

# Business Imposter

KNOW YOUR RELATIONSHIPS  TAKE STEPS TO VERIFY

Cyber criminals compromise business systems while purporting to be a business representative.



## HOW

- Funds are requested appearing to be standard operating procedure.
- Email may be hacked or a sender email may impersonate the email of the business.
- Emails sent to unassuming recipients appear to be from the business.
- Email recipients are under pressure to act fast due to an underlying emergent issue.
- Common forms of payment include wire transfers, cryptocurrency, and gift cards.

## STEPS TO VERIFY

1. Complete a cybersecurity assessment and resolve vulnerabilities.
2. Train staff regularly in cybersecurity and funds management protocols.
3. Enlist internal protocols to verify the transfer of funds by engaging multiple staff members and voice verification, using trusted contact information.
4. Help clientele to identify common scams within the industry.
5. Use the SLOW method to Slow down and verify the contact.
6. Never send money to parties that you cannot verify.



**CONSUMER ASSISTANCE PROGRAM**

ATTORNEY GENERAL'S OFFICE & UNIVERSITY OF VERMONT  
GET HELP WITH CONSUMER PROBLEMS AND REPORT SCAMS

1-800-649-2424  
[ago.vermont.gov/cap](https://ago.vermont.gov/cap)



Go online or scan QR code to watch the [Avoiding the Business Imposter Scam](#) video.