With the right planning, you can shut the door on scammers.

Spectrum®

Phishing scams are often the cause of a wire transfer fraud.

Help protect your business:

- Talk to your employees about wire fraud.
- Train your employees to identify phishing emails.
- Instruct your employees on wire transfer best practices.

Use Wire Transfer Best Practices

- Before funds are wired, put a written agreement in place with each customer or vendor. The agreement should spell out how fund transfers will work.
- Do not use email to send wiring instructions to a customer or vendor. Use regular mail, telephone or fax.
- Do not process wire transfer requests from a public email address (e.g., anybody@gmail.com); only accept requests from a company email address (e.g., anybody@abcmanufacturing.com).
- Use a call-back process to confirm payment instructions for a new vendor or to make updates to an existing one.
- Look at wire transfer requests for real estate transactions closely. Scammers are good at hacking email accounts and could pretend to be a real estate or title agent.
- Assign one person to receive requests for funds and a different person in your organization to approve them. This is called dual authorization and is a good check and balance.

Use Email Best Practices

- Require two levels of checks for employee email. This is known as dual or two factor authentication.
- Encrypt email communications that contain sensitive business information.

What More You Can Do

- Run random awareness and fraudulent knowledge tests within your staff population to test your company's fraud health.
- Check to see if your business insurance policy covers wire fraud.

Contact your agent with any questions.

The Hartford