KnowBe4
Human error. Conquered.

Phishing and Social Engineering in 2018: Is the Worst Yet to Come?

Stu Sjouwerman
Founder and CEO
KnowBe4, Inc.

Stu Sjouwerman

Founder and CEO, KnowBe4, Inc.

KnowBe4
Human error. Conquered.

About Stu

- Serial Entrepreneur, this is my fifth startup.
- Founded KnowBe4 after building an antivirus platform from scratch (VIPRE)
- We have 350 employees now, expected to be at 500 end of 2018
- Decades-long experience in creating system admin and security tools for IT professionals

About KnowBe4

- The world's most popular integrated new-school Security Awareness Training and Simulated Phishing platform, over 14,000 customers worldwide
- Founded in 2010
- Our mission is to train your employees to make smarter security decision so you can create a human firewall as an effective last line of defense when all security software fails…

Which it will

KnowBe4
Human error. Conquered.

Agenda

- Understanding the current threat landscape
- What scary new threats and innovations of ransomware, phishing and social engineering will be on the rise for 2018?
- What you can do to make your organization a harder target for cybercrime
- How to create your “human firewall”

Agenda

- Understanding the current threat landscape
- What scary new threats and innovations of ransomware, phishing and social engineering will be on the rise for 2018?
- What you can do to make your organization a harder target for cybercrime
- How to create your "human firewall"

Understanding the current threat landscape

“Everybody has a plan until they get punched in the mouth.”

- Mike Tyson

98% of Attacks Rely on Social Engineering

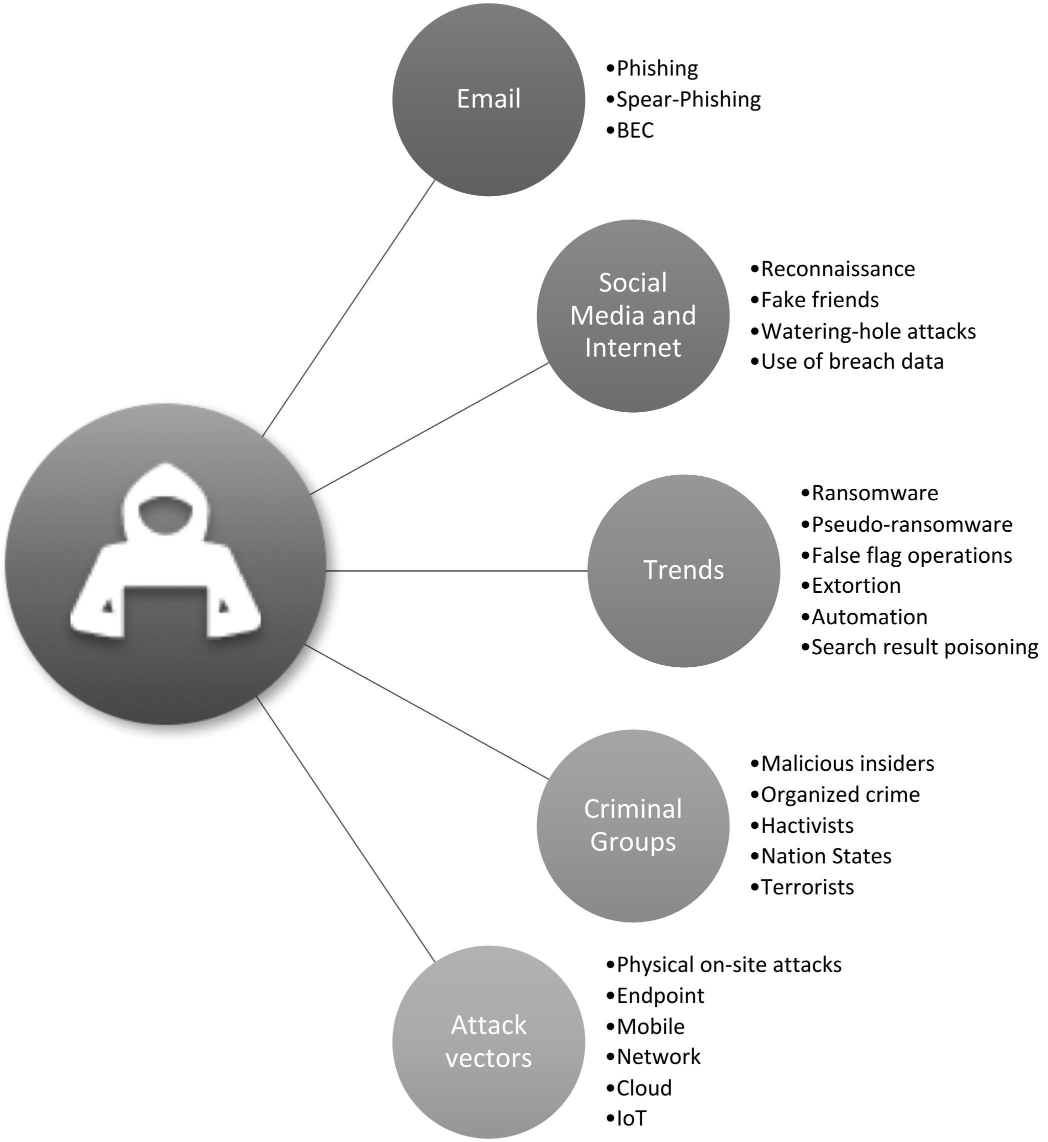
Attackers go for the low-hanging fruit:

humans

KnowBe4
Human error. Conquered.

98% of Attacks Rely on Social Engineering

Attackers go for the low-hanging fruit: *humans*



Email

- Phishing
- Spear-Phishing
- BEC

Social Media and Internet

- Reconnaissance
- Fake friends
- Watering-hole attacks
- Use of breach data

Trends

- Ransomware
- Pseudo-ransomware
- False flag operations
- Extortion
- Automation
- Search result poisoning

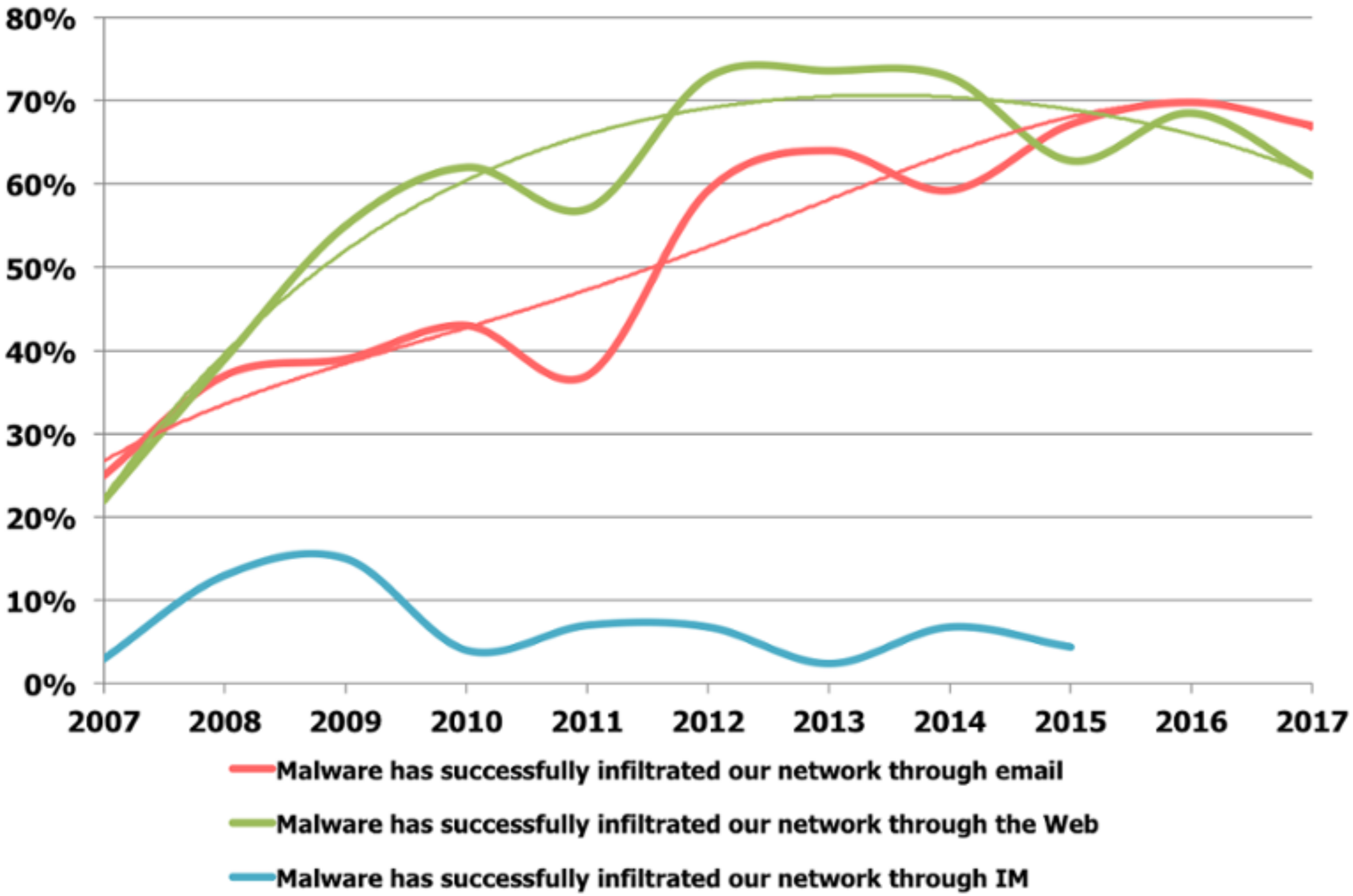
Criminal Groups

- Malicious insiders
- Organized crime
- Hactivists
- Nation States
- Terrorists

Attack vectors

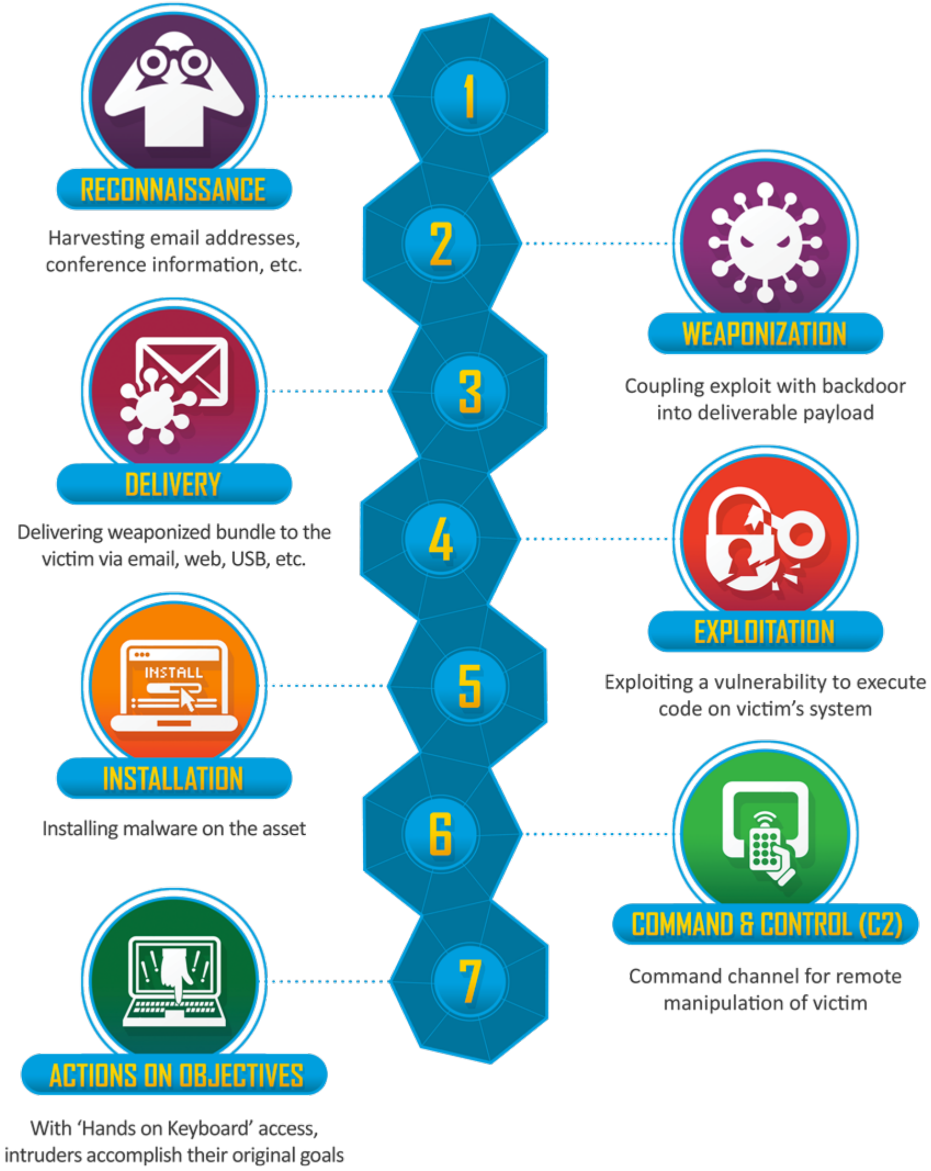
- Physical on-site attacks
- Endpoint
- Mobile
- Network
- Cloud
- IoT

Understanding the current threat landscape



the Cyber Kill Chain

Attackers generally follow these steps to compromise an organization



1. RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2. WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3. DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4. EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5. INSTALLATION
Installing malware on the asset

6. COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7. ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

KnowBe4
Human error. Conquered.

Agenda

- Understanding the current threat landscape
- What scary new threats and innovations of ransomware, phishing and social engineering will be on the rise for 2018?
- What you can do to make your organization a harder target for cybercrime
- How to create your “human firewall”

“Scary New Threat” No.1

Exponential growth of the ransomware plague, especially the “as-a-service” strains

“Scary New Threat” No.2

Hybrid pseudo-ransomware attacks will be used to distract organizations

“Scary New Threat” No.3

Automation makes detecting attacks harder

“Scary New Threat” No.4

Extortion scams will have a long tail

“Scary New Threat” No.5

Increased search result tampering will drive users to compromised websites

“Scary New Threat” No.6

New families of mobile malware will surface with powerful new features to steal creds for account takeover

“Scary New Threat” No.7

Blame-ware and “False Flag” operations will increase

“Scary New Threat” TECH BONUS

- Bitcoin wallet-attacks on user machines
- Backdooring devices via flashing firmware
- More SIM swap attacks to bypass 2FA
- IoT botnets that instead of creating havoc are out for financial gain
- First criminal use of Blockchain other than BitCoin
- A third of attacks over the next two years will target shadow IT resources and BYOD
- Cyber insurance policies will *still* not cover human error unless you specifically ask for it
- “Evil Twin” wi-fi spoofing mutates into spoofing actual cell towers!

“Scary New Threat” Wild-Ass Guesses

1. A new crypto-mining worm using NSA code will spread and steal CPU-cycles
2. A new sophisticated Fraud-as-a-Service forces FI’s to get omni-channel fraud prevention
3. A super popular system admin tool gets compromised with a backdoor
4. A brand of smart glasses gets pwned, broadcasting everything
5. A major home automation service will get hacked and millions of unwanted products are ordered
6. An explosion of skimmers on gas pumps will force smartphone payments
7. A brand-new super-exploit kit will contain dozens of 0-day vulns stolen from the NSA
8. Massive movement away from traditional antivirus toward both AI or *none at all* and rely on Win Defender

Agenda

- Understanding the current threat landscape
- What scary new threats and innovations of ransomware, phishing and social engineering will be on the rise for 2018?
- What you can do to make your organization a harder target for cybercrime
- How to create your “human firewall”

8 Points to Be A Hard Target

1. With any ransomware infection, nuke from orbit and re-image from bare metal
2. Get Secure Email- and Web Gateways that cover URL filtering and make sure they are tuned correctly
3. Make sure your endpoints are patched religiously, OS *and* 3rd Party Apps
4. Make sure your endpoints have next-gen, frequently updated security layers, but don’t rely on them
5. Identify users that handle sensitive information and enforce 2FA
6. Review your internal security Policies and Procedures, specifically related to financial transactions to prevent CEO Fraud
7. Check your firewall configuration and make sure no criminal network traffic is allowed out to C&C servers
8. Leverage new-school security awareness training, which includes frequent social engineering test using multiple channels, not just email

Agenda

- Understanding the current threat landscape
- What scary new threats and innovations of ransomware, phishing and social engineering will be on the rise for 2018?
- What you can do to make your organization a harder target for cybercrime
- How to create your “human firewall”

Your Employees Are Your Last Line Of Defense

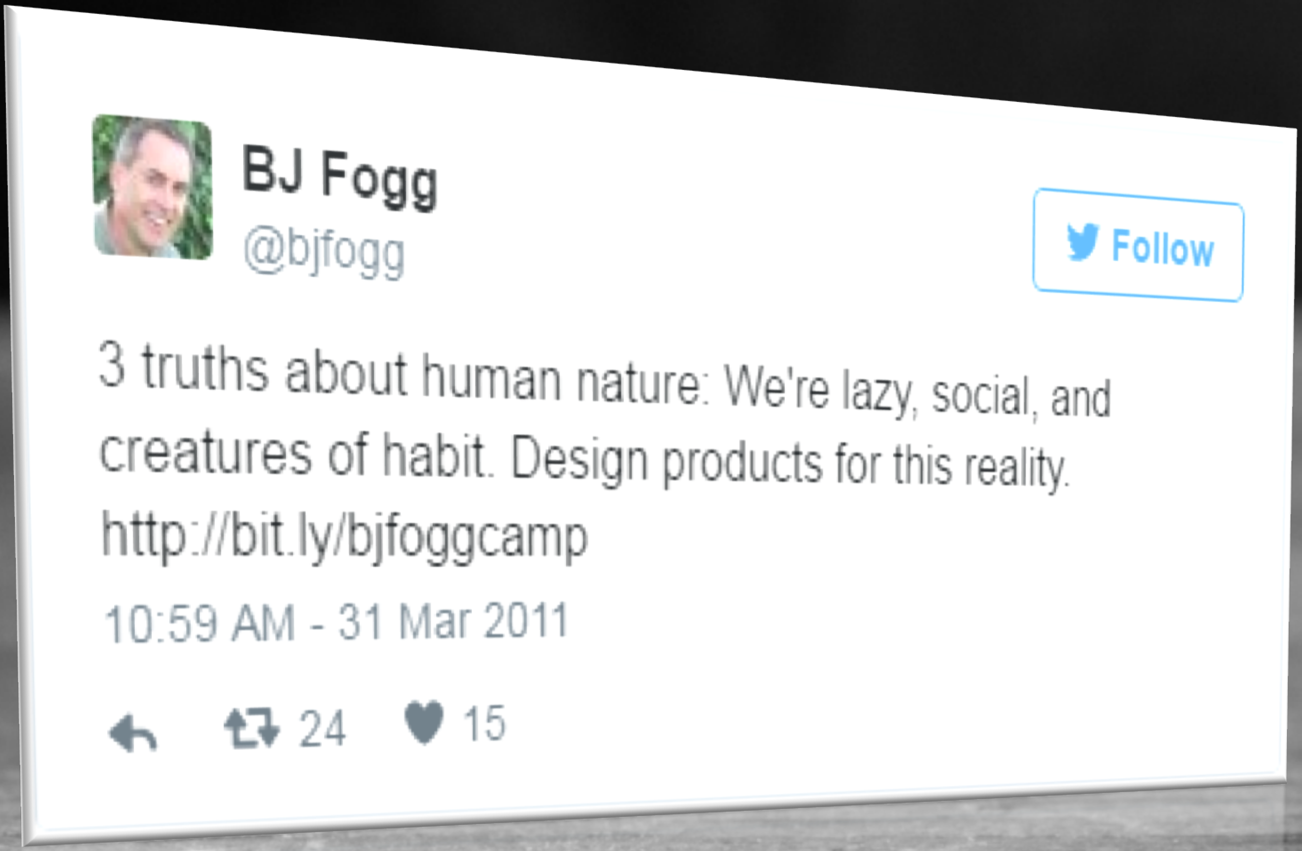
91%

of successful data breaches started with a spear phishing attack

Source: Trend Micro

- **91%** of successful data breaches started with a spear phishing attack
- **CEO Fraud** (aka Business Email Compromise) causes $5.3 billion in damages yearly
- **W-2 Scams** social engineer Accounting/HR to send tax forms to the bad guys
- **Ransomware** is a 1 Billion+ dollar criminal business in 2017, and continues to grow exponentially

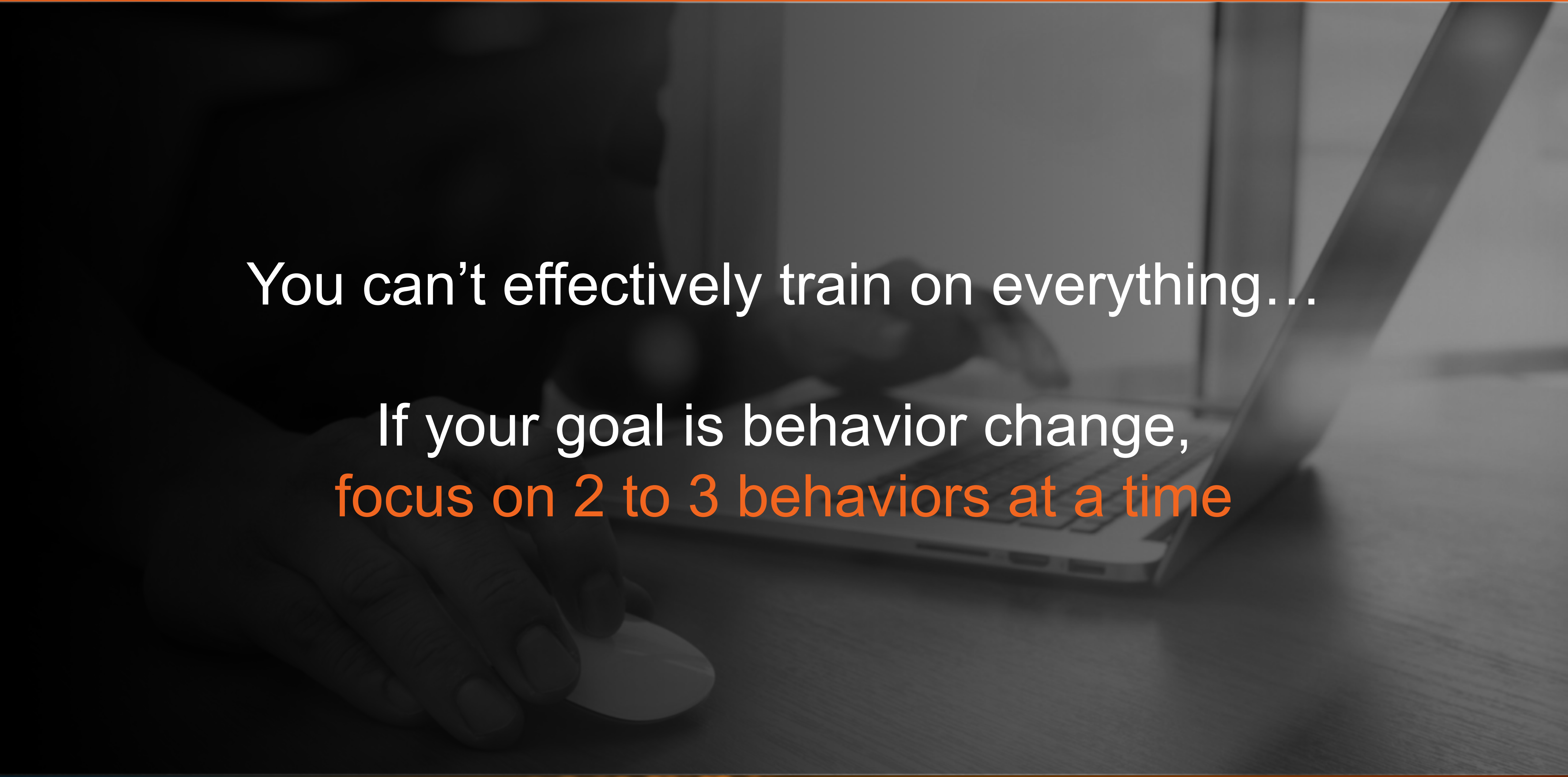
Why Is Getting the Desired Behaviors So Difficult?



BJ Fogg
@bjfogg

3 truths about human nature: We're lazy, social, and creatures of habit. Design products for this reality. http://bit.ly/bjfoggcamp

10:59 AM - 31 Mar 2011



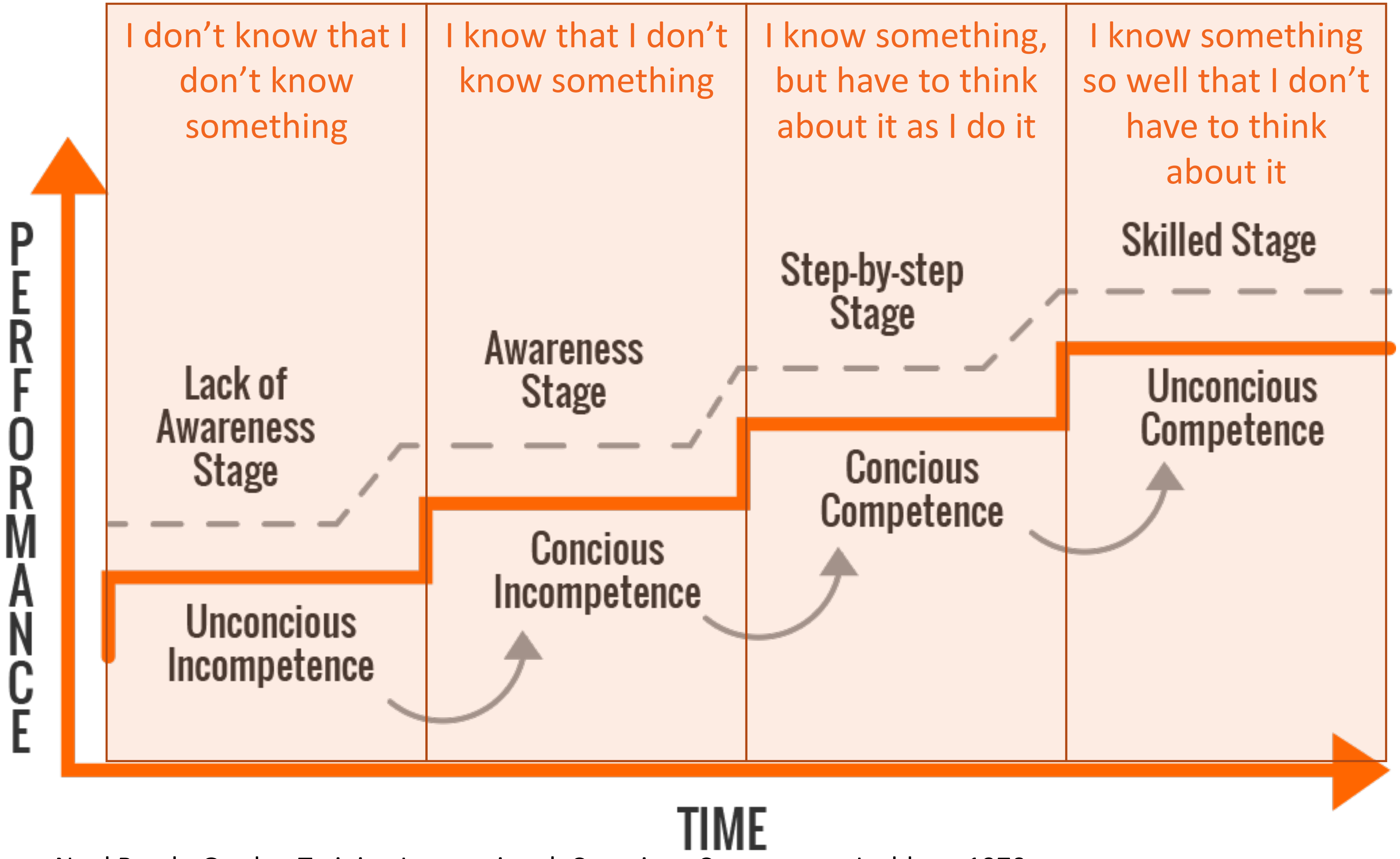
You can't effectively train on everything…

If your goal is behavior change,
focus on 2 to 3 behaviors at a time

-- a sobering truth --

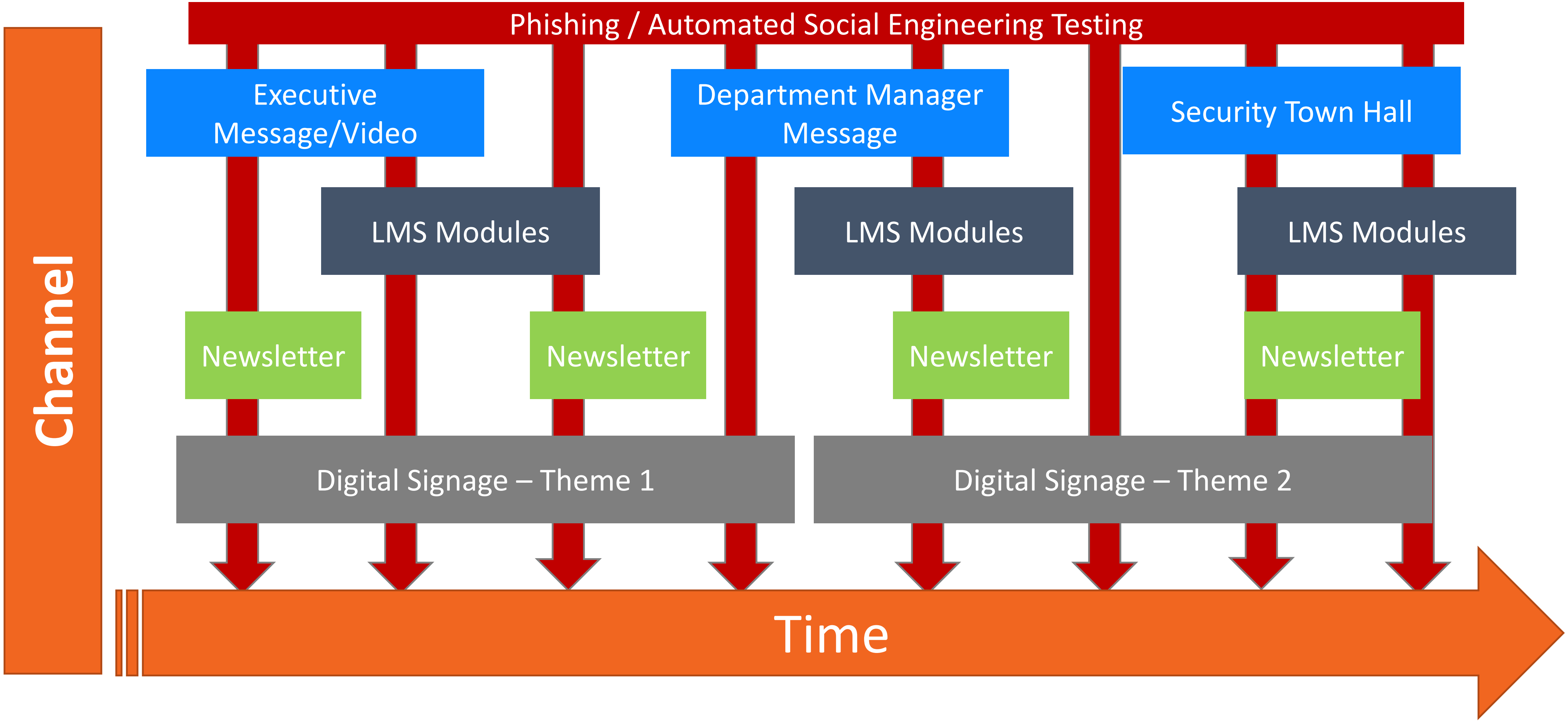
Your awareness program and content are the visible ‘face’ of your department to the rest of your company.

The Four Stages of Competence


I don’t know that I don’t know something
I know that I don’t know something
I know something, but have to think about it as I do it
I know something so well that I don’t have to think about it
PERFORMANCE
Lack of Awareness Stage
Unconcious Incompetence
Awareness Stage
Concious Incompetence
Step-by-step Stage
Concious Competence
Skilled Stage
Unconcious Competence
TIME

Noel Burch, Gordon Training International, Conscious Competence Ladder – 1970s

Plan like a Marketer. Test like an Attacker.



Phishing / Automated Social Engineering Testing

Executive Message/Video

Department Manager Message

Security Town Hall

LMS Modules

LMS Modules

LMS Modules

Newsletter

Newsletter

Newsletter

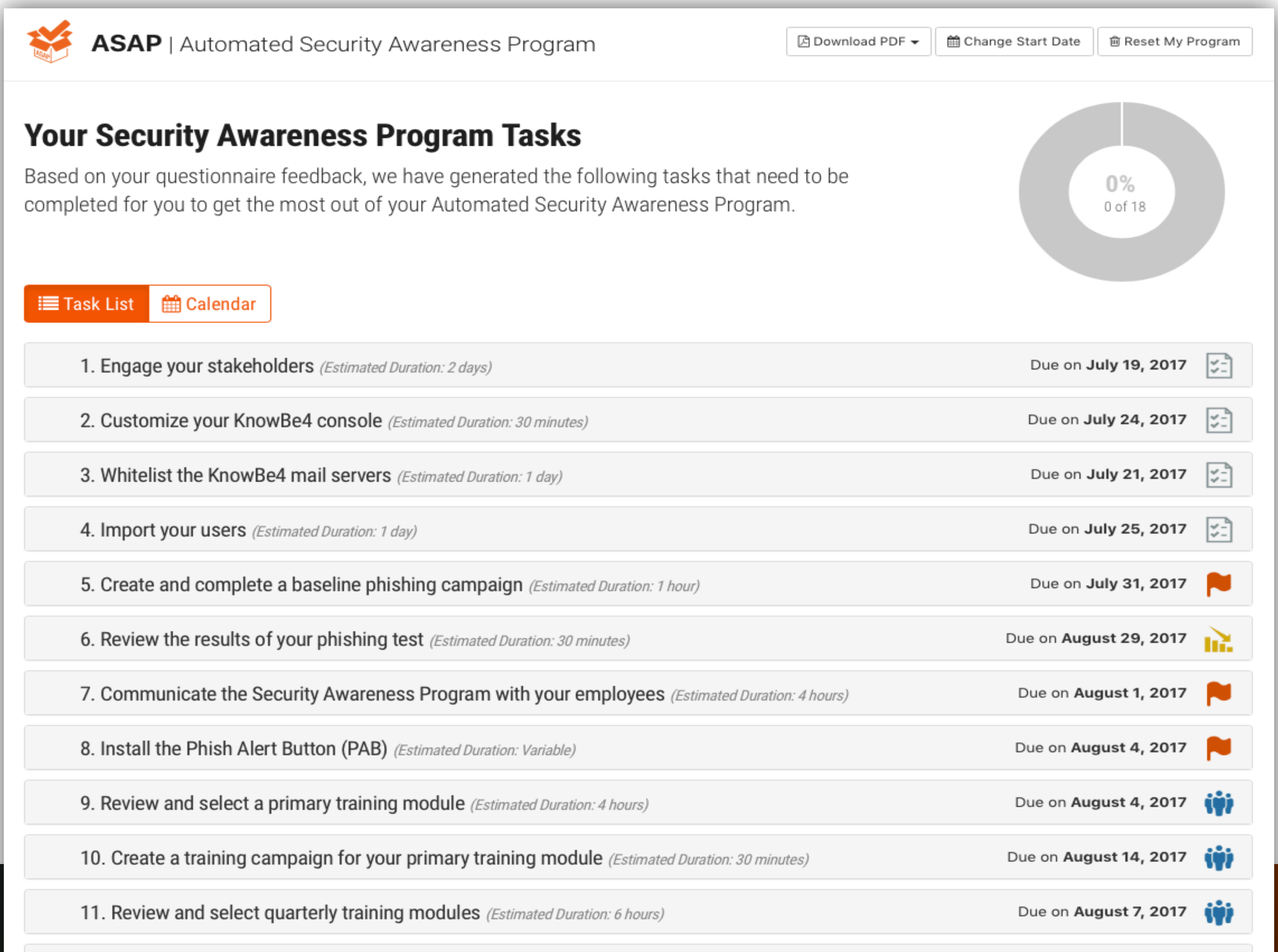
Newsletter

Digital Signage – Theme 1

Digital Signage – Theme 2

Channel

Time



Your Security Awareness Program Tasks

Based on your questionnaire feedback, we have generated the following tasks that need to be completed for you to get the most out of your Automated Security Awareness Program.

0%
0 of 18

1. Engage your stakeholders *(Estimated Duration: 2 days)* Due on **July 19, 2017**
2. Customize your KnowBe4 console *(Estimated Duration: 30 minutes)* Due on **July 24, 2017**
3. Whitelist the KnowBe4 mail servers *(Estimated Duration: 1 day)* Due on **July 21, 2017**
4. Import your users *(Estimated Duration: 1 day)* Due on **July 25, 2017**
5. Create and complete a baseline phishing campaign *(Estimated Duration: 1 hour)* Due on **July 31, 2017**
6. Review the results of your phishing test *(Estimated Duration: 30 minutes)* Due on **August 29, 2017**
7. Communicate the Security Awareness Program with your employees *(Estimated Duration: 4 hours)* Due on **August 1, 2017**
8. Install the Phish Alert Button (PAB) *(Estimated Duration: Variable)* Due on **August 4, 2017**
9. Review and select a primary training module *(Estimated Duration: 4 hours)* Due on **August 4, 2017**
10. Create a training campaign for your primary training module *(Estimated Duration: 30 minutes)* Due on **August 14, 2017**
11. Review and select quarterly training modules *(Estimated Duration: 6 hours)* Due on **August 7, 2017**

5 Points to Consider

1. Awareness in-and-of itself is only one piece of defense-in-depth, but crucial
2. You can’t & shouldn’t do this alone
3. You can’t and shouldn’t train on everything
4. People only care about things that they feel are relevant to them
5. The ongoing process is to help employees make smarter security decisions

5 Best Practices to Embrace

1. Have explicit goals before starting
2. Get the executive team involved
3. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
4. Treat your program like a marketing effort
5. Phish frequently, once a month minimum

5 Key Takeaways

1. Prioritize and make your messages and training relevant
2. Test frequently to build secure reflexes
3. Use metrics to reinforce and tell your story
4. Your awareness program operates within the larger context of your organizational culture
5. Think like a marketer, act like an attacker.

NOTE Phishing your users is actually FUN!

A Security Awareness Training Program that Works!

Baseline Testing

We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users

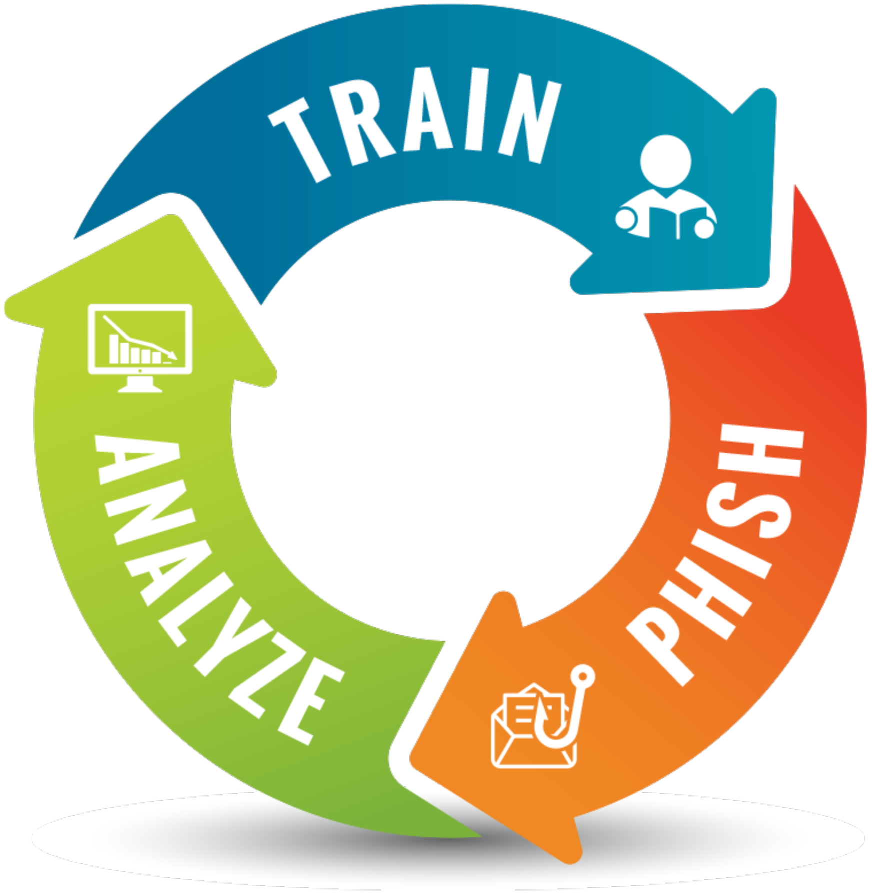
On-demand, interactive, engaging training with common traps, live hacking demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users

Fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



Resources

Free Domain Spoof Test

Find out now if hackers can spoof an email address of your own domain

Free CEO Fraud Prevention Manual

This manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim

Free Phishing Security Test

Find out what percentage of your users are Phish-prone

Free Ransomware Simulator

RanSim will simulate 13 ransomware infection scenarios and show you if a workstation is vulnerable to infection

Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click!

Free Weak Password Test

Weak Password Test gives you a quick look at the effectiveness of your password policies and any fails so that you can take action.

» Learn More at www.KnowBe4.com/Resources «