5-MINUTE STAFF TRAINING · THE TECH BRIEF · HOLIDAY 2026

Holiday scams: what to watch for at work.

Read this together at your next team meeting. It takes 5 minutes, and it covers the scams most likely to reach your office between Black Friday and New Year's.

1. The six scams

Too-good deals	Ads lead to copycat stores.	**Type the store's address yourself.**
"Package on hold" texts	Fake delivery fees steal cards.	**Track only in the carrier's app.**
"Problem with your order"	Fake login pages steal passwords.	**Check orders in the real app.**
"Call to cancel" invoices	Fake agents ask to remote in.	**Never call numbers in the email.**
Gift cards "from the boss"	Urgent texts from a new number.	**Call to confirm on a known number.**
Fake charities & e-cards	Links to fake pages or malware.	**Give on the charity's own website.**

2. Our office rules

- No purchases or payments based on a text or email alone. Always confirm by phone.
- Changed bank details from a supplier? Call them on a number we already have before paying.
- Never let a caller "remote in" to a work computer unless it's our IT team.
- It's always OK to double-check the boss.

3. If someone clicks

Disconnect from the internet, stop typing, and call IT right away. No blame: the faster we know, the less damage.

Discussion (2 minutes): Has anyone received a suspicious text or email this month? What made it look real?

Team member name _____ Date reviewed _____