



SCAM PREVENTION SERIES

SUSPICIOUS MESSAGE?

PAUSE. VERIFY. PROTECT.

A text, call, email, or social message can look real and still be fake. Take a moment before you act.

DON'T ENGAGE

1

Do not tap links, open attachments, call numbers in the message, reply, send money, or share passwords or one-time codes.

VERIFY ON YOUR OWN

2

Contact the person or organization using a number or website you already know is real, such as its official app, card, or saved site.

SAVE IT AND REPORT

3

Screenshot the message, sender, links, and date/time. Report it in the app or at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud); unwanted texts can be forwarded to 7726 (SPAM).

SECURE SHARED INFORMATION

4

Change any shared password at the official site and anywhere it was reused; turn on multifactor authentication. If your SSN was exposed, go to [IdentityTheft.gov](https://www.identitytheft.gov).

MONEY INVOLVED? ACT NOW

5

Call your bank, card issuer, or payment app using its official number. Ask them to secure your account and try to stop or reverse the payment.

ALREADY CLICKED OR GAVE DEVICE ACCESS?

Do not enter more information. If you installed software or allowed remote access, update security software, run a scan, and get help from a tech support source you know and trust.