Training Solutions, Delivered!

SECURITY FOR THE REMOTE WORKER

Leader's Guide, Fact Sheet & Quiz

Item Number: 5122

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.

5122 SECURITY FOR THE REMOTE WORKER
FACT SHEET

LENGTH: 2:27 MINUTES

PROGRAM SYNOPSIS:
In today's technology driven and ever-changing world, the ability and necessity of working from home or at a remote location is on the rise. Generally referred to as "remote work", this working arrangement commonly finds workers performing their job duties from a "home office" or a "home-based worksite." There are many benefits of remote work for both the employee and employer; however, it is important that all parties understand their responsibilities related to the safety and health of remote workers as well as the cyber security of their operations. This program provides an overview of security considerations for remote workers.

Topics include personal security for remote workers, keeping computers and networks secure and avoiding email scams.

PROGRAM OBJECTIVES:
After watching the program, the participant should be able to explain the following:
- What precautions to take to maintain personal security while working remotely;
- What safeguards to follow to keep computers and networks secure;
- How to properly respond to suspicious emails.

INSTRUCTIONAL CONTENT:

PERSONAL SECURITY FOR THE REMOTE WORKER
- Security considerations for remote workers includes both personal security and computer security.
- When dealing with work-related clients, do not give out your home address or other personal information.
- Always contact your work-related clients using your business email and dedicated business phone, if you have one.
- It's a good idea to keep your exterior doors locked while you are working so no one enters your home unexpectedly.
- If your work requires off-site meetings or travel, establish a method of communication with a supervisor or co-worker so someone knows your destination and when you expect to return.
- Also, establish a protocol for checking in as "safe" when you arrive and return from off-site travel.

CYBER & COMPUTER SECURITY
- Cyber and computer security are also key considerations for remote workers.
- Your organization may have specific hardware, software and networking requirements related to cyber security for remote workers.
- Make sure you understand and follow your organization's requirements.
- If a virtual VPN is provided by your company, be sure to use it.
- A home-based network should never be open to the public. The network should be encrypted and secured with a strong password.
- Your router and computer should be updated regularly with the most current software and virus protection and also secured with a long and unique password.
- When possible, it's best to use a completely separate computer, phone and email for work-related purposes.
- Only use the hardware, software and applications approved and vetted by your organization.
- Do not download or install any programs or applications onto your computer or devices without prior approval from your organization.
- Always be alert for scam emails that purport to need personal information or ask you to open or download a file or document.
- Many scammers try to fool you into thinking an email is from your bank, the IRS, the police or similar entities. This type of nefarious cyber activity is called "phishing."
- If in doubt, don't open any suspect email or follow any links to an unfamiliar website. Instead, call the sending organization by phone to confirm if they have sent you an important email or requested information.
- When it comes to security, remote workers must stay alert, be responsible and follow all applicable cyber safety procedures.

ANSWERS TO THE REVIEW QUIZ

1. a
2. a
3. b

SECURITY FOR THE REMOTE WORKER
REVIEW QUIZ

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

Name_____Date_____

1. When dealing with work-related clients, you should NOT give out your home address or other personal information.

a. True
b. False

2. A home-based computer network should never be open to the public.

a. True
b. False

3. If you receive a suspicious email, you should follow any links you find inside it to try to find out the email's origin.

a. True
b. False