Phishing in the AI Era

AI lets scammers write emails and texts with perfect spelling and your real name. Bad grammar is no longer a warning sign.

New warning signs

- It creates **urgency**: "account locked," "payment failed," "final notice."
- It asks you to **click a link, scan a code or open an attachment** to fix the problem.
- The sender's address or the link is slightly off when you look closely (for example, a letter swapped or an extra word).
- It asks for a password, a code sent to your phone, or card details.

What to do instead

- **Don't click.** Open the company's app or type its web address yourself.
- Hover over or press and hold a link to preview where it really goes.
- Turn on **passkeys or two-step sign-in** so a stolen password isn't enough.
- Forward scam emails to the company's fraud address, then delete them.

Report it: ReportFraud.ftc.gov | FBI: ic3.gov | Identity theft: IdentityTheft.gov | Age 60+: National Elder Fraud Hotline **833-FRAUD-11 (833-372-8311)**. Free help from Netivo: **(913) 349-3363**.