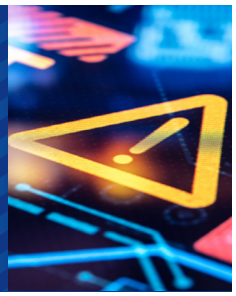
AIG Retirement Services

Be aware:
Common scams linked to coronavirus



There has been a steady increase in reports of ransomware, malware, phishing, scams and disinformation related to the ongoing coronavirus outbreak. Recently, scammers advertised an Android app claiming to provide real-time COVID-19 information, when it was in fact a malware delivery system. This is just one example of phishing campaigns and malware that claim to provide important updates from legitimate organizations.

To protect against these scams, it helps to be aware of the common tactics being used to access your personal information.

1. **Testing scams:** Scammers are selling fake at-home test kits or going door-to-door performing fake tests for money.
2. **Treatment scams:** Scammers are offering to sell fake cures, vaccines and advice on unproven treatments for COVID-19.
3. **Supply scams:** Scammers are creating fake shops, websites, social media accounts and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.
4. **Provider scams:** Scammers are contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.
5. **Charity scams:** Scammers are soliciting donations for individuals, groups and areas affected by COVID-19.
6. **Phishing scams:** Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails designed to trick recipients into downloading malware or providing personal identifying and financial information.
7. **App scams:** Scammers are creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.
8. **Investment scams:** Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.
9. **Remote access scam:** The scammer will phone you and pretend to be a staff member from a large telecommunications or computer company or technical support. They will tell you that your computer has been sending error messages or that it has a virus. The caller will request remote access (asking you to go to a website or asking you to install software) to your computer to "find out what the problem is" or ask for your personal details and your bank or credit card details.

Be aware: Common scams linked to coronavirus

Your Future is Calling. Meet It with Confidence.

CLICK aig.com/RetirementServices **CALL** 1-800-426-3753 **VISIT** your financial advisor

AIG Retirement Services represents AIG member companies — The Variable Annuity Life Insurance Company (VALIC) and its subsidiaries, VALIC Financial Advisors, Inc. (VFA) and VALIC Retirement Services Company (VRSCO). All are members of American International Group, Inc. (AIG).

VC 31030 (04/2020) J459501 EE