NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Business Email Compromise and Wire-Fraud Invoice Scams

Business email compromise is a scam that targets anyone who performs a legitimate transfer of funds, and real estate, title, and accounting offices are favorite targets because big transactions and bank-detail changes already travel by email. This guide covers how to verify a changed bank account before you pay it, and what to do if you already sent the money.

Why these offices get targeted

Three things make real estate, title, and accounting a favorite target.

Big transactions, tight deadlines
Closings and invoices move fast, so a last-minute change doesn't always get a second look.

Email already carries the money talk
Wiring instructions, invoices, and account numbers already travel by email, so a fake one blends right in.

Everyone trusts someone in the chain
Buyer, seller, agent, title company, accountant; compromising just one inbox can fool the rest.

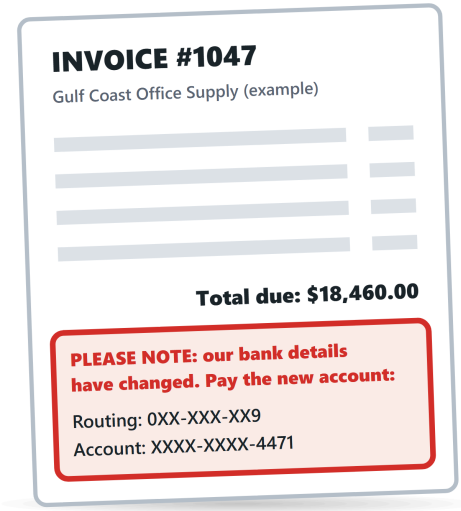
Step by step

WIRE-FRAUD SCAMS

! Would you catch the change?

An invoice looks perfect, right up until the bank account on it quietly changes.

WHAT TO DO
We're Naples Computers, and we help offices catch this, since 1993.



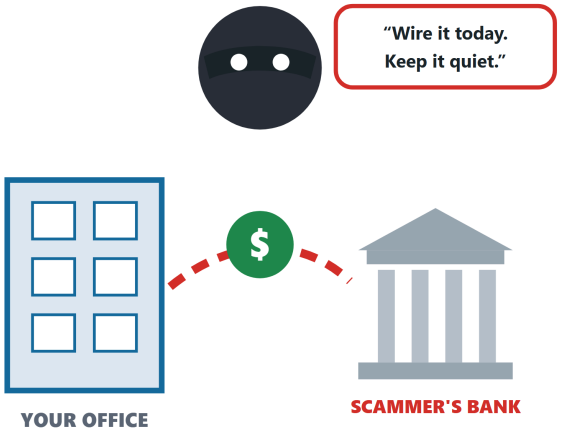
STEP 1

! Verify by phone, not email

Any time a bank account or payment method changes, call a known number to confirm it, never a number from the email.

WHAT TO DO

Use a number you already have on file; don't use one inside the message asking for the change.



Call a known number to confirm

STEP 2

! Look past the display name

Check the actual email address, not just the name shown, for a misspelled domain or an extra letter.

WHAT TO DO

Scammers lean on urgency; wire it today, keep it quiet, so slow down anyway.



A lookalike domain, hiding in plain sight

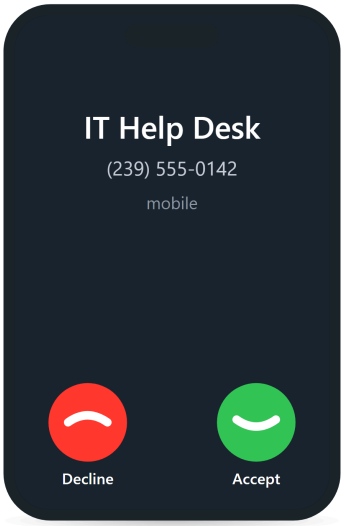
STEP 3

! Call your bank immediately

Ask for a wire recall, and give them any documents they need. Minutes matter.

WHAT TO DO

Then report it at ic3.gov, the FBI's Internet Crime Complaint Center, so it can help both your bank and law enforcement.



Every minute matters

A few tips

- [ ] Slow down on urgency
  "Wire it today" or "keep it quiet" are red flags, not reasons to hurry
- [ ] Use a second channel for big changes
  A phone call or text to a known number, never the same email thread
- [ ] Train everyone who touches money
  Not just accounting; agents, assistants, and anyone who approves a payment

Recap: wire-fraud scams

- [ ] Any bank-account or payment change gets a phone call to a known number
- [ ] Check the real email address, not just the display name
- [ ] If you already sent money, call your bank immediately for a recall
- [ ] Report it at ic3.gov so law enforcement can help

Any time a bank account or payment method changes, verify it with a phone call to a number you already have on file, never a number from the email asking for the change.

Worried your office could be a target?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**