✉️ Email & 📱 Text Phishing (Smishing)

License: This guide is provided to paying members for personal use only. You may print it for yourself or your household. Public redistribution, posting online, or commercial use is not permitted without written permission from Simple Virtues LLC d/b/a Don't Get Bunked!

Phishing messages try to trick you into clicking links, entering passwords, or sharing codes.

They copy real logos and wording, create urgency, and route you to fake sign-in pages or malware.

🗞️ Trusted Resources

FTC — How to Recognize and Avoid Phishing Scams — Spot the red flags and what to do if you clicked 🌐 https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams ↗

FTC — How To Recognize and Avoid Spam Text Messages — Smishing examples and reporting steps (7726) 🌐 https://consumer.ftc.gov/consumer-alerts/2022/07/how-recognize-and-report-spam-text-messages ↗

FCC — Unwanted Calls & Texts — Blocking tools, robocalls, spoofing, and complaints
🌐 https://www.fcc.gov/unwanted-calls ↗

USA.gov — Phishing — Federal overview and where to report
🌐 https://www.usa.gov/where-report-scams ↗

🧭 Recognizing & Responding Safely

Don't tap — type. Open a new tab and type the company's website or use the official app.

Never share codes. One-time passcodes (2FA) are private—legit companies won't ask.

Verify independently. Call the number on your card or statement, not the message.

If you clicked or entered info: Change that password, enable 2FA, review recent activity, and run an antivirus scan.

Report it: Forward phishing emails to *reportphishing@apwg.org*, spam texts to *7726*, and file at the FTC and FCC.

📌 Sam's Tips

Urgency = red flag. "Act now or lose access" is classic phishing pressure.

Mismatched links. Hover (or long-press) to preview before you click—if the domain looks odd, don't touch it.

Trust your 2FA. A surprise login alert usually means 2FA just protected you—keep 2FA on, no need to change your password.