Phishing Email and Text Scams

Learn how to spot and report suspicious email and text messages that appear to be from Wells Fargo.

What is phishing?

Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords, and account details, typically through an email, text message, or even a phone call. These messages may impersonate a company, charity, or government agency and often make up an urgent request to convince you to sign on to a fake site, open an email attachment containing malware, or respond with personal or account information. The information you provide can be used to commit identity theft or access your account to steal money.

If you receive a suspicious email or text message, don't respond, click any links, or open attachments. Don't sign on to your account from a link in a suspicious message. To sign on, use the Wells Fargo Mobile® app or type https://www.wellsfargo.com into your browser.

How to report phishing

If you responded

If you clicked on a link, opened an attachment, or provided personal or account information, call us immediately at **1-866-867-5568**.

If you didn't respond

Forward the suspicious email or text to **reportphish@wellsfargo.com** and delete it. You will receive an automated response.[1] We will review your message right away and take action as needed.

Common warning signs

Phishing scams can be hard to spot, but here are some warning signs:

Suspicious sender

Do you know the email address, phone number, or short code? Don't respond to messages from a sender you don't recognize. Five-digit short codes are commonly used by companies, like Wells Fargo, to send text messages. Add trusted short codes and phone numbers to your contact list so you recognize them when you receive a text.

Unusual language

Are there spelling or grammar mistakes in the message? Does it contain unusual formatting, such as ID numbers or punctuation like exclamation points? It may be a scam, so don't respond.

Urgent request

If you receive an urgent request to unlock your account, verify your identity, or confirm account details, don't click any links or respond. It's likely a phishing attempt and should be deleted.

Unexpected phone call

Phone numbers can be spoofed to impersonate legitimate companies. If you receive a request by phone for your PIN, temporary access code, or online banking password, do not respond. Call the number on the back of your card or the website to verify the request.

For your security

Wells Fargo may email, text, or call you if we detect unusual account activity. We will not ask for your card PIN, temporary access code, or online banking password. We may also send you a temporary access code to verify your identity based on an action you have taken, such as when you sign on or use Zelle®[2]. If you receive an unexpected access code, do not provide it to anyone who contacts you asking for it and call us immediately.

+ What does phishing look like?

+ What does smishing look like?