Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, your company has a lot to lose. Customers and partners might lose trust and take their business elsewhere — and your business could then lose money.

T YOUR BUSINESS

ke sure
o□ers email
chnology. That
send an email
mpany's server, the
ervers can confirm
mail is really from you.
, the receiving servers
ock the email and foil a
ess email imposter.

Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.

WHAT TO DO

IF SOMEONE SPOOFS YOUR COMPANY'S EMAIL

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also forward phishing emails to spam@u