IT Spot

Cyber Risks in Logistics

A practical handout for recognizing impersonation, account compromise, and shipment-related fraud

Modern attackers do not always break in by force. They often look legitimate, create urgency, and rely on people acting before they verify. A few simple habits can help your team interrupt that process before it leads to loss.

1 What attackers are doing

- Impersonating trusted contacts, carriers, or vendors
- Using stolen or compromised credentials
- Requesting last-minute operational changes
- Watching operations to identify valuable shipments or weak points

2 Common warning signs

- Urgent requests to change pickup, delivery, payment, or contact details
- Email addresses or domains that look similar but are not exact
- Pressure to skip normal approval or callback steps
- Unexpected remote access or suspicious activity on a workstation
- Logins from unusual devices, locations, or times

3 What they want

- Credentials and account access
- Shipment details and business information
- Route or telematics visibility
- Payment redirection or fraud opportunities
- A way to blend in long enough to be trusted

4 What your company can do

- Call back using a known number before making high-risk changes
- Require two-person approval for sensitive requests
- Use multi-factor authentication and review access regularly
- Limit access to systems and sensitive shipment information
- Train employees to pause, verify, and document

5 Quick response checklist

- Stop and verify before taking further action
- Capture screenshots, names, and timestamps
- Notify IT or your security contact immediately
- Reset affected passwords and review access
- Review endpoint, identity, and email activity

Verification is not a delay. Verification is protection.

Use this handout as a quick reference for staff, dispatchers, operations teams, and managers.