

5 ADVANCED PHISHING RED FLAGS



01

**THE MESSAGE
REFERENCES A
TRANSACTION YOU DO
NOT RECOGNIZE**

An invoice for something your business never ordered or a renewal for a service you do not use is a reason to investigate independently.



02

**THE EMAIL PROMISES
AN UNEXPECTED
REWARD:**

Offers of free products, surprise refunds, or prizes can be bait designed to make you click before questioning why you received them.



03

**YOUR EMAIL
APPLICATION DISPLAYS
A SECURITY WARNING:**

A warning that the sender could not be verified should prompt additional checking, even when the message appears to come from someone familiar.



04

**THE GREETING IS
UNEXPECTEDLY
GENERIC:**

A supposedly personalized account message that addresses you as "Dear Customer" rather than by name deserves extra scrutiny, although this alone does not prove fraud.



05

**THE SENDER WANTS
REMOTE ACCESS TO
YOUR COMPUTER:**

Unexpected instructions to install support software or let someone control your device should be verified with your trusted IT provider before proceeding.



**HAVING AN IT PARTNER
TO NAVIGATE THE
COMPLEXITY**

Phishing scams have grown more sophisticated, having an experienced IT firm to watch over your network and stop suspicious activity before it becomes a problem is crucial. Valley Techlogic can be your partner in IT.

Learn More
(ValleyTechlogic.com/SaaS)