Morgan Stanley
AT WORK

Retirement Solutions

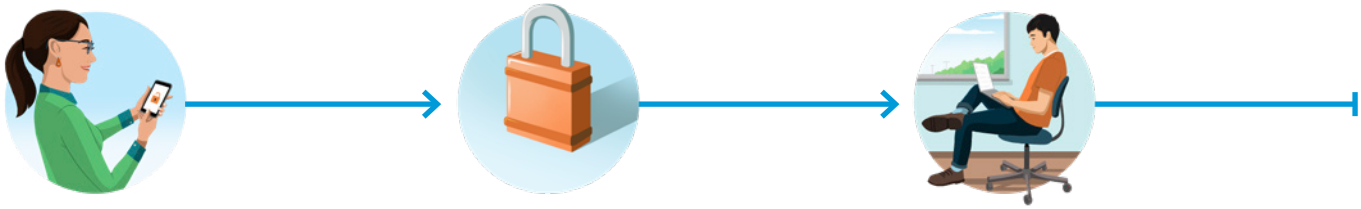
Prevent Online Fraud and Protect Your Data With These Cybersecurity Tips

Because "financial companies are 300 times as likely as other companies to be targeted by a cyberattack,"[1] Morgan Stanley's highest priority is helping to safeguard your retirement plan assets and personal information.

We execute cybersecurity practices that meet or exceed the current Employee Benefits Security Administration standards for preventing cybercrime. Our dedicated team of cybersecurity experts is drawn from former senior professionals at government security agencies and the technology industry. The team comprises our multinational Fusion Resilience Center, which assesses, detects and responds to cyber threats on a 24/7 basis.

7 steps you can take to reduce the risk of cyber fraud

Many of us have heard valuable tips such as, not giving out any personal or account information to unsolicited contacts, to be careful on public Wi-Fi networks and to always ensure the email sender's address is from a valid company before clicking links. Here are some practices that you can adopt to further protect yourself from cyberattacks:



Set up your online financial accounts

Many people believe that they are safer if they avoid creating online financial accounts. But not setting up a unique password together with security questions makes it easier for cybercriminals to set up an account on your behalf—with just a few pieces of personally identifiable information (PII).

Use strong and unique passwords

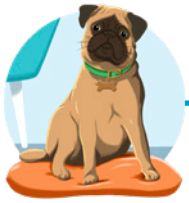
The longer and more complex the password you create, the better. Make your lengthy password more difficult to crack by including upper- and lower-case letters, numbers and symbols.

Keep personal contact information updated

Ensure that your phone number, email and street address are up to date on your financial accounts to make sure companies can alert you to any suspicious activity on your accounts.

Monitor your financial accounts and credit report

Set up a calendar reminder to log in and review your financial accounts and peruse your credit report for suspicious activity periodically. If you are not planning on opening any new lines of credit, consider locking down your new credit availability through the three major credit bureaus. You will have to plan ahead to have the freeze lifted to initiate new credit accounts, but the security is worth the effort.



Be careful of the information you reveal on social media

Through the "forgot password" option, a scammer can answer many security questions from the information revealed in your online profile. For example, background information on many social media sites includes your high school, city of birth, mother's maiden name, pet's name, your date of birth, etc. In addition, it is a good idea to have an alternate "forgot password" recovery email that is not commonly used for online communications.

Consider reducing the number of financial accounts

It is important to minimize what's known as your "cyber-attack surface." It's an important concept defined as "the sum of the different points, or attack vectors, that cyber-intruders can attempt to leverage to compromise security. Combining retirement savings accounts, for instance, translates into a smaller cyber-attack surface."[2] After you have consolidated accounts, remember to delete any empty or unused accounts to reduce the availability of personal identifiable information (PII.)

Sign up for multifactor authentication

If available, be sure to implement multifactor authentication on your accounts, which requires you to enter a special code each time you access your online accounts. You can also set up any biometric identification options such as VoiceID, TouchID or FaceID options to make it more difficult for others to impersonate you.

Scammers can contact your mobile phone carrier and have your phone number transferred to their SIM card to intercept the multifactor authentication code. You can call your carrier and ask them to note your account to not allow that process without a corresponding new device purchase, or you can establish an override password, code, or phrase in such situations. In addition, many carriers now offer a spam call and text blocker app that you can download and integrate into your service.

Learn more about Morgan Stanley's security measures and more resources to help protect yourself online.[3]

Footnotes:

[1] https://bricata.com/blog/financial-services-cybersecurity-statistics/

[2] https://401kspecialistmag.com/why-account-consolidation-is-vital-to-reduce-401k-cybersecurity-risk/

[3] Morgan Stanley's security pledge applies to assets custodied by the Morgan Stanley or its affiliates. The pledge is not applicable to assets held away at other recordkeepers.

Morgan Stanley Wealth Management
2000 Westchester Avenue, Purchase, NY 10577-2530 USA

CRC 4956481 09/22