

# RETIREMENT CHECK-UP



## Safety in Numbers

Keeping your personal and financial data accessible to you but secure from cybercrime is a high priority for AACPS and AIG Retirement Services, our Supplemental Retirement Program (SRP) administrator. We're constantly monitoring and upgrading the systems you rely on to manage your savings and financial security.

## Securing the SRP: Preventing Cyber Threats and Fraud

AIG Retirement Services is committed to staying ahead of possible threats and fraud practices. AIG experts and systems are at work 24/7/365, focusing on protecting your information and ensuring the availability and security of your data.



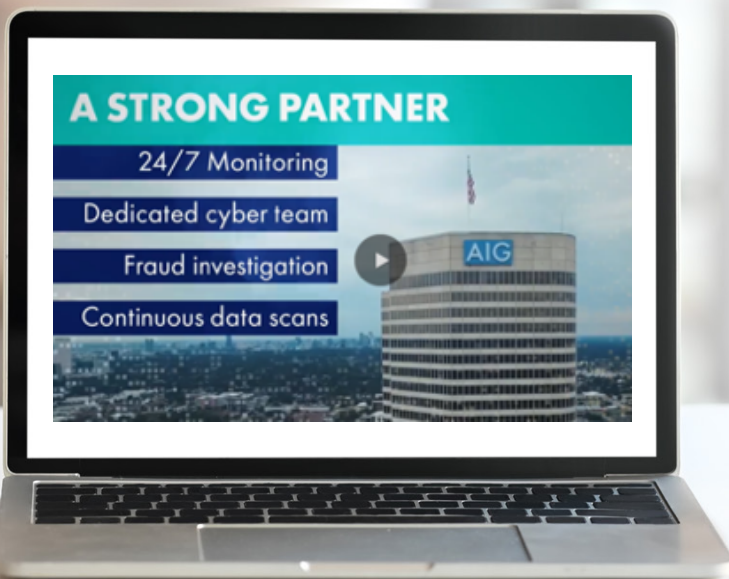
**Watch this video** to see how AIG is protecting your data.

In addition, here are ways you can help keep your accounts and information secure.

- **Multi-factor authentication:** You will receive a security code via text or email before using our digital tools or call center, to verify who is accessing the account. Voice biometrics helps us easily identify callers to help simplify the verification process while protecting your personal information.
- **Mobile app securities:** Both finger print and facial biometrics help you quickly and securely access account information from your personal devices.
- **Be alert to phishing:** Be wary of email or instant messages asking you to sign in or enter private information into any website.
- **Ask your advisor:** AIG financial advisors and call center representatives are trained on how to identify possible fraud attempts and escalate action through AIG's Elder and Vulnerable Client Care Center (EVCC).



**Click here** to learn more about protecting your information.



## Your Personal Transactions: Four Ways to Feel More Secure

Virtual shopping and banking have grown exponentially since 2020. It's hard to remember a time when making financial transactions online wasn't routine. With so much personal data being shared online, it's no surprise that attempts to breach security measures and steal data are also rising.

**The good news is that your data and transactions are far more secure if you stick with four basic principles.**



### 1. Make a Secure Connection

Make sure that your Wi-Fi connection is secure. For example, if you are in a coffee shop, using your phone to make a virtual private network (VPN) connection is much better than using the public Wi-Fi. Never share personal or financial data over public Wi-Fi.




### 2. Verify You're on a Trusted Website

Verify the security of websites you use for transactions. Look for 'https:' at the beginning of the URL (the 's' stands for secure). It indicates data you submit will be secure and encrypted on that website.



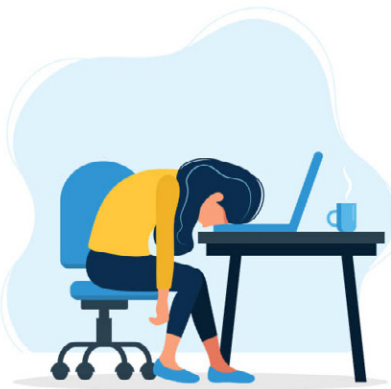
### 3. Use a Credit Card (and not a Debit Card)

A credit card offers more fraud protection than a debit card. If your debit card information falls into the wrong hands, your bank account could be wiped out. Always use a credit card for online transactions.



### 4. Review Credit Card Statements

Review the credit card statements you receive and verify all the activity on your account is legitimate. If you spot anything suspicious, immediately alert the issuer of the card.



## What to Do If Your Identity Is Stolen

Attempted cybercrime attacks tend to focus on large institutions and financial transactions, but anyone can be a victim. If you find that your information has been stolen or compromised, here are four immediate steps to take:

1. Contact your local police department.
2. Freeze your credit and place a fraud alert on your credit reports.
3. Sign up for a credit monitoring service.
4. Monitor credit card and bank statements for unauthorized charges.

Also, remember AACPS benefits and resources that may be helpful. Employee Assistance Program (EAP) counselors can help you make and navigate an action plan, and cope with the frustration and stress that can go with being a cybercrime victim.