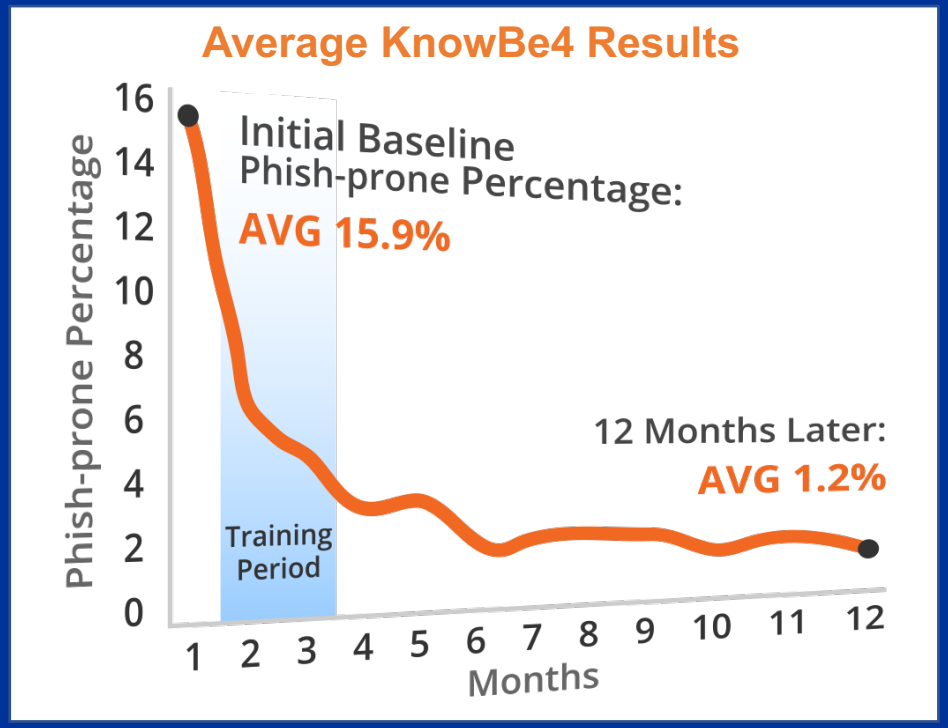
KB4-CON

# Best Practices for Developing a Security Awareness Program

by Jasmine Rodriguez, CEH, SSCP, Managed Services Engineer

KnowBe4




# About Managed Services

- Extension of your own cybersecurity team
- Comprised of cybersecurity professionals
- Technical product and program experts
- Participate in security awareness team meetings
- Implement and monitor security awareness plans
- Design and deliver spear phishing emails
- Create tailored recommendations
- Deliver customized ROI reports and metrics
- Provide personal product training to admins
- Goal is to reduce phish-prone percentage and risk

# Topic Overview

- Preparation for your Security Awareness Plan
- Creating your Security Awareness Plan
- Implementation Steps – Baseline Test, Phishing, and Training
- Monitoring your progress and ROI report selection

# Security Awareness Plan- Tips for Preparation

- Engage stakeholders/ departmental leaders
- Research training compliance requirements
- Identification of any specific user language needs
- Identification of key expected reporting metrics
- Review user directory information and complete user import
- Complete whitelisting for successful phishing security tests

# Security Awareness Plan – Elements

Baseline Test

- Email Template
- Landing Page

Mandatory Training

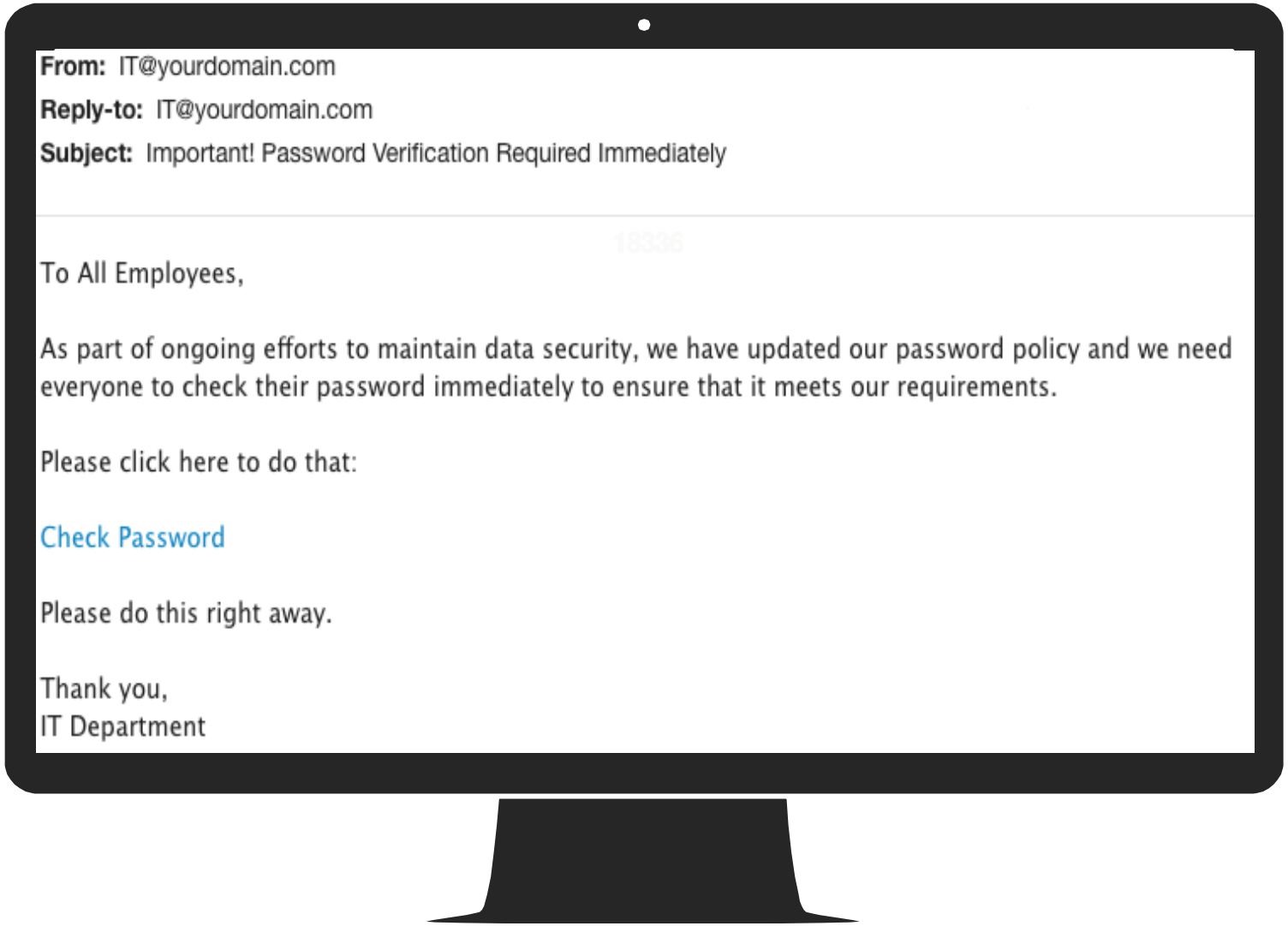
- Annual/ New Hire Training
- Scam of the Week
- Supplemental Training

Phishing and Remedial Training

- Automatic Phishing Sequence
- Remedial Training Content

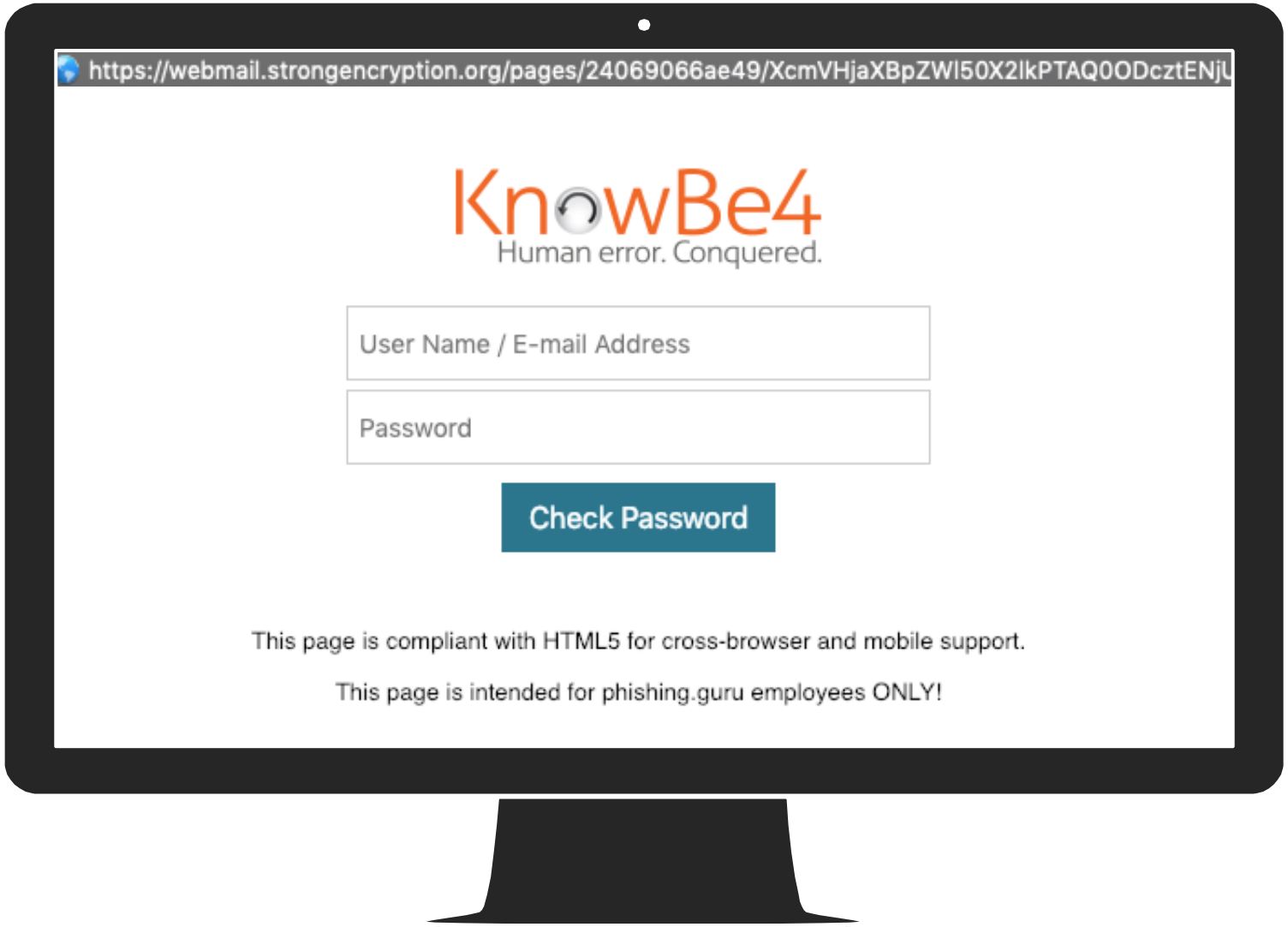
# Baseline Test – Email Template

- First phishing test for all users
- Select a generic email
- Same email to everyone
- Emails sent at the same time
- Medium difficulty email
- Results provide baseline data



# Baseline Test – Landing Page

- Displays to user after they click
- Appears as a webpage
- Functional login page
- Login is second failure
- Any data entry is not stored
- Data entry timestamp reported



# Security Awareness Mandatory Training Overview

It is best practice to assign users the following items as part of security awareness training:

- Annual training for all users utilizing module covering all aspects of security awareness
- Weekly branded & customizable Scam of The Week emails to all users
- Monthly mini-modules, videos or games
- Refresher training for users that fail phishing tests

# Security Awareness – Annual Training

**2019 Kevin Mitnick Security Awareness Training – 45 Min**

This fully interactive course takes you through four modules. Learn from real-world scenarios showing you strategies and techniques hackers use to take control of your organization.


**Security Awareness Fundamentals – 23 minutes**

A completely new version of our flagship course, this gives users a solid overview of the most important issues they will face with security awareness.

# Scam of the Week Emails

- Branded with your logo
- Sent on a weekly basis
- Educational Tips
- Customizable verbiage
- Updated weekly

KnowBe4
Human error. Conquered.

## KnowBe4 Scam of the Week: Break the Chain: Don't Fall for Viral Facebook Messages

Don't be fooled! The bad guys are on social media and you need to be alert. Their latest trick involves misinformation and panic.

It all starts when you receive a message from a Facebook "friend". This friend claims they received another friend request from you. Then, they go on to explain that you've been hacked and offer you advice on how you should handle it.

This is a hoax - your account was not hacked! This is a chain letter being used to spread misinformation. In a real profile cloning attack, the bad guy will steal your Facebook profile picture and name. Then, request people you know to gather information.

To stay clear of these attacks, always make sure to verify the person sending you a friend request before you become friends!

***Stop, Look, and Think.*** *Don't be fooled.*
*The KnowBe4 Security Team*
*KnowBe4.com*

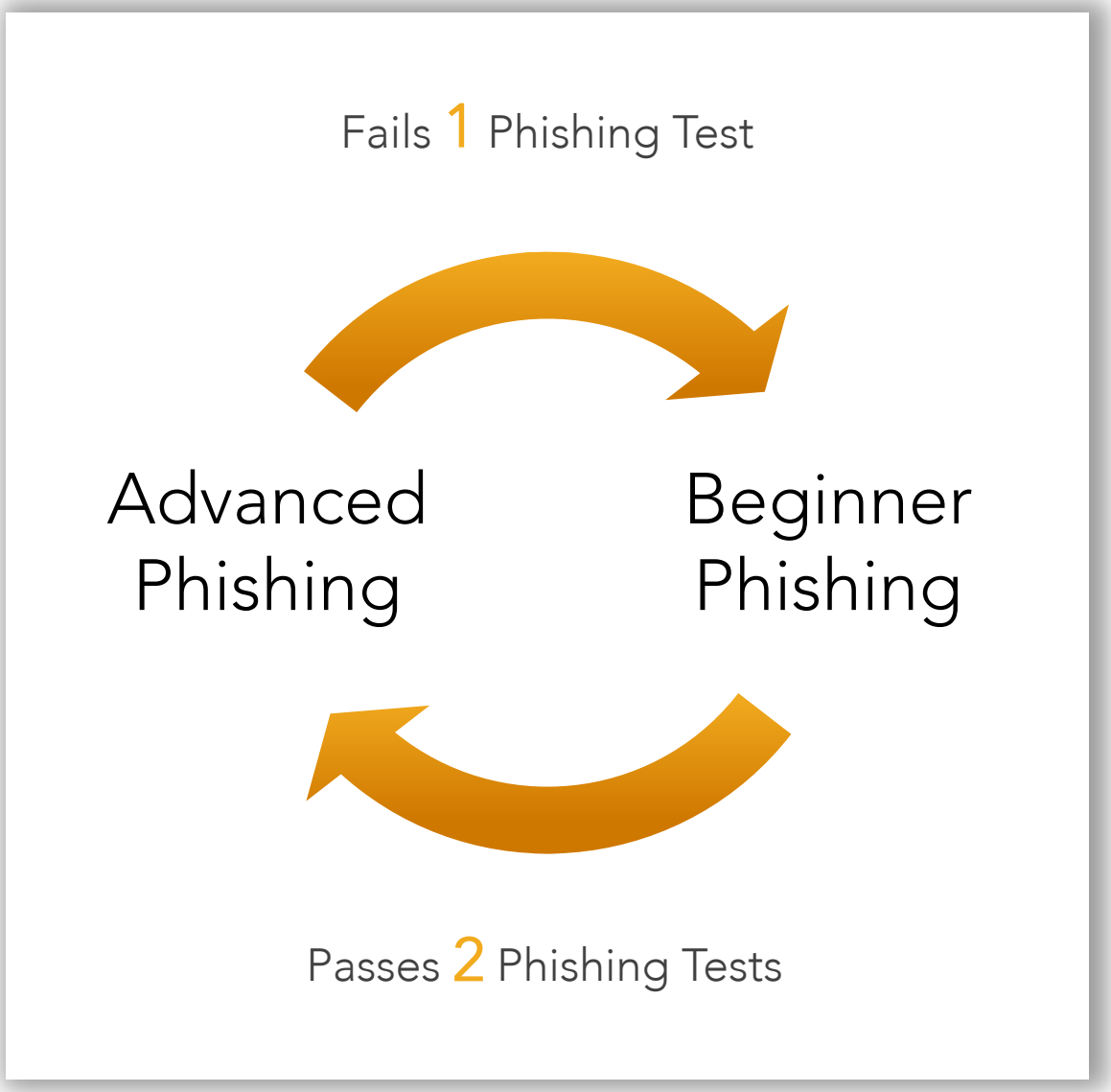
# Dynamic Phishing – Sequence Overview

Advanced

- All users start in this group
- One email per month
- More difficult emails

Beginner

- Users who fail tests move to this group
- Two easier emails per month
- Pass two tests to return to Advanced

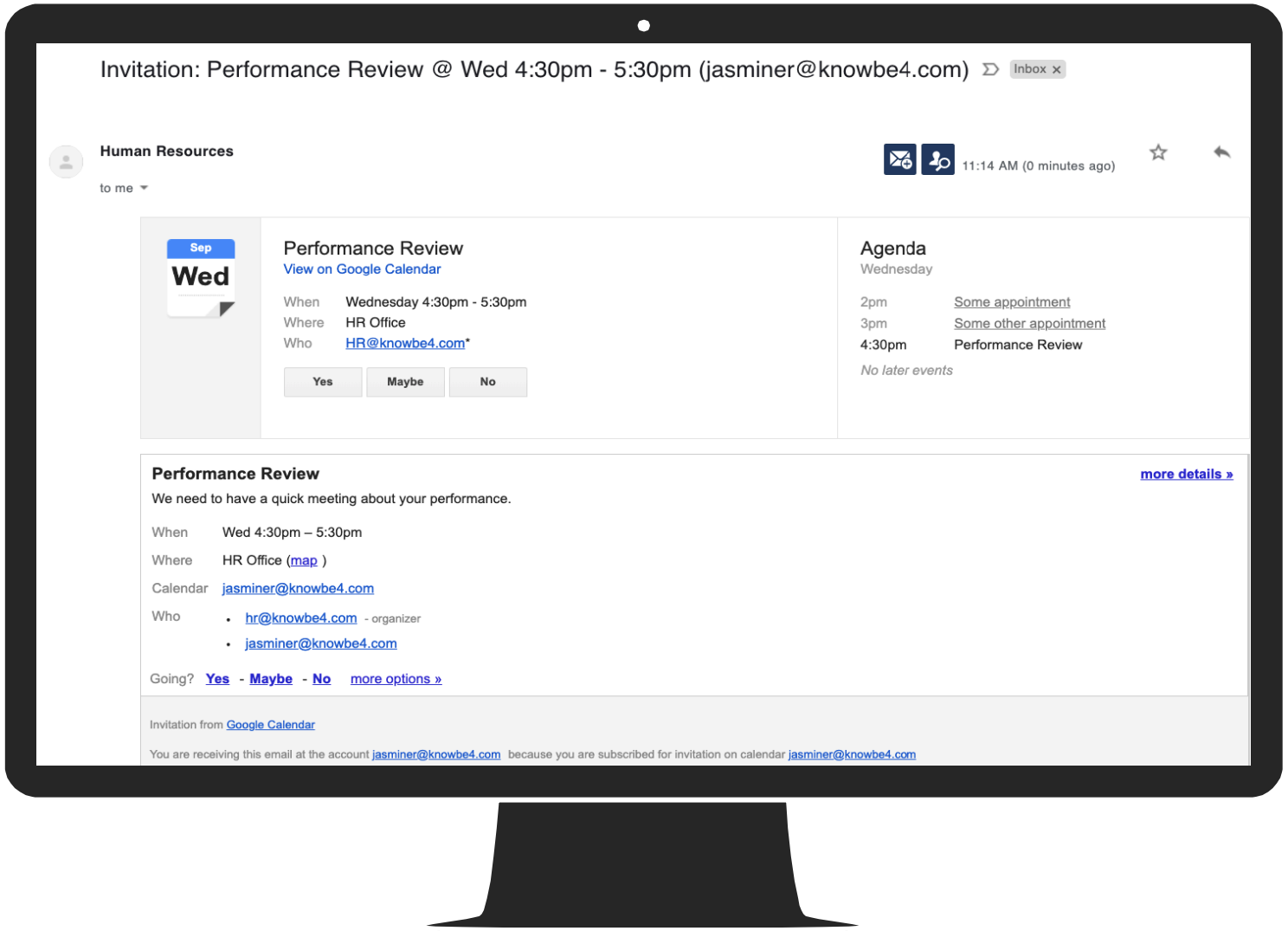


# Dynamic Phishing – Difficulty Rating

- Library of 3000+ email templates available
- Emails are organized in topical categories
- Each email is assigned a difficulty star rating
- Choose emails by star rating
- May modify difficulty rating in custom emails

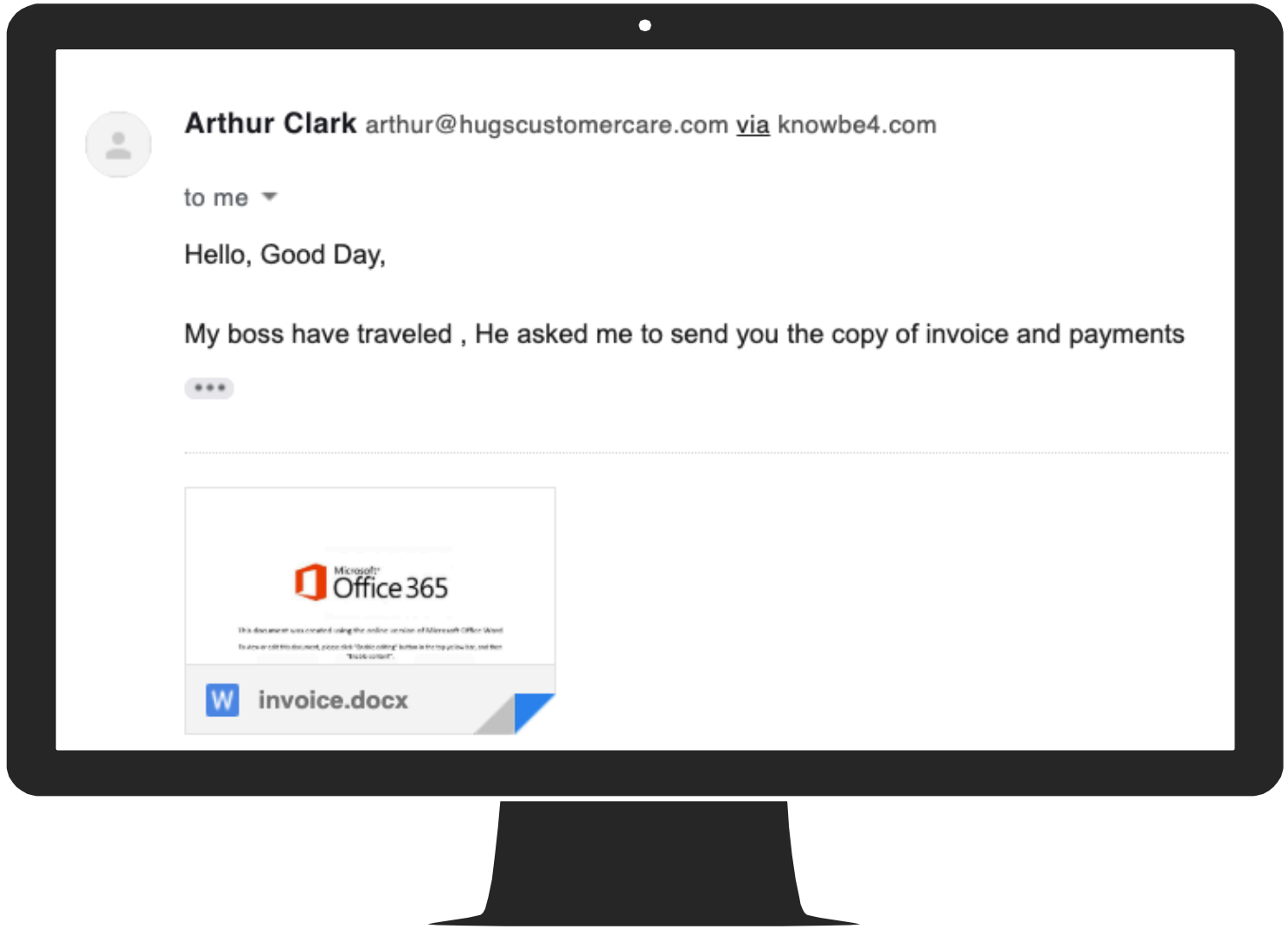
# Dynamic Phishing – 5 Star Email

- Appears authentic
- Very few red flags
- May spoof internal domain
- May be personalized



# Dynamic Phishing – 1 Star Email

- Many red flags
- May have spelling errors
- Not authentic looking
- Not personalized

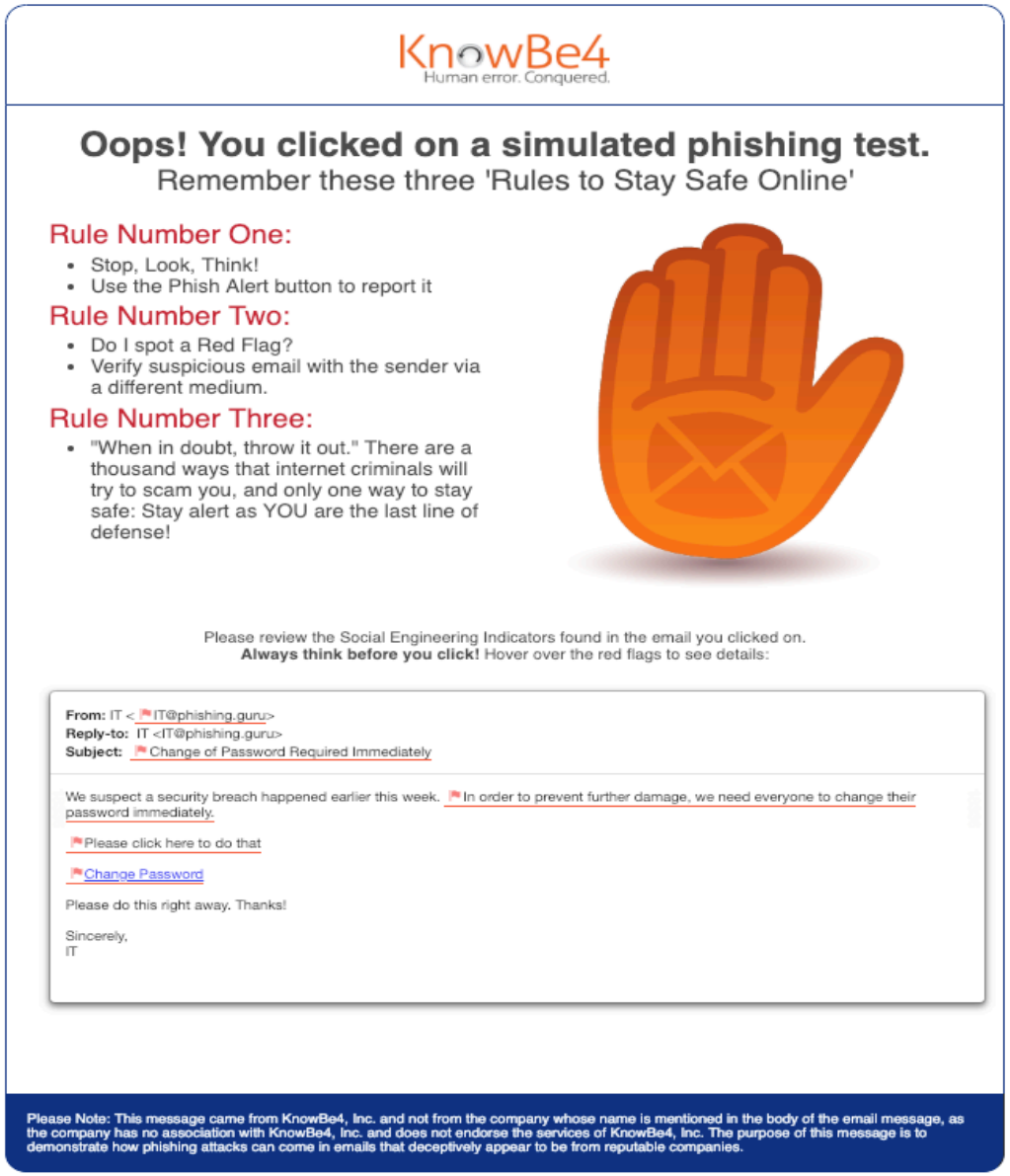


# Dynamic Phishing – Smart Groups

- Smart groups are dynamic
- Users are auto-assigned to groups based on filters
- You can filter users by their phishing test failures
- Create Advanced and Beginner Smart Groups
- Set up phishing emails to deliver to these groups

# Dynamic Phishing – Landing Page

- Social Engineering Indicators (SEI) Page
- Shows users the red flags they missed
- Provides immediate feedback and training
- Works with any email
- Customizable with your logo and colors



# Dynamic Phishing – Monitoring

- Start with Phase I categories
- Monitor failure rate
- Keep challenging users
- Introduce Phase II and III

| Phase I | Phase II | Phase III |
|---|---|---|
| Banking | Phase I | Phase I, II |
| Online Services | Business | Human Resources |
| Outdoor Sporting Goods | Current Events | IT |
| Social Networking | Holiday | Legal |
| | Mail Notifications | Healthcare |
| | | Real Estate |

# Security Awareness—Remedial Training

### Social Engineering Red Flags – 8 min

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. You'll learn how to spot red flags that alert you to possible danger in an email and then you'll help Jake Sanders, a typical computer user, steer clear of six real-world social engineering attacks.


### Phishing Fundamentals– 12 min

This module focuses on the fundamentals of phishing, including real-life examples of how it works, how it's different from spam, and what organizations can do to defend against all forms of attacks.

# Security Awareness – Supplemental Training

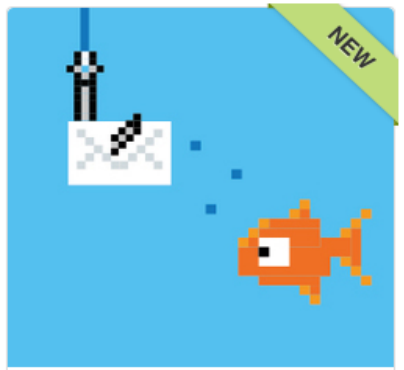
Training material formats available:

<u>Time and Progress Tracked</u>

- Modules- Quiz included
- Games- Interactive
- Videos

<u>Downloads Available</u>

- Videos
- Posters
- Newsletters




Spot the Phish Game

IT Security in the Workplace



Privacy Edition: Ep 3 - Once More Unto the Breach (Retention & Disposal)

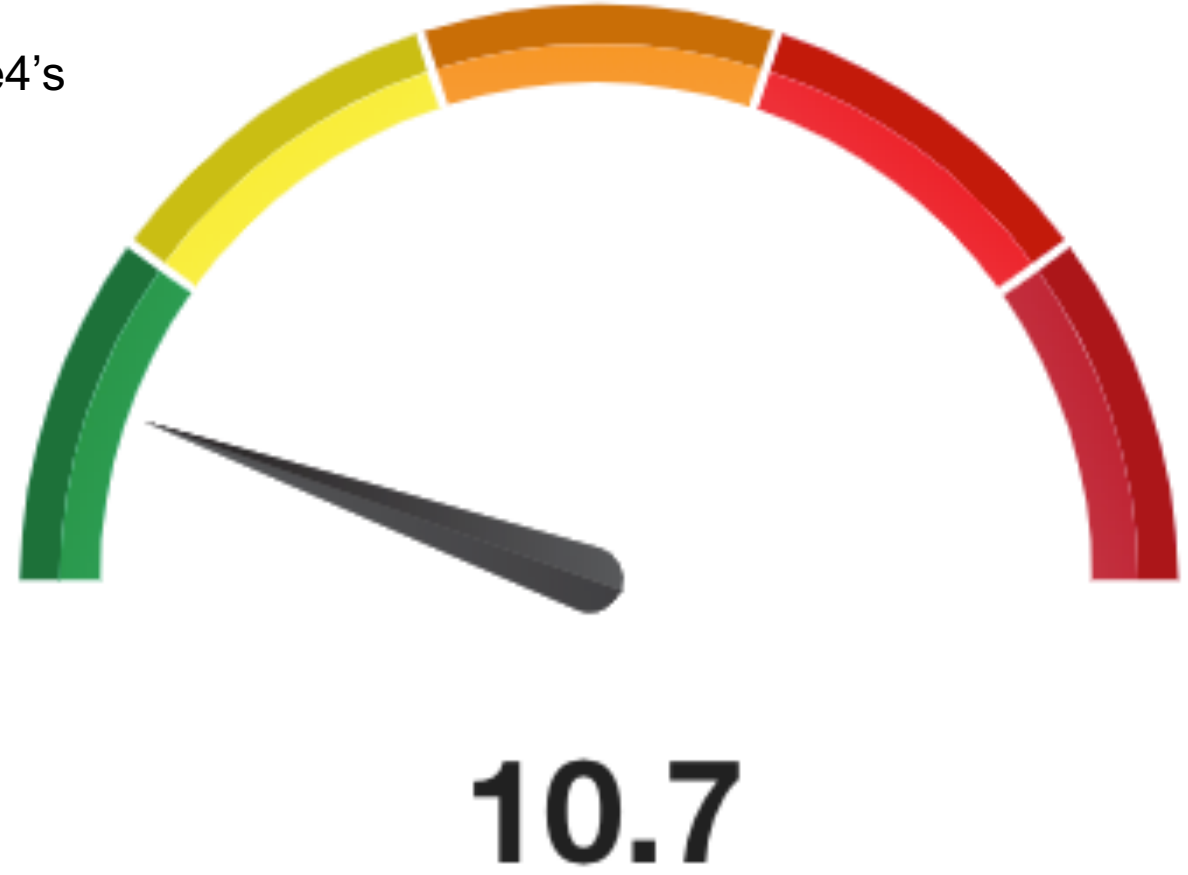

Privileged User Security Series: Secure Windows Administration


Building Secure Software Series: Ep 1 - Very Early and Often

# Showing ROI – Risk Scores

Risk scores will be generated using KnowBe4's Virtual Risk Officer from these factors:

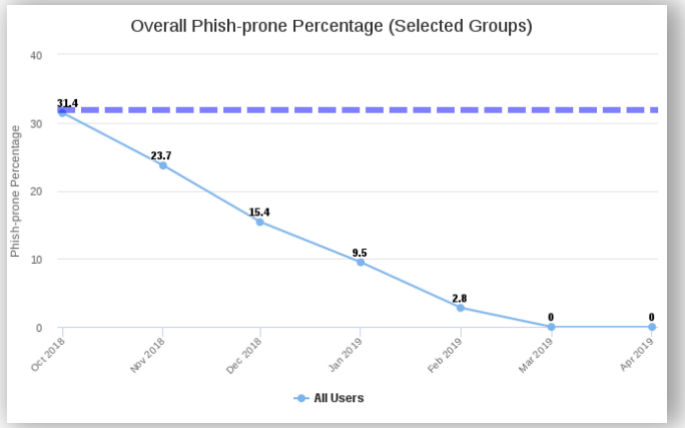
- Phish-prone Percentage
- Training Status
- Breach Data
- Job Title Related Risk
- Manual Boosters



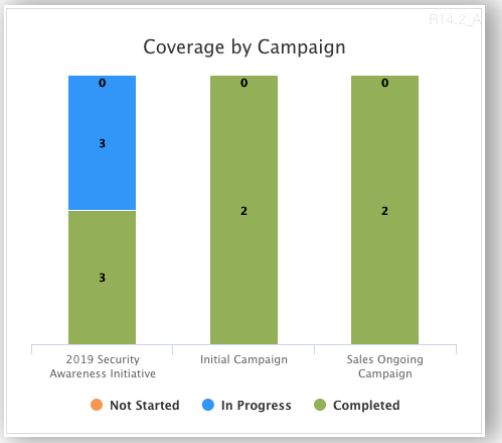
# Reviewing Analytics – Advanced Reports

- Over 60 styles of reports available
- Instant results
- Enterprise Level metrics
- Track progress over time
- Identify areas for improvement
- Create reports for any group
- Find reports by keyword search
- CSV and PDF downloads

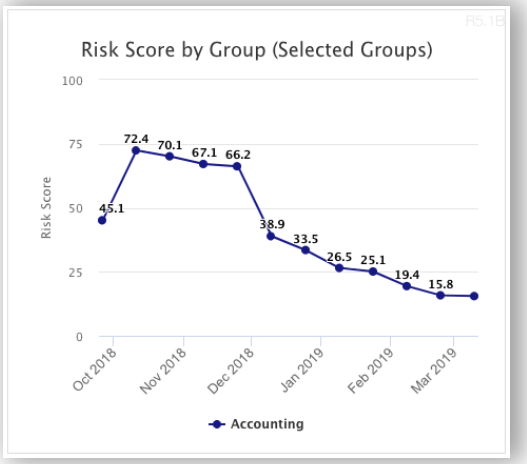
## Phish-Prone Percentage



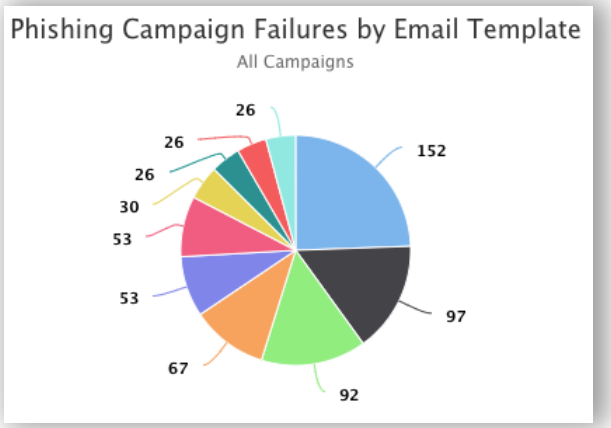

## Training Coverage




## Risk Score




## Failure Types



# Security Awareness Program – Development Summary

**Preparation**

Engage stakeholders

Gather information

Whitelisting

**Plan Creation**

Baseline Test

Training Content

Phishing Sequence

**Implementation**

Group Set Up

Campaign Set Up

**Monitoring/Reporting**

Campaign Updates

ROI Metric Review

# Thank You!

Jasmine Rodriguez, Managed Services Engineer

KnowBe4