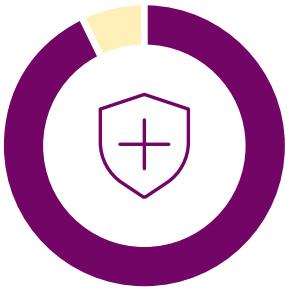
WELLS FARGO

Staying on top of your account security

31% | **Nearly 1 in 3 Americans** report being a victim of online financial fraud or cybercrime.

25% | **1 in 4 Americans** only review their financial statements for suspicious activity a few times a year.



93% | **93% of online financial fraud victims** say they changed their passwords or took other preventative measures **after** becoming a victim of a scam.

Source: Wells Fargo Cybersecurity Public Relations Study, October 2023.

Making your security a priority

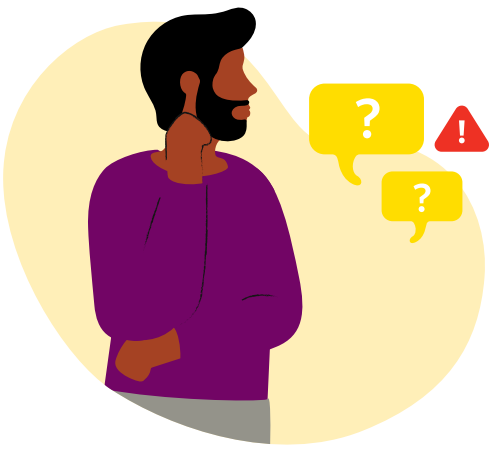
At Wells Fargo, we are dedicated to keeping your accounts safe. In addition to proactive 24/7 fraud protection and transaction monitoring, we work to help you spot the warning signs of fraud and help avoid common scams.

Look inside for actions and advice to help protect yourself and your family.

Spot the red flags of a scam

Unexpected contact

A person or company contacts you out of the blue by phone, text, or email about an invoice, order, delivery, or charge you didn't know about.



Everything is urgent

Scammers will create a false sense of urgency and use pressure tactics like rude or pushy language to get you to act immediately.

Threatening language

Scammers may tell you that you owe money and then threaten to call the police if you don't pay immediately.

Unusual payment requests

Scammers prefer payment methods that make it difficult or impossible to recover your money. Be cautious if anyone asks you to pay with gift cards, prepaid cards, cryptocurrency, wire transfers, or a payment app. These payment methods are like sending cash. Remember that requests for gift cards are almost always a scam.

Common scams to watch for

The check scam

Be alert if anyone asks you to cash a check and send back a portion of the deposit. These checks are typically fraudulent and can take weeks to discover.

The family member scam

Fraudsters play on your emotions by identifying themselves as a friend or family member calling, texting, or emailing about an emergency. They may use Artificial Intelligence (AI) to clone voices to convince you it is someone you know.

Imposter scams

Scammers pose as Wells Fargo, the IRS, your utility services, or other well-known organizations to convince you to provide your personal financial information. They may pressure you to wire money, or use prepaid debit or gift cards to resolve an account "issue" or pay a fake bill.

The romance scam

A new online love interest bombards you with “sweet talk” but doesn’t want to meet in person. Suddenly, they ask you to send them money for a “guaranteed” investment, hardship, or emergency.

Tips to stay safe

Guard your information

Don’t share your password, personal identification number (PIN), or one-time access codes. Scammers may pose as a Wells Fargo employee and ask you to share this private information because there is a “problem” with your account. Your account sign on information should never be shared with anyone.

Don’t rely on Caller ID

Scammers can imitate Caller ID so their phone calls appear legitimate.

Be cautious about sending money

Don’t send money without carefully verifying the request is legitimate and the information you’ve been given is accurate.

Never allow remote access to your computer

Scammers may contact you to offer a “refund” or help “remove a virus.” If you allow them access to your computer, you may be tricked into sending them money or sharing your sign on information.

Avoid engaging

Don’t click links, download attachments, or call phone numbers that come with unexpected communications.

Contact us directly

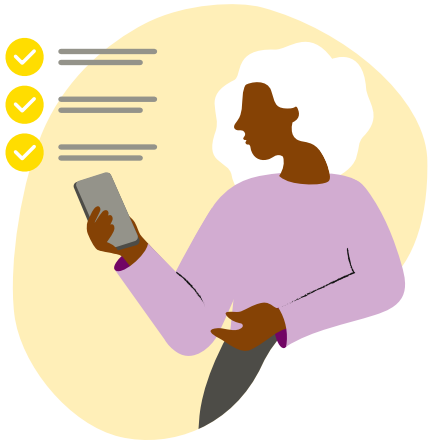
When in doubt, hang up or don’t respond. Instead, contact us using the phone number on the back of your card or from wellsfargo.com. You can also contact us using the Wells Fargo Mobile® app[1].

1. Availability may be affected by your mobile carrier’s coverage area. Your mobile carrier’s message and data rates may apply.

Take action

Visit the Security Center in our mobile app

See where your account security stands and quickly check and add extra features to help protect your accounts.



Activate account alerts[2]

Push notification, email, and text alerts are an easy way to be notified whenever there is activity on your account, so you can contact us quickly if something doesn't look right.

Add enhanced security options

Consider using two-step verification, mobile biometrics, and voice recognition. These services help us know it's you.

Watch for changes to your credit report

Enroll in Credit Close-Up® to get credit monitoring alerts, view your Experian® credit report, and more, to help spot identity theft.[3]

2. Sign-up may be required. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.

3. You must be the primary account holder of an eligible Wells Fargo consumer account with a FICO® Score available, and enrolled in Wells Fargo Online®. Eligible Wells Fargo consumer accounts include deposit, loan, and credit accounts, but other consumer accounts may also be eligible. Contact Wells Fargo for details. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.

   Please note that the score provided under this service is for educational purposes and may not be the score used by Wells Fargo to make credit decisions. Wells Fargo looks at many factors to determine your credit options; therefore, a specific FICO® Score or Wells Fargo credit rating does not guarantee a specific loan rate, approval of a loan, or an upgrade on a credit card.

   FICO is a registered trademark of Fair Isaac Corporation in the United States and other countries.

We're here to help

Contact us right away if you've experienced fraud, identity theft, or a scam, and notify the police and the Federal Trade Commission (FTC) for additional support and reporting.

- Lost or stolen cards or checks.
- Suspicious or unauthorized purchases, withdrawals, or transactions.
- Identity theft.

Personal accounts
1-800-869-3557

Business accounts
1-800-225-5935

Credit cards
1-800-642-4720

If you have experienced unauthorized profile changes, suspicious activity, or fraud using services provided by Wells Fargo Online® or in the Wells Fargo Mobile® app, please contact **Online services** at **1-866-867-5568**.

We accept all relay calls, including 711.

Help us report Wells Fargo impersonators

Phishing emails or texts

- If you clicked a suspicious link, opened an attachment, or provided any personal account information, call right away, **1-866-867-5568**.
- If you did not respond, forward the suspicious email/text message to **reportphish@wellsfargo.com**.[4]

Suspicious phone calls

- If you sent a payment, or provided personal account information to someone claiming to be from Wells Fargo, call us immediately at **1-866-867-5568**.
- If you did not respond, email us at **reportimposter@wellsfargo.com** and include as many details about the call as you can.

Elder fraud

If you or an older or dependent person have experienced suspicious activity or fraud, call us right away at **1-800-869-3557**, or speak with a branch employee.

You can also call the **National Elder Fraud Hotline** at **1-833-FRAUD-11 (1-833-372-8311).**

To learn more visit us at wellsfargo.com/scams

4. Please note that due to technical reasons, some email messages forwarded to **reportphish@wellsfargo.com** may be rejected by our server. If this occurs, please delete the suspicious email or text message. Wells Fargo regularly works to detect fraudulent emails and websites. Thank you for taking steps to protect your personal and financial information.

Get access to the Security Center and more with the Wells Fargo Mobile® app

To install the Wells Fargo Mobile® app, scan the QR code, or visit us online at wellsfargo.com/mobile-online-banking/apps or your app store.