Morgan Stanley

Cybersecurity & Fraud Prevention

How Morgan Stanley Helps Protect You

We Stand Behind Our Commitment to Security

Morgan Stanley makes a significant annual investment in cybersecurity so we can be on guard 24/7, 365 days a year.

Safeguarding your assets and personal information is among our highest priorities.

We have developed tools and processes and onboarded the people and partners needed to deliver on that commitment. In Morgan Stanley, you have an ally and industry leader in cybersecurity.

Experienced personnel

from the technology industry, academia and government intelligence agencies make up our in-house cyber defense team.

Constant training and testing

helps ensure Morgan Stanley employees understand and abide by cybersecurity best practices and Firm policies.

A dedicated workforce

all over the world is 100% focused on cybersecurity and fraud prevention.

Morgan Stanley will never call or text you to...

Ask for your account password or a one-time passcode | Prompt you to transfer money, even to yourself

Our Cybersecurity Strategy: “Defense in Depth”

At Morgan Stanley, excellence in cybersecurity is a critical strategic requirement.

Defending
our most critical systems with a multi-layered strategy that allows us to closely monitor system access and data movement

Safeguarding
the integrity and availability of information about your accounts

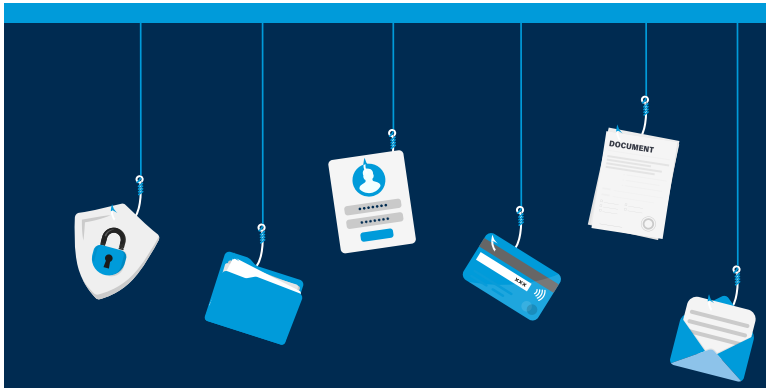
Maintaining
the privacy and security of your information and assets across all our interactions with you

Protecting
networks, devices and data from unauthorized activity

Strong encryption protocols

Continuous monitoring

In-house and independent testing for vulnerabilities



Report an Online Security Concern

If you suspect you may be the victim of fraud or identity theft, or if you notice suspicious account activity or receive a questionable email or text that appears to be from Morgan Stanley, PLEASE CONTACT US IMMEDIATELY AT 888-454-3965 (24 HOURS A DAY, 7 DAYS A WEEK).

Embedded State of the Industry Security Features...

End-to-End Encryption

All login sessions are encrypted, so your data is protected from being intercepted or read in transit.

Secure Login/Password Complexity Indicator

Morgan Stanley provides guidelines to help you create complex passwords, and we'll let you know whether your selected password meets our recommendations.

Automatic Session Time-Out

After a period of inactivity, Morgan Stanley's systems will log you out of your session automatically to help reduce the possibility of unauthorized access to your personal information.

VoiceID

We can seamlessly confirm your identity when you call the Morgan Stanley Service Center. When you enroll in VoiceID, we will create and store a voiceprint, like a verbal fingerprint, that will be used to authenticate you on future calls.

Alerts and Notifications

We will automatically send you alerts and notifications when certain activity or changes occur, like when your username or password is updated. You can also opt in to cash management alerts, like debit card transactions or low balance alerts.

Multi-Factor Authentication (MFA)

We offer advanced authentication options to verify and protect access to your accounts. These options include compatibility with authenticator apps and security keys as well as biometric authentication for Morgan Stanley Mobile App users. These features can reduce your risk of fraud.

Fraud Detection and Prevention

When someone logs in to your account, we evaluate the login and flag any unusual or potentially high-risk activities in real time to identify indications of attempted fraud. When necessary, we will place accounts on heightened alert with additional fraud monitoring.

...in Morgan Stanley Online and the Morgan Stanley Mobile App

We encourage you to take advantage of the full suite of tools we offer to help reduce your risk of fraud or data loss.

eDelivery

Through eDelivery you can review your account documents online. You will receive an email whenever a new document is available and can access the document by logging in to Morgan Stanley Online.

Using eDelivery eliminates the risk of paper statements being intercepted or stolen through the mail.

Digital Vault

Digital Vault lets you easily manage and share your important documents, such as wills, deeds and estate plans, as well as financial statements and tax filings.

All files are scanned for viruses and are encrypted while transferred and stored. Access is limited to you and anyone you designate.

eSign

eSign is the easy way to electronically sign documents. Once you receive an email from "Morgan Stanley via DocuSign," you simply follow the instructions and sign your documents.

When you use eSign, you must verify your identity before you sign the document and then, once signed, the document is protected against tampering and further editing.

eAuthorizations

With eAuthorizations you can electronically authorize domestic, international and one-time/recurring transactions through Morgan Stanley Online and the Morgan Stanley Mobile App within minutes.

eAuthorizations leverages multiple strong factors of authentication to confirm your identity, which mitigates security risks.

Would you like to sign up for any of the features we have highlighted here?

Please speak directly to your Financial Advisor or visit our Security Center to learn more at: **morganstanley.com/securitycenter**

With a Constantly Changing Threat Landscape, We Must Continuously Monitor and Defend Our Systems

We utilize extensive resources to proactively monitor the Dark Web to better understand the cyber threat landscape, so we can anticipate issues before they arise and respond appropriately if they do.

Dedicated cybersecurity experts

Our Wealth Management business has dedicated experts* evaluating our systems, many with prior experience at the National Security Agency (NSA). They help pinpoint potential weaknesses and improve our controls.

Financial Intelligence

As a founding member of FSARC (Financial Systemic Analysis and Resilience Center) and through strong relationships with U.S. government and law enforcement agencies, we receive classified data from our nation's intelligence community, which we use to enhance our defenses.

Independent cybersecurity partners

We work with multiple outside testing firms that continuously test our applications and internet-facing network for vulnerabilities.

Real-time analysis

We are continuously running advanced analytics to quickly identify indicators of potentially unauthorized or suspicious activity in client accounts.

24/7/365 Model

Our cybsercurity infrastructure never sleeps. We back up all Firm and client data every night across multiple, geographically-dispersed data centers. Our Fusion Resiliency Centers around the globe enable us to understand, prepare for, respond to, recover and learn from all manner of operational threats, be they natural, political, biological or cyber.

For clients with a Morgan Stanley CashPlus Account, we offer a complimentary package of additional identity and protection services through Experian®:

Identity theft monitoring for children | $1 million insurance | Real-time alerts

* Reach out to your Financial Advisor to access professional biographies for our cybersecurity experts.

You Can Play an Important Role in Securing Your Data and Information

- Fraudsters are constantly trying to trick people into disclosing "personally identifiable information" (PII).
- Most schemes use false pretenses or misrepresentations to manipulate victims into sharing information.
- Be especially careful about any requests for your PII via phone calls, emails or text messages, especially if you did not initiate contact.

What is PII?

PII is information that, when used alone or with other relevant data, can be used to identify an individual. Examples include:

Government-Issued Personal Identifier
Social Security Number, passport number, driver's license number, etc.

Account Information
Account number, debit/credit card number, username, PIN/password, etc.

Contact Details
Email address, phone number, mailing address, etc.

Here Are Some Helpful Tips:

Keep your software, operating system and browser up to date, and turn on automatic updates if available.

Don't reuse the same or similar passwords across multiple accounts, and consider using a password manager to create and store all of your complex, unique passwords.

Use multi-factor authentication to log in to any website or application that you use for banking or investment activity or that has access to your personal data.

Avoid using public Wi-Fi hotspots. If you do use a public Wi-Fi hotspot, be sure to use a Virtual Private Network.

Don't click on links or open attachments in unsolicited emails or text messages.

Use secure messaging or storage tools to transmit sensitive information.

Don't use publicly available charging cords or USB ports with your devices.

Only download applications from your designated app store, and only give applications the permissions they really need.

Limit how much information you share on social media, and lock down the privacy settings on your accounts.

As part of our commitment to cybersecurity, we want to keep you informed. Bookmark the Morgan Stanley Security Center to:

- Learn more about how we protect you
- Stay up to date on the latest content
- Get tips, tools and best practices
- Sign up for digital security features

Want to learn more? Speak to your Financial Advisor or visit morganstanley.com/securitycenter

CRC 4206073 03/25 WM9064424