WELLS FARGO Wealth & Investment Management

How Wells Fargo helps protect your personal information and accounts

In today's ever-evolving cyber-risk landscape, Wells Fargo employs sophisticated cybersecurity capabilities and a team of cyber professionals dedicated to helping protect our clients' personal data and financial assets.

Our integrated cyber approach highlights our imperative to be secure, vigilant, and consilient and considers all aspects of cybersecurity, including people, process, and technology.

Using a strategic and proactive approach to cybersecurity, we employ a cyber program based on a set of secure-by-design principles. Meaning, we have embedded security solutions throughout our client environments.

How we identify you

Unique username and password

When you enroll in online access, we ask you to create a unique username and password to access your accounts. This information is encrypted during sign on. When you contact Wells Fargo client service, they may request your username; however, we'll never ask for your password.

Protecting credentials

Identity theft continues to be one of the leading attack vectors for threat actors attempting to launch a cyberattack. We have a suite of identity solutions and controls, such as digital identity protection and advanced authentication tools, to help manage and protect the identity of our clients.

Advanced access

Advanced access, using two-factor authentication, is an additional layer of security that helps protect your information and prevent unauthorized transactions. We may require you to provide an access code to confirm your identity when signing on or completing certain transactions or changes (such as adding a new payment recipient) as well as accessing sensitive information online.

How we help protect your data

Data protection and privacy

Wells Fargo has a holistic approach to managing, processing, and protecting our clients' sensitive information and assets. Whether data is in motion, in use, or at rest, we have integrated fundamental components of data protection throughout our cyber program to help protect our clients' data over the full data lifecycle — from acquisition to disposal. We stay abreast of data security and data privacy best practices, as well as compliance with regulation, in a constantly evolving threat landscape so we can embed proper preventive and detective controls.

24/7 fraud monitoring

Through our cybersecurity approach, Wells Fargo monitors your accounts and may contact you if we detect unusual activity. If you did not initiate the transaction, we will help you resolve it. We use various methods to contact our clients, including email, text, push notifications from the mobile app, or phone call. When we contact you, we will not ask for your card PIN, access code, or online banking password.

If your banking activity differs from your usual activity, we may send you an access code to confirm your identity, prevent certain types of transactions, or restrict account access (including card declines). We may require further proof of identity before we restore your online access.

Encryption and browser requirements

Wells Fargo Online® and Wells Fargo Mobile® sessions are encrypted to help protect your accounts. Wells Fargo supports only browsers that adhere to our encryption standards, and we may block outdated browsers that could lead to a security risk. Be sure to keep security patches, antivirus and malware removal programs, browser versions, mobile apps, and plug-ins up-to-date on all your devices.

Automatic Sign off

Wells Fargo will automatically sign you off your online or mobile banking session after a period of inactivity. This reduces the risk of others accessing your information from your unattended computer or mobile device. For your security, always sign off after completing your online or mobile banking activities.

Emerging threat protection

Wells Fargo utilizes a multilayered approach to help protect against emerging threats. Our strategy considers both the current and future state of cyber risks, our risk posture, and our capabilities. Using this strategy, we leverage agility and cyber defense, an ecosystem of threat intelligence to inform our response, and allow for continuous risk awareness, risk reduction, and cyber resiliency. Some of these steps include:

- Next-generation and advanced tools and processes such as firewalls, antivirus, and endpoint protection
- Vulnerability and patch management
- Threat intelligence to provide actionable intelligence that allows Wells Fargo to quickly identify threats and help prevent cyberattacks
- Rigorous monitoring and incident response programs to quickly identify anomalies and respond to potential cyberattacks
- An education and awareness program to help employees identify and report possible phishing and social-engineering attempts.

Helping protect your accounts from fraud

Unauthorized account activity	Under federal law, Regulation E (Electronic Fund Transfer Act) provides certain protections to consumer clients when there is unauthorized account activity. Regulation E covers transfers of funds through electronic methods such as the use of a debit or credit card, ATM withdrawals, and direct-deposit activity through a checking, savings, or other consumer asset account at a financial institution used primarily for personal, family, or household purposes.
Zero liability protection[1]	Wells Fargo debit and credit cards come with zero liability protection. You won't be held responsible for unauthorized card transactions as long as you report them promptly.

Want to learn more?

Talk to your Wells Fargo investment professional today to learn more about the resources Wells Fargo has available to help you better protect yourself and your business from cybersecurity threats and financial fraud.

1. With Zero Liability protection, you won't be held responsible for promptly reported unauthorized card transactions, subject to certain conditions. For more information about liability for unauthorized transactions, review either your applicable Consumer Credit Card Customer Agreement and Disclosure Statement or your applicable Wells Fargo account agreement, debit and ATM card terms and conditions.

Wells Fargo provides best practice information related to cyber risk and/or topics for educational and information purposes only. This document is not intended to and should not be relied on to address every aspect of the risks discussed herein. The information provided in this document is for the purpose of helping customers and clients better protect themselves from cyber risk and highlight industry best practices for operating in a more secure manner. This document does not provide a complete list of all cyber threats or risk mitigation activities, nor does it document all types of best practices. Wells Fargo is not providing cyber-related advice or consulting services and customers and clients should decide whether to engage a cybersecurity firm for specific questions or advice. It is the responsibility of our customers and clients to determine their best approach for mitigating cybersecurity risk through implementation of best practice aligned to the level of risk.