# CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

## Protect Your Business from Money Mules

**Key Message:** Organized criminals recruit unsuspecting intermediaries to help steal funds from small businesses.

**Executive Summary**

"A growing threat of fraudulent wire transfers from local businesses to overseas locations has raised numerous online banking concerns. Successful cyber attacks resulting in fraudulent wire transfers with average losses of $100,000 to $200,000 US dollars per victim, frequently trace back to malware infections on the local business entity's computer. These incidents primarily target small to medium sized businesses and may involve amounts as small as $10,000 US dollars or as much as several million dollars. [1]"

In this podcast, Chad Dougherty, a member of CERT's Cyber Threat and Vulnerability Analysis Team, discusses the rise in small businesses that have had their bank accounts cleaned out by organized criminals. Criminals recruit and use unsuspecting "money mules" to receive and transmit stolen funds and move them from their country of origin to another that the criminal can access, often undetected.

---

### PART 1: HOW ORGANIZED CRIME USES MONEY MULES AND MALICIOUS CODE

#### Why Small Businesses Are a Prime Target

The use of money mules is a new take on traditional, online financial fraud.

Small businesses typically

- have more cash in their accounts than individuals
- do not have a formal security policy
- have insufficient defenses or defenses that are more easily circumvented than larger businesses
- do not have the same protections against liability and fraudulent transactions that individuals do (Unlike individual credit card fraud, business owners are responsible for stolen funds.)

#### How Criminals Recruit Money Mules

Targeted individuals (money mules)

- receive a "work at home" spam email, promising a steady income stream
- provide their personal bank account credentials
- wait for a message to transfer funds that have been deposited in their account
- transfer the funds from their account, using a payment transfer service such as Western Union, to a designated account provided by their criminal contact
- keep a percentage for their efforts

Once a money mule participates in a single transfer, they rarely hear from the criminal again.

#### Why Criminals Use this Scheme

Money mules help protect the criminal's identity. In addition, criminals use a large number of money mules to move funds from a single account so that each transfer remains undetected due to being relatively small (for example, $9,000).

### How Victim Computers Are Compromised

Computers used by small businesses are compromised using many of the means that home users are subject to, including

- drive-by downloads: As the victim browses a selected website, code on the site exploits a vulnerability in the victim's browser (or other installed software). The code allows more sophisticated, malicious software to be installed on the victim's computer.
- attacks on general purpose PCs: When a general purpose PC used for online banking transactions is compromised, this PC provides a gateway to the business's bank accounts.
- "man-in-the-browser" attacks: This attack often uses sophisticated malicious code that gives the account holder the impression that all is well with their balances and transactions while money is being stolen behind the scenes.

---

## PART 2: ACTIONS BUSINESSES CAN TAKE TO PROTECT THEIR ACCOUNTS

### How Do You Know If This Is Happening to You?

Most of the time victims find out that their funds have been stolen when they are unexpectedly overdrawn on a transaction or funds are missing from their account.

Sometimes, if the bank is on its toes, they will call the business owner to question a transaction before it is completed. Unfortunately, once a transfer is completed it cannot be reversed.

### What Small Business Owners Can, and Should, Do

Owners can take the following actions to protect themselves:

- Make sure they understand, up front, what protections their bank offers as well as the business owner's liability for fraudulent transactions.
- Use a system specifically designated for online banking and only for this purpose. Maintain tight security on this machine, install all patches, and keep anti-virus software up to date. Do not install any general purpose applications such as email, which can be easily compromised.
- Set up transfer thresholds with the bank, such that transfers in excess of the threshold require an "out-of-band" authorization (phone call, fax, text message). Such authorizations do not involve the same system that is being used to make the transfer.
- Ask their bank for services that profile normal small business behavior (for example, payroll at month end) and compare this to ongoing transactions to detect abnormal or unexpected behavior.

Some banks will register a particular IP address as the legitimate source for online banking transactions. But if the business owner's computer has been compromised and is being used by a criminal, this doesn't help.

### Resources

Krebs on Security blog posts, particularly those under "Target: Small Businesses"

[1] "Information and Recommendations Regarding Unauthorized Wire Transfers Relating to Compromised Cyber Networks." Joint Secret Service/Multistate ISAC advisory, 12 March 2010.