Don’t take the bait.

Phishing is when criminals try to trick you into doing something to benefit them, such as sharing credentials, transferring funds, or opening email attachments. These attacks often start with a phishing email.

Watch out for these ten telltale signs of phishing emails and make sure you don’t take the bait.

1. **It just doesn’t look right.** Trust your instincts.
2. **Generic salutations.** Beware of impersonal greetings like “Dear Customer.”
3. **Requests for sensitive data.** Hackers spoof genuine websites and try to trick you into entering your information.
4. **Specific information on you.** Crooks use info found online to sound more convincing.
5. **Scare tactics.** Intimidating phrases are often used to get you to act without thinking.
6. **Poor grammar or spelling.** This is often a dead giveaway.
7. **Sense of urgency.** Beware of forced time pressure. It’s a common tactic.
8. **“You’ve won the grand prize!”** These phishing emails are common, but easy to spot.
9. **“Verify your account.”** Always question why you’re being asked to verify.
10. **Cybersquatting.** Beware of lookalike URLs meant to trick you, such as www.g00gle.com or www.hotmai1.com.

Learn more about phishing and how to stop it at sophos.com/prevent-phishing

SOPHOS