AP SAFETY TRAINING
Training Solutions, Delivered!

CYBERSECURITY

Leader's Guide, Fact Sheet & Quiz

Item Number: 5236

This easy-to-use Leader's Guide is provided to assist in conducting a successful presentation.

PREPARING FOR THE MEETING

Here are a few suggestions for using this program:

a) Review the contents of the Fact Sheet that immediately follows this page to familiarize yourself with the program topic and the training points discussed in the program. The Fact Sheet also includes a list of Program Objectives that details the information that participants should learn from watching the program.

b) If required by your organization, make an attendance record to be signed by each participant to document the training to be conducted.

c) Prepare the area and equipment to be used for the training. Make sure the watching environment is comfortable and free from outside distractions. Also, ensure that participants can see and hear the TV screen or computer monitor without obstructions.

d) Make copies of the Review Quiz included at the end of this Leader's Guide to be completed by participants at the conclusion of the presentation. Be aware that the page containing the answers to the quiz comes *before* the quiz itself, which is on the final page.

CONDUCTING THE PRESENTATION

a) Begin the meeting by welcoming the participants. Introduce yourself and give each person an opportunity to become acquainted if there are new people joining the training session.

b) Introduce the program by its title and explain to participants what they are expected to learn as stated in the Program Objectives of the Fact Sheet.

c) Play the program without interruption. Upon completion, lead discussions about your organization's specific policies regarding the subject matter. Make sure to note any unique hazards associated with the program's topic that participants may encounter while performing their job duties at your facility.

d) Hand out copies of the review quiz to all of the participants and make sure each one completes it before concluding the training session.

5236 CYBERSECURITY
FACT SHEET

LENGTH: 5 MINUTES

PROGRAM SYNOPSIS:
When your employee is at risk, your business is at risk. Organizations need to be one step ahead of the criminal wave. Americans are more worried about cybercrime than being a victim of violent crime and with good reason. Any computer connected to the internet is vulnerable and most users are not properly trained to avert cyberattacks. Hackers are becoming more sophisticated in their attempt to confiscate email accounts and employee data. This program discusses cyber defense awareness training programs, hackers, data breaches and security solutions.

PROGRAM OBJECTIVES:
After watching the program, the viewer will be able to explain the following:

- Why it is important for organizations to create a cyber defense awareness training program;
- Which issues should be addressed in your awareness program;
- How to protect your business from ransomware.

PROGRAM OUTLINE:

THE IMPORTANCE OF CYBERSECURITY

- Americans are more worried about cybercrime than being a victim of violent crime and with good reason.
- Any computer connected to the Internet is vulnerable and most users are not properly trained to avert cyberattacks.
- Hackers are becoming more sophisticated in their attempts to confiscate email accounts and employee data. When your employees are at risk, your business is at risk and organizations need to be one step ahead of a criminal way.

CREATING A CYBER DEFENSE AWARENESS TRAINING PROGRAM

- Your spam filter, firewall, IPS, SIEN, NAC, AP white listing and other security controls will not ensure complete safety. Errors in code are inevitable and they are human.
- Cyber defense is half technology and half human. An awareness program must be created to address account security and the importance of implementing strong authentication.
- In fact, many regulations and cyber insurance companies require such training. Employees need to know how to identify these attacks before they click a link or download software. It is essential to sell the importance of security to your staff.

ISSUES THAT SHOULD BE ADDRESSED BY YOUR AWARENESS PROGRAM

- Every 39 seconds there is a hacker attack and a hacker only needs one person in your company to take the bait. Given that 91 percent of data breaches start with phishing emails and scams, let's take a look at topics that should be included in your awareness training program.
- Check out the valuable guide developed by the US Chamber of Commerce Internet Essentials for Business 2.0. Use cloud-based software to keep data safe in the event of a breakdown at any one server. Instruct how to identify phishing emails and social engineering scams.
- List the impact of lost data, lost revenue, lost access to a computer network and the risk of private information being divulged.
- Check for unsecured Wi-Fi since their hotspots often lack proper encryption.
- List what websites and personal email services are available to access at work. Create a policy for mobile devices, especially when allowing BYOD.
- Change passwords every 60 days.
- Ask every employee three important questions: Does the user understand cyber security practices and corporate policy? Does the user pose a phishing risk to the organization? Does the user actively report suspicious activity?
- Monitor and ensure policies are in place and in practice. Keep in mind that sabotage can happen from within.

PROTECTING YOUR BUSINESS FROM RANSOMWARE

- One ransomware infection will consume an average of 33-man hours to resolve and is expected to cost businesses $11.5 billion in 2019.
- Equip each computer with antivirus software and antispyware. Update regularly.
- Safeguard your internet connection using a firewall and encrypting information.
- Ensure your Wi-Fi network is secure and hidden, and password protect the router.
- Require employees to use strong passwords and change often.
- Control physical access to computers (especially laptops) and network components.
- Do not use the same computer to process payments and surf the internet.
- Require users to password their devices, encrypt their data and install security apps to prevent stealing info while on public networks.
- Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

SUMMARY

- If all this seems overwhelming, you do have another option: Hire a cyber security specialist, but the most important thing is to protect your business. Start today.
- The global cost of cybercrime is expected to exceed 2 trillion this year.

CYBERSECURITY

ANSWERS TO THE REVIEW QUIZ

1. a

2. c

3. a

4. b

5. a

6. b

CYBERSECURITY
REVIEW QUIZ

Name____Date_________________________________

The following questions are provided to determine how well you understand the information presented in this program.

1. Americans are more worried about cybercrime than being a victim of violent crime

a. True
b. False

2. ________________ of data breaches start with phishing emails and scams.

a. 71 percent
b. 81 percent
c. 91 percent

3. Passwords on computers and mobile devices should be changed every __________.

a. 60 days
b. 90 days
c. 120 days

4. One ransomware infection will consume an average of ____________ to resolve.

a. 13 man-hours
b. 33 man-hours
c. 46 man-hours

5. You should NOT use the same computer to process payments and surf the internet.

a. True
b. False

6. Only checkout and sign-up pages need to be protected on your public-facing websites.

a. True
b. False