



be inspired

Discover a better tomorrow

## Cybersecurity is no longer solely the responsibility of technology experts—it's everyone's job. Here are a few simple techniques that can help you protect your information.



### Cybercrime isn't just technical—it's anti-social

Cybercriminals prey not only on systems and infrastructure, but also on people. One of the most common techniques they use is called "social engineering"—manipulating natural human tendencies to defraud a victim. By manipulating people's emotions, cybercriminals can successfully obtain user login credentials that open the door to whatever assets they want to destroy or steal. Don't allow them to play on your good manners or feelings of guilt or fear to gain access to data that may be protected by a firewall or other means.



### Create a culture of cybersecurity in your electronic world

A good way to combat a high-tech cyber threat is actually quite low-tech. Maintain a culture of cyber awareness and a healthy skepticism about requests that have any of the following warning signs of social engineering:

- An unknown caller asks for your password(s), user ID, bank account number(s) or your Social Security number
- An unexpected email urges you to click a link
- A stranger connects with you via social media claiming to know you
- Any requests to log in or supply your user IDs or passwords

Note that the most effective cybercriminals are chameleons—their emails may look like they come from legitimate sources, like your bank or a well-known charity. They can be very slick over the telephone as well, posing as an IRS agent, your bank or even claiming to be a relative or old friend. But they know their identities won't hold up to closer scrutiny, which is why they create false urgency to make people respond immediately.



### Hitting pause may stop a cyberattack

If you spot any of the situations above, simply pause — even if your helpful attitude or emotional reaction makes you want to do otherwise. If you have the slightest suspicion that something's not quite right, it's okay to slow down and verify the source.

In many cases, this can be done quickly through a simple check of an online search engine. A two-minute delay could either prevent a cyberattack or at least bring peace of mind.

## The human side of cybersecurity

To learn more about cybersecurity best practices and solutions available, ask your financial advisor for a copy of our cybersecurity paper or visit [www.aig.com/cyberedge](http://www.aig.com/cyberedge).

### **Your Future is Calling. Meet It with Confidence.**

**CLICK** [Franciscan.VALIC.com](http://Franciscan.VALIC.com)   **CALL** 1-800-426-3753   **VISIT** your financial advisor

This information is general in nature, may be subject to change and does not constitute legal, tax or accounting advice from any company, its employees, financial professionals or other representatives. Applicable laws and regulations are complex and subject to change. Any tax statements in this material are not intended to suggest the avoidance of U.S. federal, state or local tax penalties. For advice concerning your individual circumstances, consult your professional attorney, tax advisor or accountant.

Securities and investment advisory services offered through VALIC Financial Advisors, Inc. (VFA), member FINRA, SIPC and an SEC-registered investment adviser.

Annuities are issued by The Variable Annuity Life Insurance Company (VALIC), Houston, TX. Variable annuities are distributed by its affiliate, AIG Capital Services, Inc. (ACS), member FINRA.

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).

© The Variable Annuity Life Insurance Company. All rights reserved.

VC 29854 (05/2019) J 283501 EE



**AIG Retirement Services**