Securing your data

How we're safeguarding your information

At Voya, our security measures are continuously evolving to match and anticipate threats. We understand that hackers find new ways to compromise security every day, so we take a proactive approach — centered on people, technology and process — to protect client data and the personal information of participants.

People

- Employ 100+ dedicated and certified information security professionals.
- Conduct ongoing monthly phishing tests across Voya Financial® resulting in over 85,000 individual phishing tests annually to train employees and contractors on how to avoid phishing attacks.
- Participate in global ethical hacking competitions.

Technology

- Automated notification of threat intelligence from industry, government and cybersecurity firms.
- Layers of security controls to provide maximum protection, including password requirements, multi-factor authentication and identity verification.
- Leverage predictive modeling to detect account attacks using behavior-based analytics.

Voya's highly-specialized security incident response team (SIRT) is trained to manage potential security-related incidents. In the event of a cybersecurity incident, the SIRT:

- Follows detailed procedures pursuant to a cybersecurity playbook.
- Partners with teams across the Voya organization to ensure timely mitigation and remediation efforts.
- Identifies the threat, performs analysis to assess the impact and potential exposure to Voya and its customers, and determines the appropriate steps for resolution.
- Communicates any potential impacts of the incident to clients and business partners and provides necessary details on how it will be resolved.

PLAN | INVEST | PROTECT

VOYA® FINANCIAL

Process

- Department of Homeland Security provides us with information on domestic and international threats, which we incorporate into our security protocols.
- Part of the Financial Services Information Sharing and Analysis Center (FS-ISAC) – a government-sponsored organization that helps us stay informed of security risks.
- Monitoring of daily activities within accounts, proactively flagging potential fraudulent behaviors for investigation.
- Industry best practice policies and controls as evidenced by SOC 1 and SOC 2 certifications.

Voya's security professionals are certified by the industry's top third-party organizations

Certified Information Systems Security Professional is an independent information security certification from the International Information System Security Certification Consortium.

Certified Information Systems Auditor is the global standard for information systems audit, control and security professionals.

Certified Information Security Manager is for professionals involved in information security, assurance, risk management and governance issued by ISACA.

Certified Ethical Hacker is a qualification obtained by assessing the security of computer systems, using penetration testing techniques.

Certified Business Continuity Professionals is for professionals that have demonstrated both, knowledge and skill in the business continuity/disaster recovery industry.

Always transparent and here to help

We encourage you to reach out to your Voya representative with questions at any time. We believe in transparency — and are committed to keeping you informed of how we are safeguarding your information.

PLAN | INVEST | PROTECT