LOSS PREVENTION

PROTECT YOUR PASSWORDS

In our roles, we use a variety of passwords for different systems. In the hands of a bad actor, these passwords can allow someone with malicious intent to access information that is confidential and proprietary to the company.

Visit us at
www.bspk.com
@bspksf

BSPK

BSPK

How to use Weekly Meeting Topic Guides

What are the Weekly Meeting Topic guides?: One-page topic guides to help managers educate their sales team on sales growth topics and strategies.

Goal: BSPK morning meetings are designed for one simple purpose:
to modify behaviors in order to achieve a desired result.

Weekly Topic: The meeting is intended to be delivered daily for an entire week in order to ensure that all team members have fully absorbed the content before moving on to the next topic.

Sections: BSPK morning meetings are divided into 4 easy steps.

- Introduction
- Questions for the team
- Teach the topic
- Set the expectation

Meeting time: A morning meeting should be no longer than 15-20 minutes.

Best practices:

- Review the content before your morning meeting
- Deliver the meeting in your own voice without reading verbatim from the meeting notes
- Use the guide as a reference but always make eye contact with your team
- After the meeting, be present on the sales floor and be prepared to provide in-the-moment coaching where needed

Weekly Meeting Topic
Protect Your Passwords

Confidential

Step 1 Introduction

Good morning, team. Today we are going to discuss how to keep your passwords safe. In our roles, we use a variety of passwords for different systems. In the hands of a bad actor, these passwords can allow someone with malicious intent to access information that is confidential and proprietary to the company.

Step 2 Questions for the team

- What are some of the systems that you access with a password?
- What would be the consequences for the company if these systems were compromised?

Step 3 Teach the topic

Let's discuss some best practices for password safety.

Use a strong password: When choosing a password, use a combination of upper case and lower case characters, numbers and special symbols. Avoid easily guessable words in your password such as the company name, street names, family names or pet names. Instead, choose something that you can remember but nobody else would be able to guess.

Use different passwords: Don't use the same password for everything. In the event that one of your passwords are compromised, this limits the scope of a potential breach. If you ever suspect that one of your passwords has been exposed, change it immediately and inform the IT department right away.

Never Share Passwords: Never share your passwords with anyone, including your manager. Passwords are personal and are intended to be used only by the individual user. Nobody in our company should ever ask for your password so if you ever receive a call or email from someone asking for your password, report it right away to the IT department.

Beware of Phishing: When entering your passwords, always verify the website address. Sometimes a website may look real but it may actually be a fake website disguised to steal your information.

Are there any questions?

Step 4 Set the expectation (this is how you can say it)

This week we are placing a focus on password security. Please remember these important tips to help safeguard our company and its resources. We rely on each of you to do your part. Thank you all for your attention and diligence.