computer within an organization or relying upon a malicious insider to transmit data or create fake customer accounts. By implementing the following precautions and practices, organizations may reduce their risk:

- Use anti-virus and anti-spyware software, and keep the definitions up to date.[6]
- Limit access to sensitive data to authorized personnel.
- Regularly check records, including employee lists and recent financial transactions. Look for new employees that Human Resources staff does not recognize, or for unauthorized transactions.
- Consider isolating the computers that perform banking and accounting functions. In small organizations, it may be feasible to use a separate laptop for these tasks. Larger organizations may be able to designate computers used to perform these tasks and apply stricter policies and access controls on those computers.
- Watch for suspicious behavior or activities from employees.[7]
- If you notice any problems, immediately contact the appropriate authorities. Depending on the circumstances, these authorities may include your IT department, your accounting department, and law enforcement.

Additional Resources

US-CERT Resources

- "Avoiding Social Engineering and Phishing Attacks" (http://www.us-cert.gov/cas/tips/ST04-014.html)

Other Resources

- Internet Crime Schemes: Employment/Business Opportunities (http://www.ic3.gov/crimeschemes.aspx#item-7)
- Money mule blog articles by Brian Krebs (http://krebsonsecurity.com/tag/money-mules)
- "Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams" (http://www.fsisac.com/files/public/db/p264.pdf)
- "Fraud Advisory for Businesses: Corporate Account Take Over" (http://www.fsisac.com/files/public/db/p265.pdf)

---

[6] See "Understanding Anti-Virus Software" (http://www.us-cert.gov/cas/tips/ST04-005.html) and "Recognizing and Avoiding Spyware" (http://www.us-cert.gov/cas/tips/ST04-016.html).

[7] The CERT® Insider Threat Center (http://www.cert.org/insider_threat/) offers insider threat resources for organizations.