# Be cyber secure: how to build a cyber awareness program

Your employees are the first line of defense against cyber criminals. Adopting a cybersecurity awareness training program will help you create a culture of security throughout your organization, and prepare employees to detect potential threats and minimize the risk of a cyber breach.

## Develop strong internal tools and processes

### → Define roles and responsibilities

**Create** formal cybersecurity policies for digital interactions of all kinds, including the use of devices and software.

**Define** role-based guidelines for each team, including what individual members need to know about IT security, online safety and privacy.

**Build** a formal security handbook that codifies these guidelines and share it with your employees.

**Assign** employees clear security-related responsibilities in the event that cyber threats are detected, including who has decision-making authority.

### → Provide formal training

**Offer** managers step-by-step actions they can take to educate new hires while providing ongoing training for existing employees.

**Provide** employees with access to educational, training and certification programs that offer knowledge of cyber threats and hands-on experience with them.

**Refresh** employees' knowledge of industry best practices and standards every six months.

**Supplement** linear sources of education, such as books, training guides and online videos, with interactive exercises and team-based activities that test employees' skills.

### → Integrate learning opportunities

**Transform** routine cybersecurity challenges, such as phishing emails or social engineering attacks, into simulated real-world scenarios that employees can learn from.

**Offer** instructional feedback as workers tackle these challenges and help them determine the best way to address each situation.

**Quiz** employees on what they've learned, review the results and discuss where their actions could have been more effective.

**Share** the insights obtained from these exercises with the rest of the organization.

## Reinforce cyber awareness

**Plan** and schedule regular employee engagement campaigns that promote awareness of current cybersecurity trends.

**Reach** out to employees on a routine basis, weekly or monthly, to inform them about hot topics in the cybersecurity space.

**Create** a communications plan and workflow for dealing with IT security incidents and make sure your teams are familiar with it.

**Use** security issues as opportunities for employees to learn best practices.

## Establish lines of communication

**Identify** the key person(s) accountable for cybersecurity within each of your organization's departments and circulate their contact information. Do the same for each of your partners and vendors.

**Implement** official communications channels, online forums or emergency email accounts, through which employees can report cybersecurity incidents.

**Use** standardized templates for threat reports and updates to help employees share information quickly.

## To learn more

The Global Information Security (GIS) team at Bank of America is made up of information security professionals, staffing multiple security operations centers across the globe, who work 24/7 to keep data and information safe.

*Visit www.business.bofa.com/managingfraudrisk to learn how to help protect yourself and those closest to you.*

## IMPORTANT INFORMATION

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC are members of the NFA.

Investment products offered by Investment Banking Affiliates:

| Are Not FDIC Insured | Are Not Bank Guaranteed | May Lose Value |
|---|---|---|