Preventing Payment Fraud

Technology has enabled businesses to execute transactions in minutes. The downside is that it's made it easy for thieves to conduct their business quickly, as well. Hundreds of thousands of dollars can disappear from your account in less than an hour after receiving an email request for a wire transfer. Fraudsters know this. Here are a few key pieces of advice to help keep yourself from becoming a victim of wire fraud:

Enforce Dual Controls	Implement -- and enforce -- dual controls, which requires two individuals to approve a wire transfer.
Pick Up The Phone	Call the number you have for the individual authorized to request a wire transfer -- don't rely on the number provided in an email message.
Follow Email Protocol	When replying to emails, delete the information in the "To" field and manually enter the contact information you have on record. That can help stave off phishing scams.
Consider ACH Transfers	When possible, use same-day ACH transfers, which makes it easier to recall payments.
Enforce Authorization Procedures	Don't be afraid to call the head of the company to verify wire requests. Conversely, owners and CEOs should understand why the finance department needs to call them, and they should comply with proper authorization processes, as well.
Limit Exploitable Information	Don't set up "Out of Office" automated email replies. Fraudsters who get access to your account will be able to know when you're away and use that to their advantage.
Customize Payment Requests	For regular vendors, create wire transfer templates that can only be accessed by a single authorized requestor and approver. Also, any changes to banking information will require two people to authorize the change.
Recognize Vendor Behavior	Know your customers. Recognize any changes in behavior in your communications, such as a request that includes a different payment location.
Be Vigilant	Apply extra scrutiny to international wire requests.