



DON'T GET CAUGHT

PHISHING & BUSINESS EMAIL COMPROMISE

Don't believe everything you read. Take phishing awareness training seriously.

Signs of a Suspicious Email

- It requests you to take action
- It implies a sense of urgency
- Indicates adverse consequences if ignored
- Sounds too good to be true
- Requests sensitive information
- Asks you to buy gift cards
- Involves wire transfer instructions

That "unexpected package delivery" may be a virus, not a parcel going to your house...

Important Notes

- Hover over links and email addresses to expose their true identity.
- Look for evil doppelgangers like @Arnazon.com (ARNazon instead of Amazon).
- Use the known vendor website to investigate alerts instead of clicking the link.
- Your bank, the IRS, and Amazon will never request confidential information by email.
- Always confirm wire transfer instructions using non-email methods, such as verbally.

**Remember that clever adversaries can circumvent SPAM filters.
Your actions will determine if a phish succeeds.**