BANK OF AMERICA

FACT SHEET

How to Build a Cyber Awareness Program

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

Here are three things you can do now that could help protect your company from the unwanted attention of cyber criminals.

Inside

1 Develop strong internal tools and processes

Define roles and responsibilities

Create formal cyber security 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 and hands-on experience with cyber threats.

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.

Cyber Security by the Numbers

$6 trillion

Estimated cost to the world from cyber crime by 2021, up from $3 trillion in 2015.

(https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf)

95%

Percentage of cyber incidents that succeed due to human error.

(https://venturebeat.com/2014/06/19/95-of-successful-security-attacks-are-the-result-of-human-error/)

Integrate learning opportunities

Transform routine cyber security 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 to determine the optimal means for addressing each encounter.

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

Share the insights gleaned from these exercises with the rest of the organization.

Reinforce cyber awareness

Plan and schedule regular employee engagement campaigns that promote awareness of current cyber security trends.

Reach out to employees on a routine basis — weekly, or monthly — to inform them about hot topics in the cyber security 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 cyber security within each of your organization's departments and circulate that person's 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 cyber security incidents.

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

Cyber Security by the Numbers

80%

Percentage of IT business leaders who anticipate a critical breach or successful cyber event.

(https://newsroom.trendmicro.com/press-release/cyberthreat/trend-micro-survey-finds-80-percent-us-businesses-expect-critical-breach-2)

43%

Percentage of all cyber incidents that are aimed at small businesses.

(https://enterprise.verizon.com/resources/20reports/2019-data-breach-investigations-report.pdf)

900

Average number of cyber crime complaints received by the FBI each day.

(https://pdf.ic3.gov/2018_IC3Report.pdf)

2 Be aware of the most current cyber threats

It is vital to be aware of the most common forms of cyber crime so you can prepare your defenses.

Malware
Malicious software designed to compromise or damage electronic devices.

Ransomware
A type of malware designed to encrypt a computer system or systems until a ransom payment is made.

Identity theft
Stealing private information to assume another person's identity.

Hacking
Unauthorized access to a digital device, computer system or network to obtain information, disrupt operations or promote malicious activity.

Phishing
The use of email from seemingly legitimate sources to elicit users to expose personal information to cyber criminals.

Social engineering
When cyber criminals pretend to be trusted individuals in order to trick users into giving out sensitive information.

Business email compromise (BEC)
When cyber criminals use business email in an effort to obtain sensitive information or perform fraudulent financial transactions.

Cyber Security by the Numbers

77%

Percentage of business leaders who admit they don't have a formal cyber security incident response plan that's applied consistently throughout their organization.

(https://www.techrepublic.com/article/report-77-of-companies-dont-have-a-consistent-cybersecurity-response-plan/)

$8.9MM

The amount of money cyber criminals gained from ransomware incidents in 2019.

(https://www.bbc.com/news/technology-51474109?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-story)

314 days

Life cycle of a malicious incident from breach to containment.

(https://databreachcalculator.mybluemix.net/?_)

3 Promote positive cyber habits

Help employees understand that good cyber security begins with them, so they should speak up and say something if they spot suspicious activity.

Stay current with industry rules, regulations and requirements, noting that professional standards and best practices can shift frequently as new technologies, tools and capabilities are introduced.

Analyze and assess possible areas of risk exposure across your networks, systems and applications (including user interactions).

Make certain to involve all areas of your business, your partners and vendors when planning your employee engagement strategy.

Review current training programs regularly to identify opportunities for improvement.

Reinforce learning and insights at multiple touchpoints to boost employee recall and awareness of cyber security topics.

Use policy violations and strategic errors as teachable moments to provide immediate instruction and insight.

Global Information Security at Bank of America

The GIS team is made up of information security professionals staffing multiple security operations centers across the globe that work 24/7 to keep data and information safe.

For more information, go to www.bankofamerica.com/privacy/overview.go