Tutela Digitalis
SEE THE SCAM BEFORE IT SEES YOU

THE ESSENTIAL FIELD GUIDE

The Scam-Defense Checklist

Almost every scam — no matter how sophisticated — relies on the same handful of moves. Learn to spot them, and they stop working on you. Keep this guide somewhere you'll see it.

01 The 7 Warning Signs

If you see two or more — stop.

- [ ] **Urgency & pressure.** "Act now," "your account will be closed," "only 10 minutes left." Real institutions don't rush you.
- [ ] **An unexpected contact.** A call, text, or email you didn't initiate — about money, a delivery, a prize, or a problem you didn't know you had.
- [ ] **A request for secrecy.** "Don't tell anyone," "this is confidential." Isolation is a scammer's favorite tool.
- [ ] **An unusual payment method.** Gift cards, crypto, wire transfers, or "keep the change" overpayments. These are chosen because they can't be reversed.
- [ ] **A request for codes or passwords.** No legitimate company will ever ask for your one-time code, PIN, or full password.
- [ ] **A mismatch you can verify.** The sender's email domain, a link's real destination, or a phone number that doesn't match the official one.
- [ ] **It feels too good — or too frightening.** Both extremes are designed to override your judgment. Strong emotion is the goal, not a side effect.

02 Three Questions Before You Click

1. **Did I expect this?** If a message arrives out of nowhere, treat it as suspicious until proven otherwise.
2. **What are they actually asking me to do?** Click, pay, share a code, install something? Name the action — it's usually the giveaway.
3. **Can I verify this independently?** Don't use the link or number they gave you. Look it up yourself and contact the source directly.

03 The First 60 Seconds

If you think you've been hit.

1. **Stop all contact immediately.** Hang up, close the chat, don't reply. The pressure is the trap.
2. **Don't send another cent.** If you've already paid, that's recoverable far more often than a second payment.
3. **Call your bank's official number.** The one on your card — not one anyone gave you. Ask them to freeze and flag the transaction.
4. **Change passwords from a different device.** Start with email and banking. Turn on two-factor authentication.
5. **Write down what happened.** Names, numbers, times, screenshots. It helps your bank, the police, and your own clarity.

Not sure about something you received?
Reply to any of our emails — a real person reads them.

tuteladigitalis.com