Shield Your Organization from Quishing:
A Step-by-Step Guide to Using Keepnet Labs' Quishing Simulator

Introduction to Quishing

Quishing is a type of phishing attack that involves the use of QR codes to trick individuals into revealing their personal information or downloading malicious software.
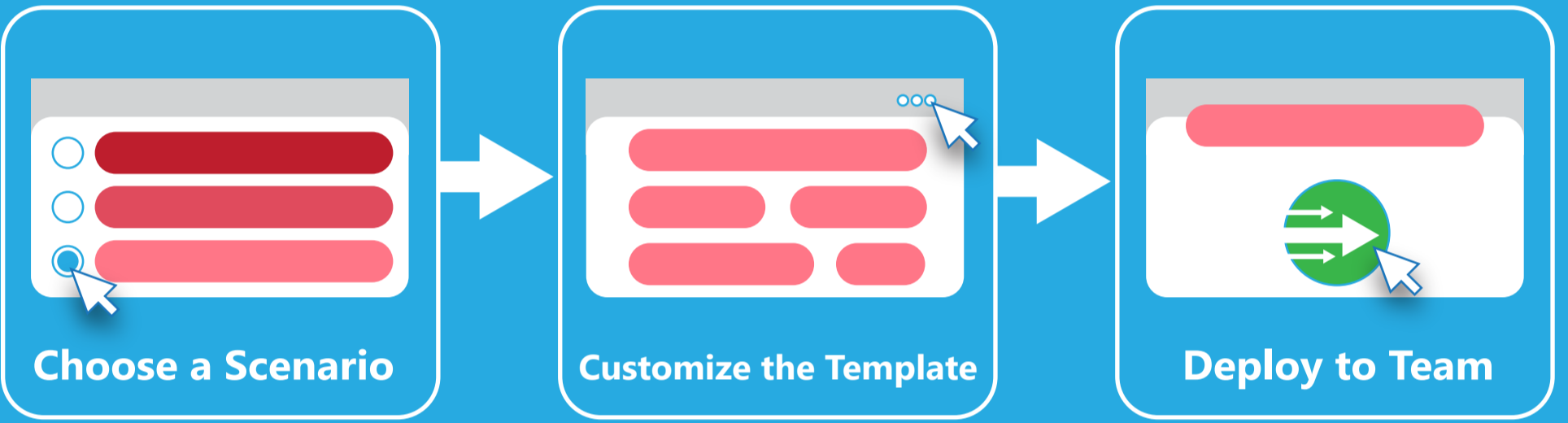
How Quishing Attacks Work

Scan → **Deceptive Link** → **Phishing Site**

WWW

Introducing the Quishing Simulator

Meet Keepnet Labs' Quishing Simulator: Your Training Tool Against QR Code Phishing.

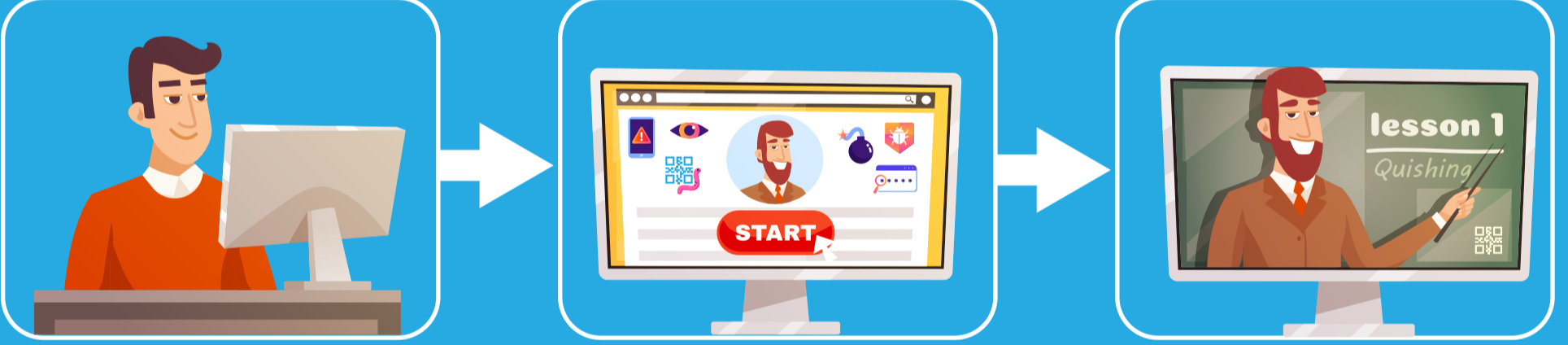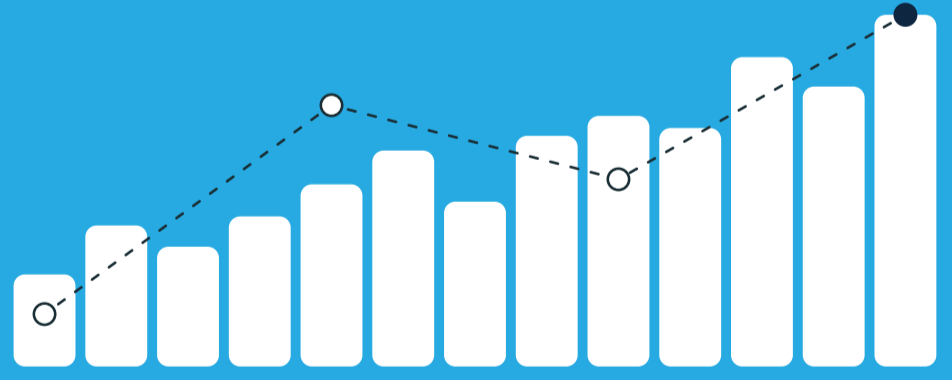## Setting Up the Simulator

Choose a Scenario → **Customize the Template** → **Deploy to Team**

Engaging in Simulations

Interactive, Real-World Scenarios for Enhanced Learning
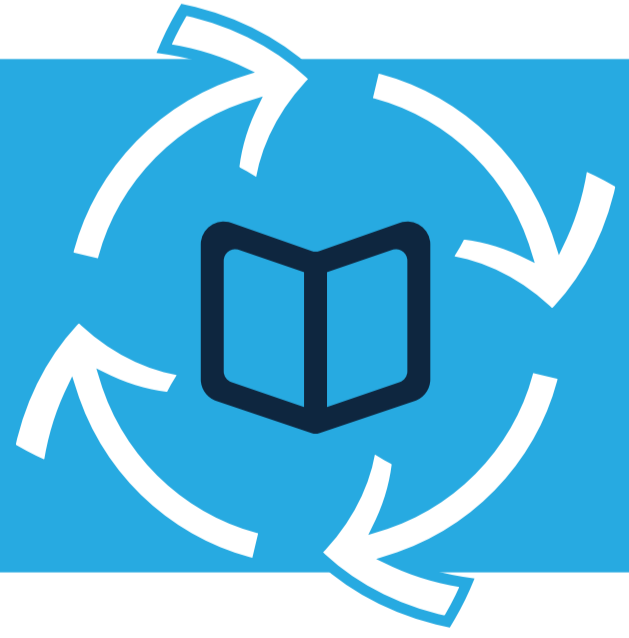
lesson 1 Quishing

Analyzing Results

Track Progress and Assign Behavior-Based Training Content Based on Incorrect Behavior

Increase employees' reporting capability up to 90% success in 6 months

Continuous Learning

Regular Updates & Repeat Simulations for Ongoing Vigilance

Request a Demo

You'll learn how:

- Create sophisticated Quishing campaigns to boost your employees' skills in identifying and responding to real threats.
- Customize Quishing templates quickly and localize these to your business needs to raise employee awareness.
- Track incorrect user behaviors and generate a human risk score to benchmark your business in your industry.