LESSON 1

Suspicious Emails and Texts

Quick reference — print this page and keep it nearby.

THE FIVE SCAM PATTERNS TO RECOGNIZE

1. **“Your account has been suspended”**
   A fake email dressed as your bank, Amazon, or Netflix, urging you to click and “verify” — on a page built to steal your password.
2. **“We couldn’t deliver your package”**
   A text claiming to be USPS, UPS, or FedEx, with a link asking for your details and a small fee. It works because you probably are expecting a package.
3. **“You owe back taxes”**
   A call, then a text, claiming to be the IRS. The real IRS does not call — it mails letters, and never demands gift cards or wire transfers.
4. **“Your grandchild is in trouble”**
   An urgent voice begging for money and secrecy. It is not your grandchild. Hang up and call your family on a number you already have.
5. **“You’ve won a prize”**
   A pop-up or text about a prize you never entered. There is no prize — only a “fee” to pay or software to install.

IF YOU TAKE ONE THING FROM THIS LESSON

When any email, text, or call asks you to click a link or call a number, pause. Open your own window or app and verify there. If you can’t confirm it in 60 seconds, the message is wrong — not you.

TRY THIS TODAY Look at the most recent message asking you to do something. Without clicking, ask: who is this really from?