LOSS PREVENTION

PHISHING

Phishing is a deceptive tactic used by cybercriminals to trick people into divulging sensitive information. These attacks involve fraudulent emails that often appear legitimate but are designed to trick you intro sharing login credentials or personal information.

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
Phishing

Confidential

Step 1 Introduction

Good morning, team. This week we're going to delve into a crucial topic that concerns the security of our organization: phishing. We will discuss how to recognize and respond to phishing attempts, enhancing our collective defense against these threats.

Step 2 Questions for the team

- Who can tell me what phishing is?
- Have you encountered any suspicious emails recently? If so, how did you handle them?

Step 3 Teach the topic

Phishing is a deceptive tactic used by cybercriminals to trick people into divulging sensitive information. These attacks involve fraudulent emails that often appear legitimate but are designed to trick you intro sharing login credentials or personal information.

Here are some key points to consider when identifying phishing attempts:

- **Sender's Email Address**: Pay attention to the sender's email address, especially if it looks suspicious or unfamiliar. Often times the domain name will be a mis-spelling of an authentic domain.
- **Urgency and Threats**: Phishing emails often create a sense of urgency or include threats to prompt immediate action.
- **Links and Attachments**: Be cautious of links or attachments in emails, especially from unknown sources, as they may contain malware or lead to phishing websites.
- **Spelling and Grammar:** Phishing emails often contain spelling or grammatical errors, which can indicate their illegitimacy.
- **Request for Personal Information:** Be wary of emails requesting sensitive information such as passwords, account numbers, or Social Security numbers.

It's essential to report any suspicious emails or messages to our IT department immediately. Remember, our vigilance plays a crucial role in safeguarding our organization's data and systems from cyber threats.

Are there any questions?

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

Moving forward, I encourage everyone to remain vigilant and proactive in identifying and reporting phishing attempts. We will continue to provide resources and training to enhance our cybersecurity posture and protect our organization's assets. Together, we can effectively combat phishing threats and ensure the security of our data and systems.