Before you act

Money, account access or an unexpected request

STOP. Pause the payment, new bank details, login, code sharing or access request. Urgency is a reason to check.

VERIFY. Use a number or channel you already trust, independently of the message. Confirm the specific request. Caller ID, a familiar voice and a genuine-looking email thread are not enough.

CONFIRM. Get the required approval from a second authorized person. If the right person is unavailable, hold and use the agreed escalation route. Two people reading the same email is not independent verification.

REPORT. Use your organization's reporting channel. Preserve the message safely as IT instructs. Report even if you clicked, shared information or paid. Do not include passwords or one-time codes in a report.

Trusted reporting contact: ____________________________

Authorized approver / backup: ________________________

Where to find verified vendor contacts: ________________

Bank fraud contact location: __________________________

Money already sent? Contact the bank/payment provider immediately and ask about stopping or recalling the payment. Recovery is not guaranteed. Notify management/IT and report to IC3.gov and ReportFraud.ftc.gov as appropriate. A technical or immediate safety emergency needs the relevant professional/emergency service, not a training inquiry.

Suncoast Tech Expertise | Dominic Spinnato | (941) 529-7863

Awareness education. Follow your organization's approved procedures.