FORGE

The Arkansas Cyber Defense Center

Money Transfer Fraud

This type of attack involves using false or misleading information to convince a business owner or employee to send money to an unintended, malicious third party.

Who could be targeted?
Businesses of any size and employees at any level can be targeted for transfer fraud because attackers can use a targeted amount of money proportional to the size of the business or position of employee being attacked.

Why be aware of this attack?
Money transfer fraud can happen at any level within an organization. Attackers may pose as an individual or another business in order to gain someone from your business' trust. Once an attacker has that rust, they will often ask for access to your business' financial information in order to make a transfer. This can cause financial loss, reputational damage, legal liabilities, and operational disruption.

What do threat actors want?
The main purpose behind money transfer fraud is to defraud a business for monetary gain.

Common tactics:

- Crooks will set up fake emails and websites in order to look like a vendor or supplier to convince businesses to send them money.
- Attackers may send invoices for early payment, or they may call demanding early payment. They may use intimidating language in order to scare somebody into sending a payment so they do not get into trouble.
- There are often promises of high returns on investments. For example, the attacker may offer to help with a loan for your business's expansion project, but then leave you high and dry once you have pooled your money with theirs.

POWERED BY SBA
U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc
501-239-9599