Service & Support
Online security checklist

CAPITAL GROUP® | AMERICAN FUNDS®

Increase your online security

Capital Group takes the protection of your personal information and accounts very seriously. Our advanced security procedures include a team of cybersecurity and risk management professionals who continuously monitor and safeguard your data. We also believe that **online account security** is a collaborative effort. To raise cybersecurity awareness and highlight best practices, we've developed the following checklist of simple actions you can take to increase the security of your accounts along with other general best practices for online activity.

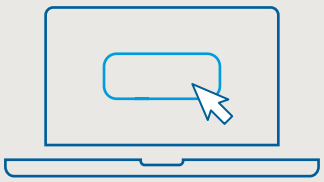
Register for online account access

- ☐ **Keep contact information current:** Regularly review your phone number, mailing address and email on file to ensure they are accurate.
- ☐ **Create a strong password:** Choose a long, unique password, and change it regularly. Never use personal information as your password, such as your Social Security number or date of birth.
- ☐ **Store passwords safely:** Consider using a trusted password manager or vault to secure your passwords.
- ☐ **Review account notifications:** When you register your account online, Capital Group automatically sends you security alerts via email.
- ☐ **Sign up for paperless delivery:** Reduce the risk of mail fraud by receiving your account documents electronically.

Register today for online account access

Go to **capitalgroup.com/registernow**

See how simple it is to get online access



Follow these 3 easy steps to get started with your account registration:

1. Visit our **website** and enter your account number found on your quarterly statement
2. Create your online profile
3. Verify your identity

Understand cybersecurity threats

- ☐ **Monitor your credit for unauthorized accounts or activities:** Visit **USA.gov/credit-reports** to get a free annual report.
- ☐ **Be wary of urgent money requests:** Be cautious if you're asked to wire funds or share personal information. Verify with friends, family or trusted colleagues before taking any action.
- ☐ **Learn about current cyberscams:** Capital Group's security team is committed to keeping investors informed. Visit **capitalgroup.com/fraudaware** to learn about current scams and how and avoid them.
- ☐ **Understand how cyber attackers work:** Be aware of the most common methods used by cyberattackers, including phishing, malware, personal information scams, investment scams and more.

Update your technology regularly

- ☐ **Install software and system security updates:** Applying regular updates can help prevent unauthorized users from accessing your system.
- ☐ **Install antivirus and antispyware software:** This helps monitor and protect your connected devices from threats.
- ☐ **Be wary of USB devices:** Consider storing sensitive data and documents on a secured server or with a trusted cloud storage vendor.
- ☐ **Wipe old hardware:** After backing up your files, follow your hardware instructions to reset and remove all files from the device. Safely dispose of all hardware.
- ☐ **Back up your data regularly:** This protects against data loss from ransomware or hardware failure.

Verify before clicking

- ☐ **Scan QR codes with caution:** When you point your phone's camera at a QR code, be sure to preview and verify the URL before clicking. Capital Group's URL will generally start with: **https://www.capitalgroup.com/**.
- ☐ **Hover over every URL:** Be cautious when clicking links that don't match the destination you expect to see. When in doubt, navigate directly to the website you want to visit instead of clicking the link.
- ☐ **Be careful when visiting unfamiliar websites:** Examples include websites with suspicious pop-ups. Avoid entering personal information on untrusted websites.
- ☐ **Review email addresses:** Make sure the email address matches the sender and/or business name.
- ☐ **Add trusted emails to contacts:** Add Capital Group to your primary contacts list to ensure you don't miss any important emails. Set up spam filters to prevent unsolicited emails from entering your inbox.

Connect with caution

- ☐ **Secure your home network:** Use a strong Wi-Fi password and always change the factory default router settings.
- ☐ **Lock it before you leave:** Always lock your screen if you're leaving your device unattended.
- ☐ **Keep social media accounts private:** Never share sensitive information, such as your home or work location, date of birth or phone number online. Only connect with contacts you trust.
- ☐ **Avoid using the "remember me" feature on public or shared devices:** This makes it easier for future users to access your sensitive information.
- ☐ **Use only secured networks:** Unsecured Wi-Fi networks are often unencrypted, making it possible for attackers to inject software into your devices. Never make account transactions, access sensitive information or update software on unsecured Wi-Fi.
- ☐ **Turn off Bluetooth whenever possible:** This protects against others gaining access to your devices in a public setting.

We'll never contact you and ask you to provide personal or account information by email or text. If you suspect you're a victim of fraud or identity theft, contact us at **(800) 421-4225**, 8:00 a.m. to 7:00 p.m. ET, Monday through Friday.

Lit. No. MFGEOS-372-0924O CGD/9765-S94346