TRXCK

TRXCKWRLD.COM

Don't Get Scammed

A driver's security checklist: the messages, passwords, and habits that keep your accounts and your money yours.

SPOT IT: EMAIL

- [ ] Sender address almost right: one letter off is the tell
- [ ] Urgency and fear: real companies do not rush you like that
- [ ] A link or attachment you did not ask for: do not touch it
- [ ] Asked for passwords, bank details, or your SSN: never by email

YOUR ELD AND YOUR APPS

- [ ] Change the ELD's default password the day it is installed
- [ ] Keep the ELD and its app updated; old firmware is an open door
- [ ] Bluetooth and Wi-Fi off when you do not need them
- [ ] Load board apps only from the official store, never from a link

SPOT IT: TEXTS AND QR CODES

- [ ] Texts about payments, cancellations, or accounts you did not start: assume fake
- [ ] An app download offered by text: the app stores are the only door
- [ ] QR codes on tickets, invoices, or stickers: check the address before you tap
- [ ] A tech support number that texted you: look the real number up yourself

IF IT HAPPENS

- [ ] Change passwords from a clean device, email and money accounts first
- [ ] Call your bank and your factoring company immediately
- [ ] Report it to the FBI's Internet Crime Complaint Center at ic3.gov
- [ ] Warn your dispatch and your broker: the next target is your contacts

LOCK IT DOWN

- [ ] A different strong password for every account that touches money
- [ ] Two-factor on email, banking, factoring, and load boards: non-negotiable
- [ ] Updates installed, not postponed: they carry the security fixes
- [ ] Public Wi-Fi is public: no banking or load boards on truck stop Wi-Fi without a VPN

Most scams start with one message that felt a little off. Trust that feeling; checking costs a minute, a hijacked account costs a season.