I principi dello standard C-TPAT

IPQ Tecnologie srl

Partner per lo sviluppo d'impresa

Raffaela Vitiello

INTRODUZIONE

- C-TPAT è l'acronimo di *Customs-Trade Partnership Against Terrorism*
- C-TPAT è un programma volontario proposto dal Governo degli U.S.A.
- C-TPAT richiede ai lavoratori:
  - Adesione ai principi (indossare il badge, mettere in sicurezza la propria postazione, ricordare ai colleghi di rispettare le regole);
  - Consapevolezza (prestare attenzione ad attività sospette);
  - Collaborazione (gli eventi sospetti devono essere comunicati).

PERCHE’ CERTIFICARSI?

Essere un partner di fiducia per l’US Customs garantisce benefici operativi e finanziari, quali:

→ Corsia facilitata per i processi di importazione ed esportazione

→ Meno interruzioni della catena di fornitura dovute alle ispezioni in dogana

→ Riduzione di penali in caso di violazioni in dogana

→ Protezione del marchio e vantaggi rispetto alla concorrenza.

PRINCIPALI AREE COINVOLTE

TEMI DI INTERESSE

- Persone sospette
- Attività sospette
- Oggetti o pacchi sospetti
- Identificazione dei dipendenti
- Controllo dei visitatori
- Sicurezza informatica
- Sicurezza documentale

PERSONE SOSPETTE

Prestare attenzione a qualsiasi persona che…

- non è accompagnata ed è senza il badge aziendale o il badge visitatori, specialmente se in un'area ad accesso limitato
- indossa abiti non abituali per la realtà aziendale
- si sta intrattenendo in un'area o alla reception
- sta utilizzando la scrivania, il computer, l'auto di qualcun'altro
- sta correndo, in particolare trasportando qualcosa
- si sta nascondendo dietro porte, scrivanie, ecc.

PERSONE SOSPETTE

Come comportarsi?

- Chiedere alla persona se ha bisogno di aiuto
- Capire se la persona è un dipendente o un visitatore:
  - se è un **dipendente**, chiedere di poter visionare il badge,
  - se è un **visitatore** al di fuori delle aree consentite, accompagnarlo alla reception o dalla persona di riferimento
- Comunicare immediatamente l'accaduto al proprio responsabile

ATTIVITA' SOSPETTE

Prestare attenzione a…

- Oggetti che ostruiscono punti di accesso
- Videocamere scollegate o coperte (se presenti)
- Sistemi di chiusura manomessi
- Oggetti che vengono lanciati da veicoli, in particolare se stanno viaggiando ad elevata velocità.

ATTIVITA' SOSPETTE

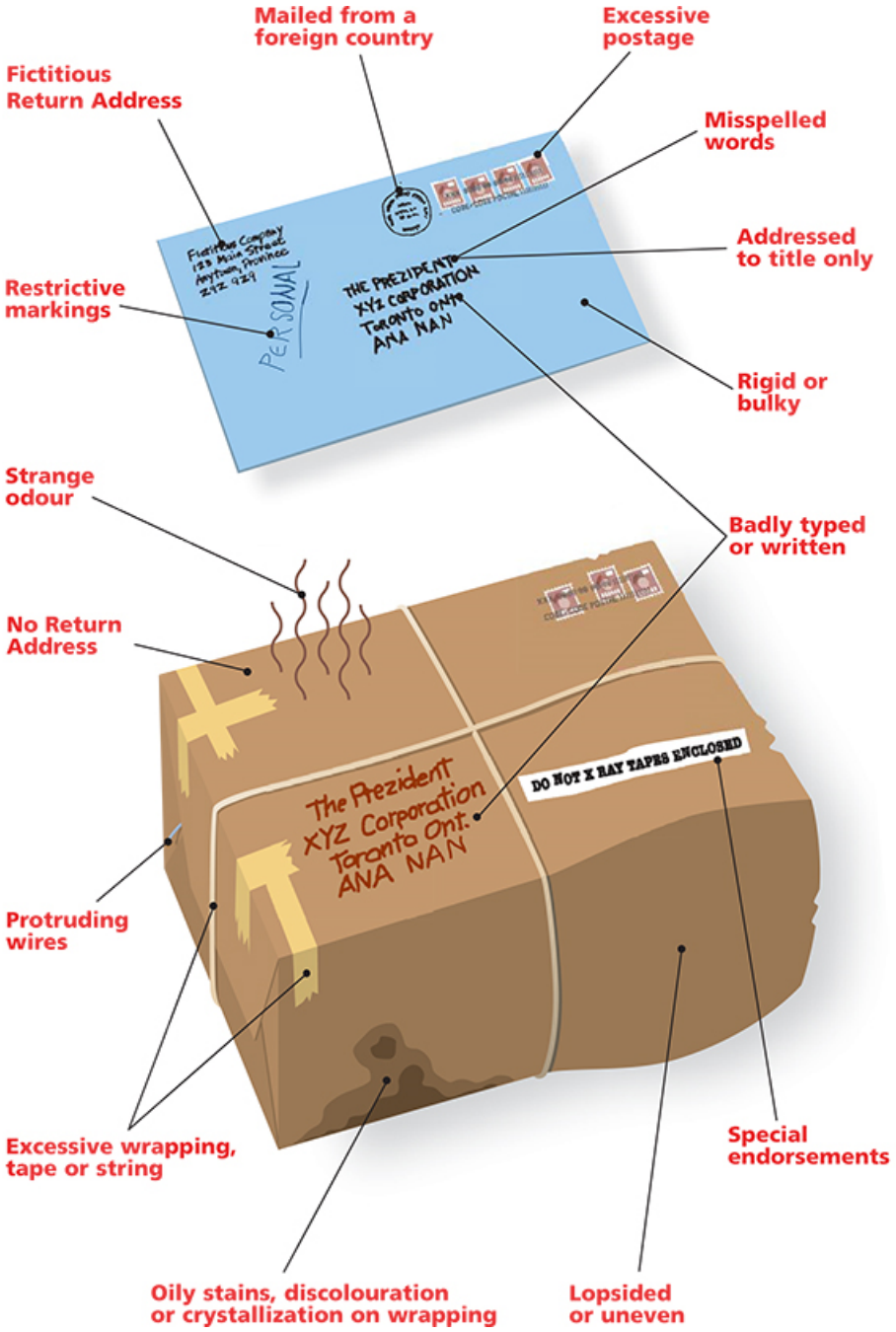
Come comportarsi?

Comunicare immediatamente l'accaduto al proprio responsabile, in modo che possa decidere se far intervenire le autorità competenti.

OGGETTI O PACCHI SOSPETTI

Prestare attenzione a…

- Oggetti non identificati o scatole che appaiono anomale o che non appartengono all'area in cui sono collocate
- Segni strani sulle scatole (codici sconosciuti, colori anomali) o caratteristiche anomale (peso, numero, forma)
- Sostanze strane che fuoriescono dalla confezione (polvere, liquidi, ecc.)
- Oggetti strani nella zona centrale di un'area (es. reception, atrio, ecc.)


Mailed from a foreign country
Excessive postage
Fictitious Return Address
Misspelled words
Addressed to title only
Restrictive markings
Rigid or bulky
Strange odour
Badly typed or written
No Return Address
DO NOT X RAY TAPES ENCLOSED
Protruding wires
Special endorsements
Excessive wrapping, tape or string
Oily stains, discolouration or crystallization on wrapping
Lopsided or uneven

OGGETTI O PACCHI SOSPETTI

Come comportarsi?

- Avvisare tempestivamente il proprio responsabile / la sicurezza / la polizia postale.
- Maneggiare con cura eventuali scatole sospette, senza scuoterle
- Isolare la scatola sospetta ed ispezionarla
- Non aprire il pacco sospetto

IDENTIFICAZIONE DEI DIPENDENTI

Le responsabilità del dipendente:

- Assicurarsi che il badge sia sempre ben visibile
- Conservare accuratamente il badge, senza lasciarlo incustodito

CONTROLLO DEI VISITATORI

- Prima dell'ingresso in azienda: informare il visitatore delle politiche interne e comunicare alla reception l'arrivo previsto dell'ospite.
- All'ingresso: registrare la presenza del visitatore e consegnargli il tesserino di riconoscimento.
- Durante la visita: l'ospite dovrà sempre essere accompagnato da un riferimento interno e non dovrà mai essere lasciato solo.
- All'uscita: assicurarsi che il visitatore abbia registrato la propria uscita e che abbia restituito il tesserino.

SICUREZZA INFORMATICA

- Non condividere le credenziali di accesso al tuo computer con estranei.
- Effettua il log-off dal tuo profilo ogni volta che ti allontani dal tuo computer.
- La password dovrebbe essere cambiata ogni 60-90 giorni.
- Non condividere la tua password con nessuno.
- Non scrivere la tua password su nessun documento.

SICUREZZA INFORMATICA

Per selezionare la password:

- Utilizza pw difficili da indovinare
- Non utilizzare la stessa pw in più di un profilo
- La pw dovrebbe essere un mix di lettere, numeri e simboli

SICUREZZA DEI DOCUMENTI

- Seguire tutte le procedure interne per la gestione dei documenti
- Non lasciare documenti riservati incustoditi, soprattutto quando ci si allontana dalla propria postazione di lavoro
- Al termine del lavoro, assicurarsi di salvare i documenti in una cartella protetta o collocare le copie cartacee in un archivio dedicato.