



Phishing Attack Landscape and Benchmarking

The data you need to know



Stu Sjouerman
Founder and CEO
KnowBe4, Inc.



Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.



Stu Sjouwerman
Founder and CEO, KnowBe4, Inc.

About Stu

- Serial Entrepreneur, this is my fifth startup.
- Founded KnowBe4 after building an antivirus platform from scratch (VIPRE)
- We have 400 employees now, expected to be at 600 end of 2018
- Decades-long experience in creating system admin and security tools for IT professionals



Perry Carpenter
Chief Evangelist & Strategy
Officer

About Perry

- MSIA, C|CISO
- Former Gartner Analyst leading research and advisory services to CISOs, Security Leaders, and security vendors around the world
- Led security initiatives at Fidelity Information Services, Alltel Telecommunications, and Wal-Mart Stores
- Lover of all things:
 - Security
 - Psychology
 - Behavioral Economics
 - Communication Theory
 - Magic, misdirection, and influence

About KnowBe4



- The world's most popular integrated new-school Security Awareness Training and Simulated Phishing platform, over 15,000 customers worldwide
- Founded in 2010
- Recognized as a Leader in the Gartner Magic Quadrant for Computer-Based Training (CBT)
- 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

Agenda

1. Understanding the current phishing landscape
2. New phishing benchmark data by industry
3. Actionable tips to create your “human firewall”

Agenda

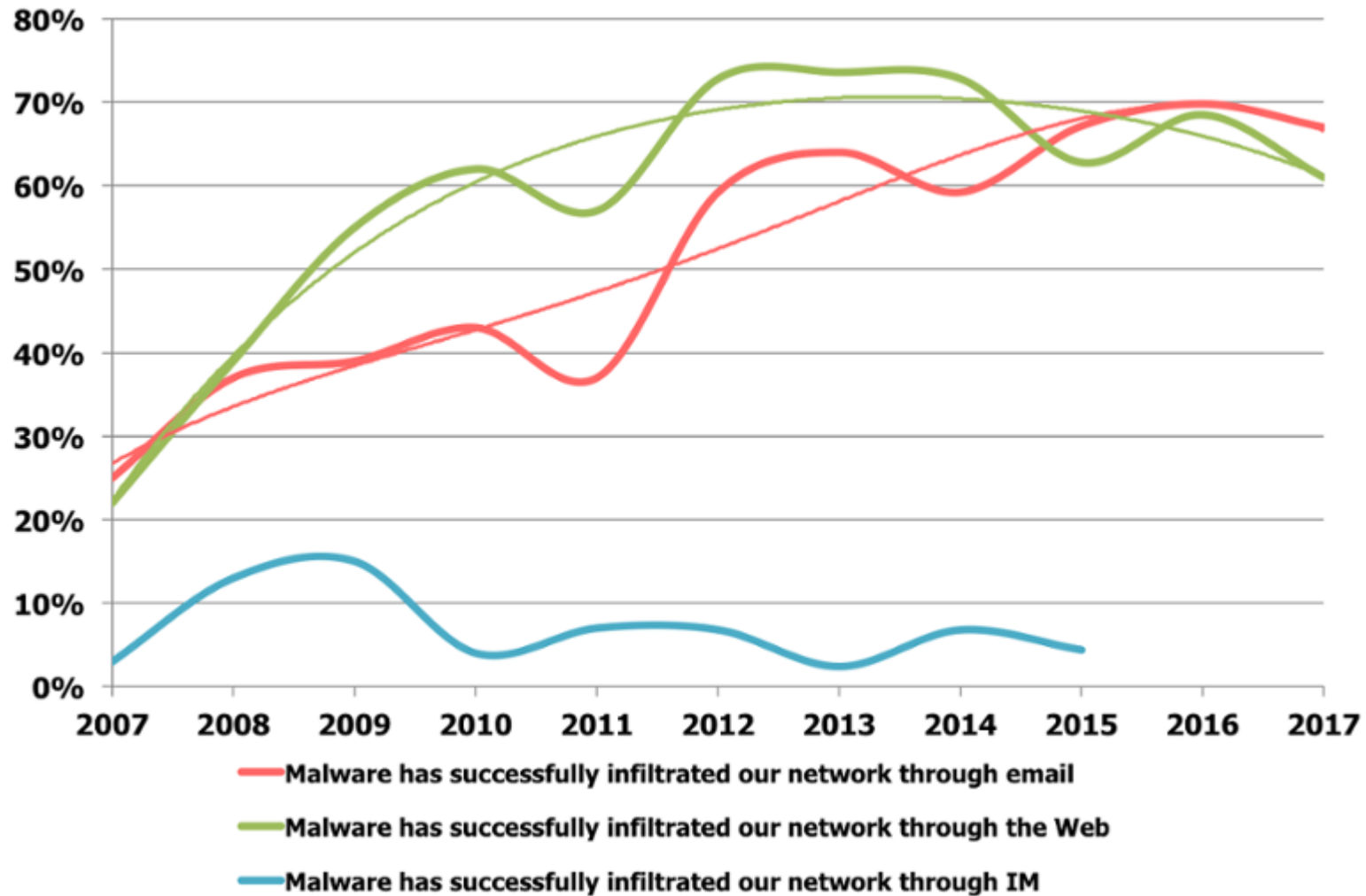
1. Understanding the current phishing landscape
2. New phishing benchmark data by industry
3. Actionable tips to create your “human firewall”

98% of Attacks Rely on Social Engineering

Attackers go for the
low-hanging fruit:

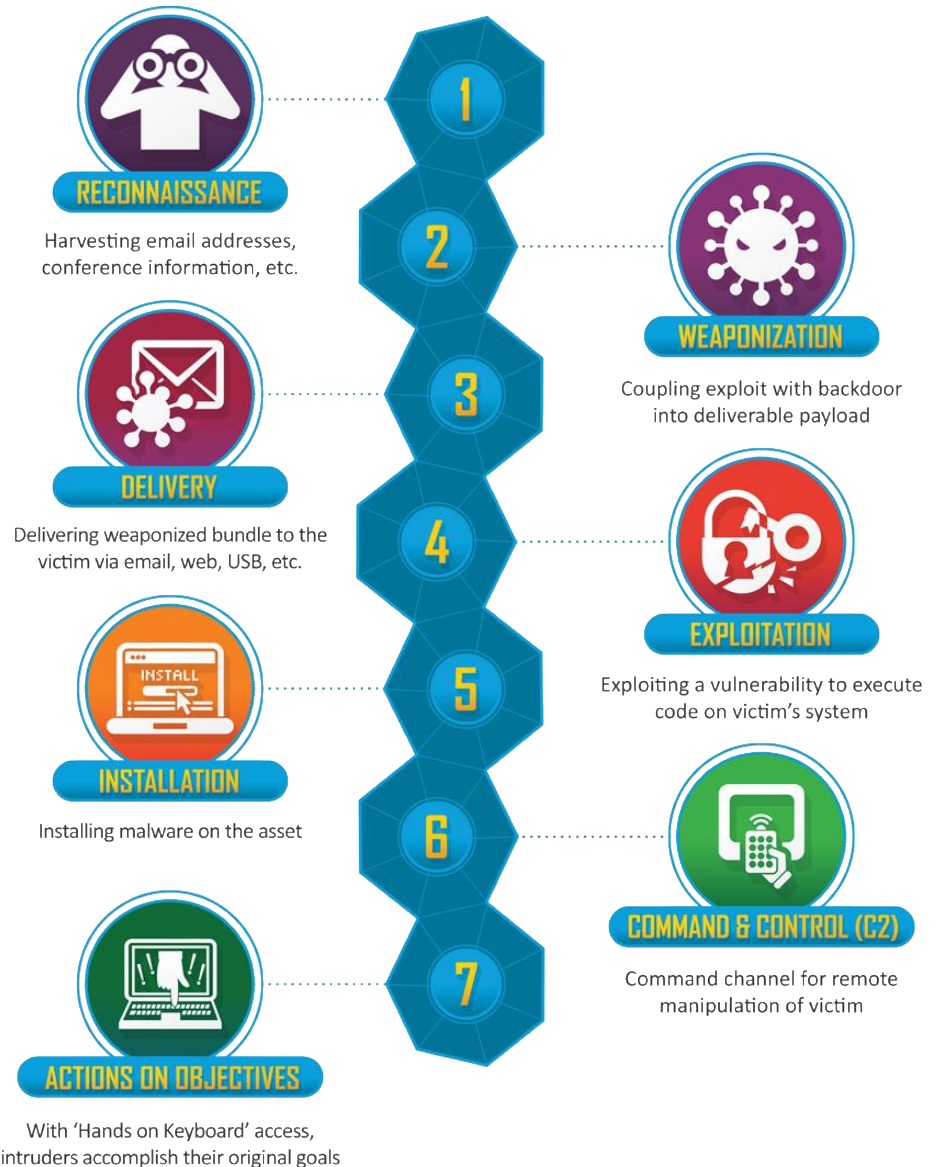
humans

Understanding the current threat landscape



the Cyber Kill Chain

Attackers generally follow these steps to compromise an organization



Agenda

1. Understanding the current phishing landscape
2. New phishing benchmark data by industry
3. Actionable tips to create your “human firewall”

Methodology and Data Set

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)
- Allowing for a '**follow-the-user-result**' from initial PST baseline, to results after 90 days of combined CBT and phishing training, to the result after one year of combined phishing and CBT

Industries

Energy & Utilities
Financial Services
Business Services
Technology
Manufacturing
Government
Healthcare & Pharmaceuticals
Insurance
Not For Profit
Education
Retail & Wholesale
Other

Size ranges

1 – 249
250 – 999
1000+

For this study, the approximate number of organizations in each size range were as follows:

*1 – 249 employees (~8K organizations)
250 – 999 employees (~2K organizations)
1000+ (~1K organizations)*

Benchmark Phish-prone Percentage by Industry

Baseline Phish-prone Percentage (B-PPP)			
Industry	1 – 249 employees	250 – 999 employees	1000+ employees
Energy & Utilities	31.56	29.34	22.77
Financial Services	27.41	28.47	23.00
Business Services	29.80	31.01	19.40
Technology	30.68	30.67	28.92
Manufacturing	33.21	31.06	28.71
Government	29.32	25.12	20.84
Healthcare & Pharmaceuticals	29.80	27.85	25.60
Insurance	35.46	33.32	29.19
Not For Profit	32.63	25.94	30.97
Education	29.20	26.23	26.05
Retail & Wholesale	31.58	30.91	21.93
Other	30.41	28.90	22.85

27%
Avg. Initial Baseline PPP
across all industries and sizes

Average PPP by Size of Organization

Org Size	Initial PPP
1 - 249	30.1 %
250 - 999	28.5 %
1000+	25.06 %

Results after 1 Quarter of CBT and Phishing Testing

90 Day Phish-prone Percentage (90-PPP)			
Industry	1 – 249 employees	250 – 999 employees	1000+ employees
Energy & Utilities	12.53	13.31	13.40
Financial Services	10.01	9.09	14.53
Business Services	12.89	13.99	13.86
Technology	14.12	16.93	19.83
Manufacturing	13.87	14.24	9.88
Government	13.13	12.76	7.90
Healthcare & Pharmaceuticals	16.81	11.02	15.79
Insurance	13.39	16.49	13.23
Not For Profit	16.01	17.28	17.07
Education	16.95	17.16	22.56
Retail & Wholesale	13.39	10.47	10.49
Other	14.86	16.37	19.97

13.3%
Avg.
90 Day PPP
across all industries and sizes

Average PPP by Size of Organization

Org Size	90 Day PPP
1 - 249	13.11 %
250 - 999	13.20 %
1000+	14.10 %

Results after 12 Months of CBT and Phishing Testing

365 Day Phish-prone Percentage (365-PPP)			
Industry	1 – 249 employees	250 – 999 employees	1000+ employees
Energy & Utilities	2.83	1.87	5.56
Financial Services	1.54	2.22	5.81
Business Services	1.89	3.09	1.27
Technology	2.02	2.42	2.69
Manufacturing	2.16	3.13	2.47
Government	1.87	1.46	1.52
Healthcare & Pharmaceuticals	2.00	1.65	2.17
Insurance	2.23	2.68	5.26
Not For Profit	2.47	2.24	3.01
Education	2.80	1.91	5.31
Retail & Wholesale	2.14	1.87	2.68
Other	1.82	3.18	4.21

2.17%
Avg.
One Year PPP
across all industries and sizes

Average PPP by Size of Organization

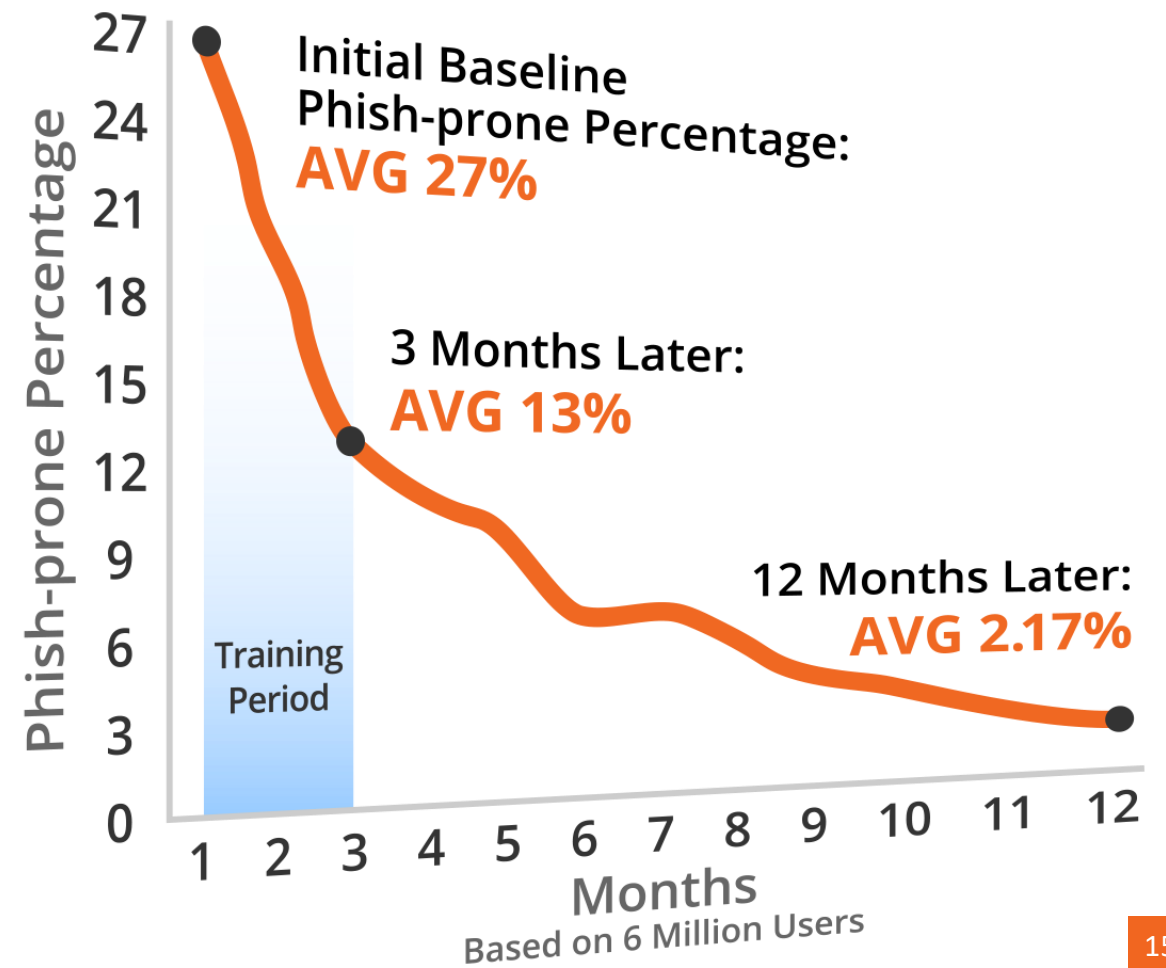
Org Size	12 Month PPP
1 - 249	1.94 %
250 - 999	2.21 %
1000+	3.04 %

*Percentages are calculated for users who experienced a combination of CBT *and* at least 10 phishing tests.*

The Results are in:

and they are encouraging

Security awareness, coupled with frequent simulated phishing training, will help employees make smarter security decisions, everyday



Agenda

1. Understanding the current phishing landscape
2. New phishing benchmark data by industry
3. Actionable tips to create your “human firewall”

People are a **critical layer** within the **fabric** of our **Security** **Programs**

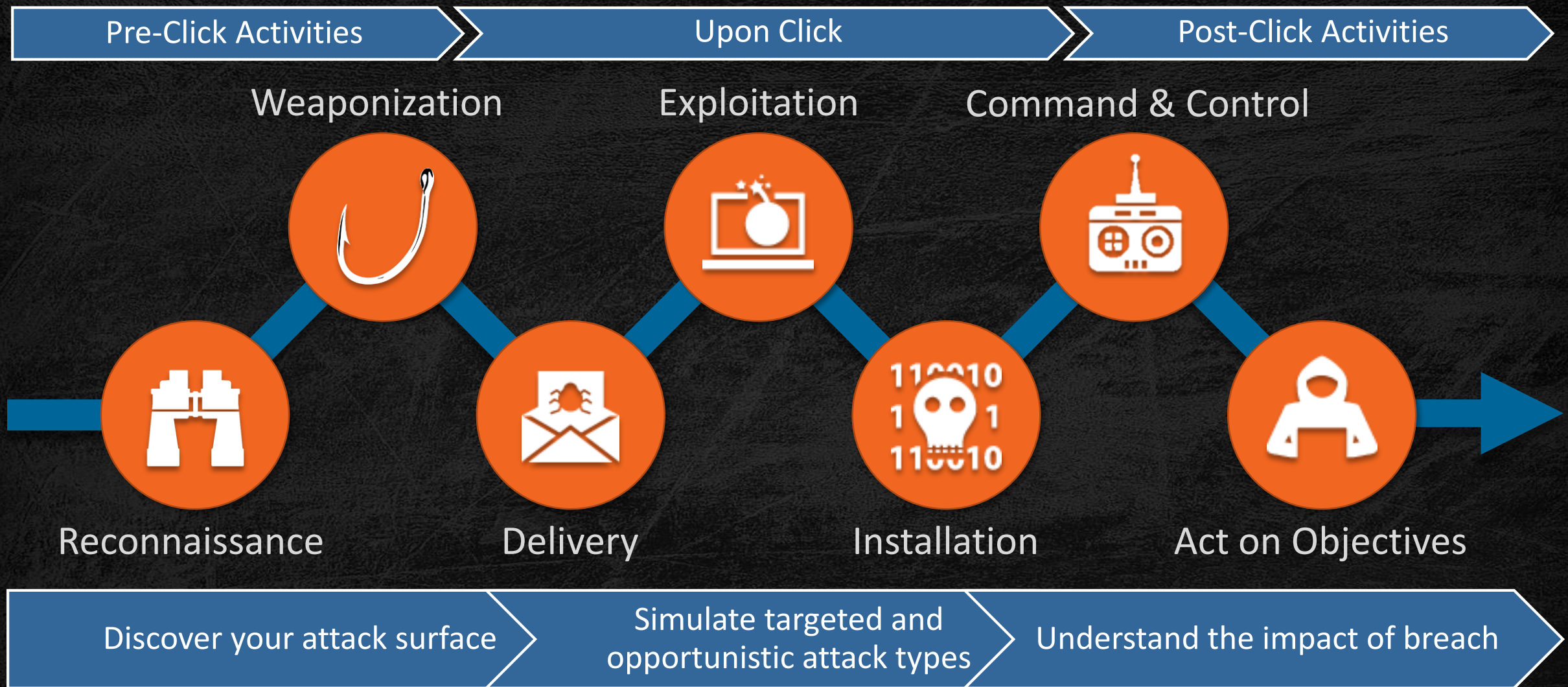


Security Awareness and *Secure Behavior* are NOT the Same Thing



**Just because
I'm *aware*
doesn't mean
that I *care*.**

Train by Simulating the Steps taken by Attackers



Discover Your **Social** **Engineering** Attack Surface

How The Bad Guys Attack



A cybercriminal does a 'deep search' for email addresses of your organization on the Internet

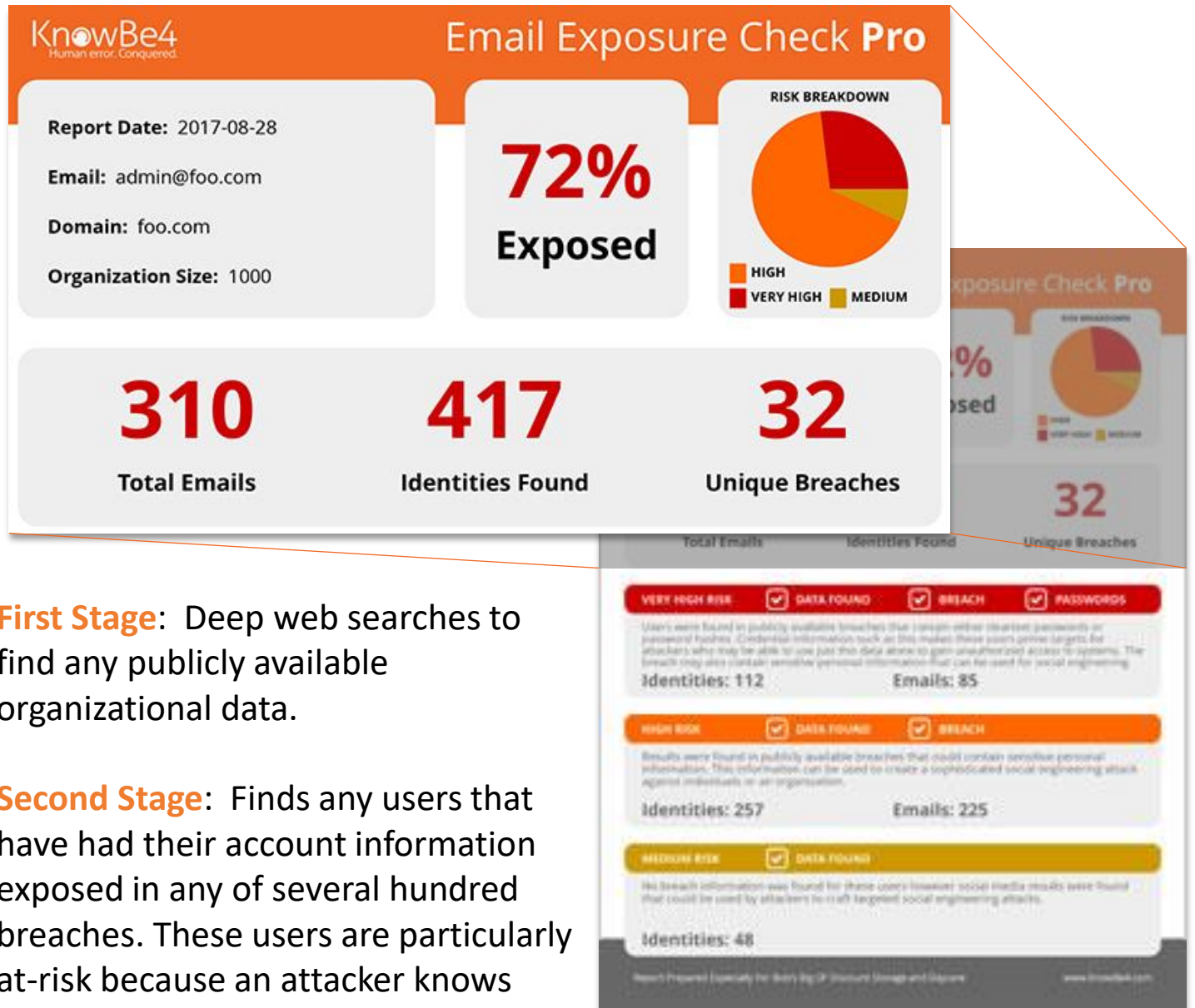
They find all publicly available email addresses of your employees

They use these to launch a phishing attack on as many employees as possible

Free tool to help simulate this:

- Email Exposure Check Pro
- Domain Spoof Test

Email Exposure Check Pro (EEC)



First Stage: Deep web searches to find any publicly available organizational data.

Second Stage: Finds any users that have had their account information exposed in any of several hundred breaches. These users are particularly at-risk because an attacker knows more about that user, up to and including their actual passwords!

Combine EEC Pro and Weak Password Test to find Soft Targets


Find Employees with Bad Password Hygiene

KnowBe4 Weak Password Test

VULNERABLE
81 accounts

NOT VULNERABLE
25 accounts

FOUND 162 WEAKNESSES



Weak Password Test uses more than 10 million common passwords to find weak passwords on your domain, also you can easily add your own passwords in our dictionary. The pie chart shows what weaknesses have been found on the provided domain.

Click the "Start Test" button to re-run the test.

Start Test

All Accounts 106

Weak Passwords	28	Account Name	Weak Password	Non-Unique Pa...	Empty Password	Clear Text Pass...	Password Not...	Password N
Non-Unique Passwords	49	AAA-BBB						
Empty Password	2	adfsService						
Clear Text Password	0	ADIService		✓				✓
Password Never Expires	71	Administrator		✓				✓
Password Not Required	5	AlanisMorissette	✓	✓				✓
LM hashes	2	Alin		✓				✓
AES Keys Missing	1	ariel						✓
Kerberos DES-only	3	Ashley						✓
Pre-authentication missing	1	ben		✓				✓
		billmurray	✓	✓				✓
		Bret		✓				✓
		brian		✓				✓
		bruce	✓	✓				✓
		brucew	✓	✓				✓
		captkirk	✓					✓
		carygrant		✓				✓
		Cher		✓				✓

Copyright © KnowBe4 Inc. 2017

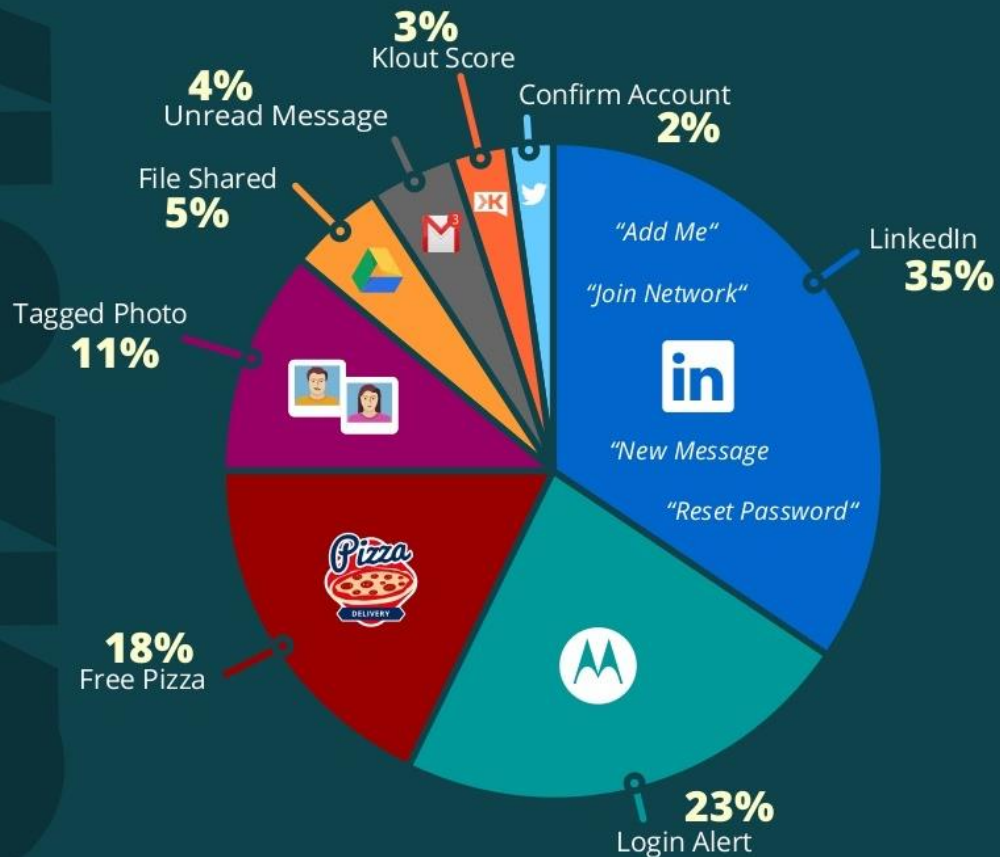
v. 1.0.0.8

Bait the hook!

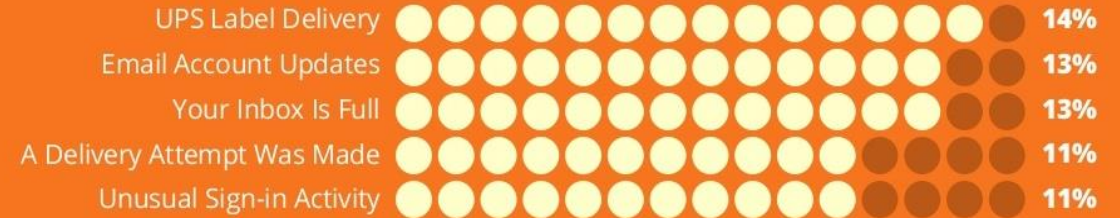
- Understand the types of email subjects that will realistically test your users susceptibility to phishing.
- Know the types of 'in the wild' phishing scams that are occurring so that you can work to inoculate your users!

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 5 GENERAL EMAIL SUBJECTS



KEY TAKEAWAY



Email is an effective infection vector because it gives attackers the control to craft and distribute enticing material to both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.



TOP "IN THE WILD" ATTACKS

- Direct Deposit of Payment on Your Checking Account
- Irregular Activity on Your SunTrust Online Account
- Closing Extension/Final Closing Statement
- Bank transfer of 75,000 USD
- Drake: Account Validation
- Threats of Legal Action About Invoice 72393
- RFQ Quote the Models
- PayPal: Your account has been limited
- Your Order #335816 placed on Friday is paid

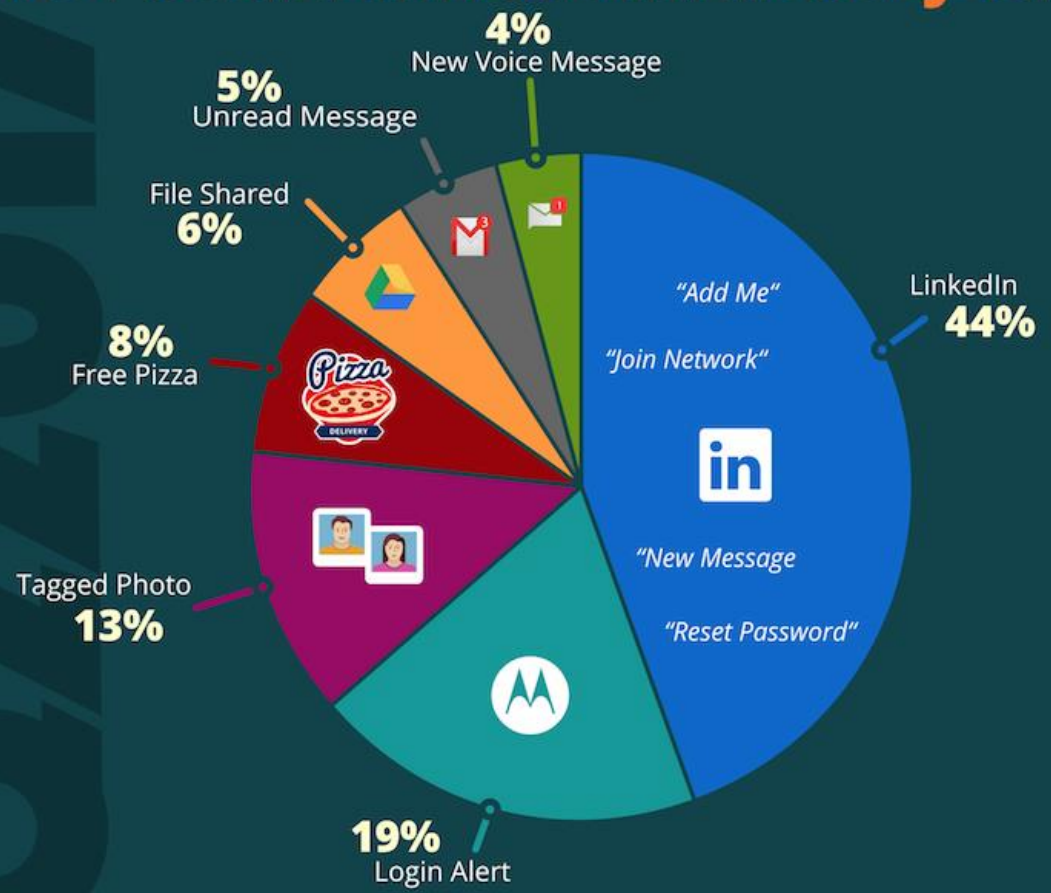
KEY TAKEAWAY



These attacks are effective in that they are using the personal finances of the target as the lure. Also, a single-stage phish is easier to accomplish than multi-stage because it exploits an immediate psychological 'knee jerk' impulse.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS

	Security Alert	21%
	Revised Vacation & Sick Time Policy	14%
	UPS Label Delivery 1ZBE312TNY00015011	10%
	BREAKING: United Airlines Passenger Dies	10%
	A Delivery Attempt was made	10%
	All Employees: Update your Healthcare Info	9%
	Change of Password Required Immediately	8%
	Password Check Required Immediately	7%
	Unusual sign-in activity	6%
	Urgent Action Required	6%

KEY TAKEAWAY

i Email is an effective infection vector because it gives attackers the control to craft and distribute enticing material to both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.



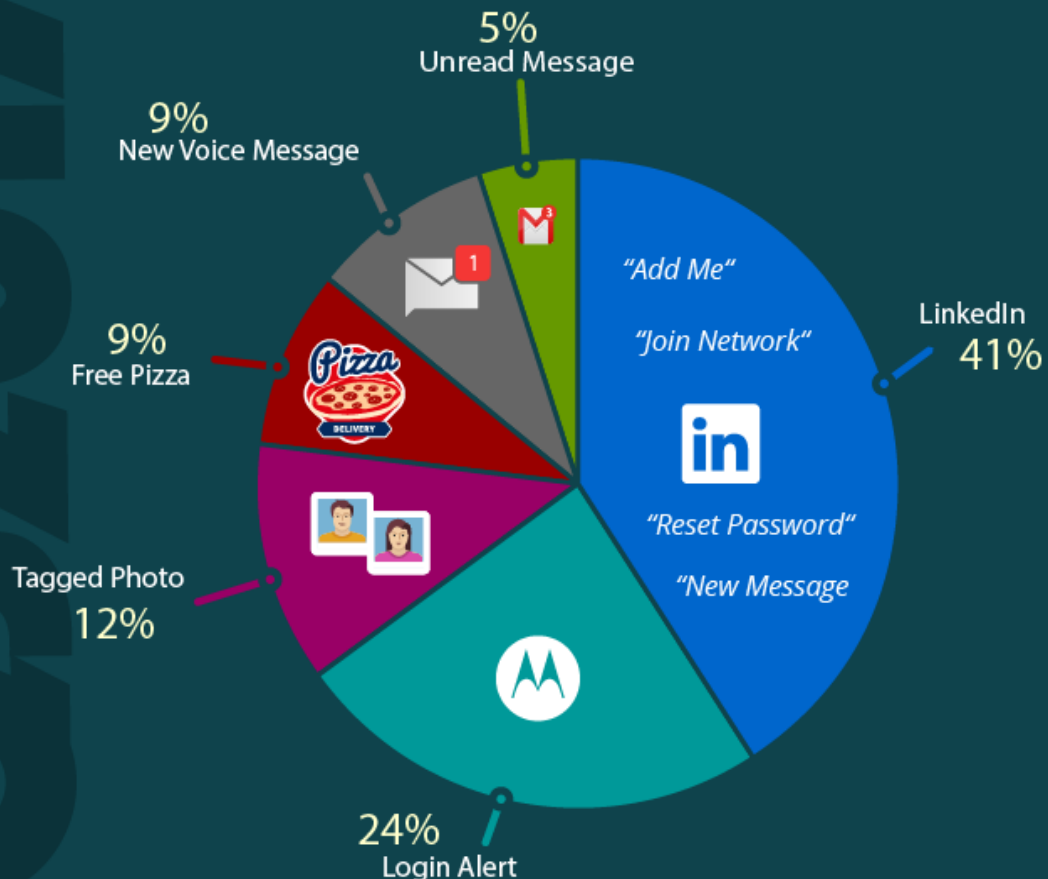
TOP "IN THE WILD" ATTACKS

- Direct Deposit of Payment on Your Checking Account
- Irregular Activity on Your SunTrust Online Account
- Closing Extension/Final Closing Statement
- Bank transfer of 75,000 USD
- Drake: Account Validation
- Threats of Legal Action About Invoice 72393
- RFQ Quote the Models
- PayPal: Your account has been limited
- Your Order #335816 placed on Friday is paid

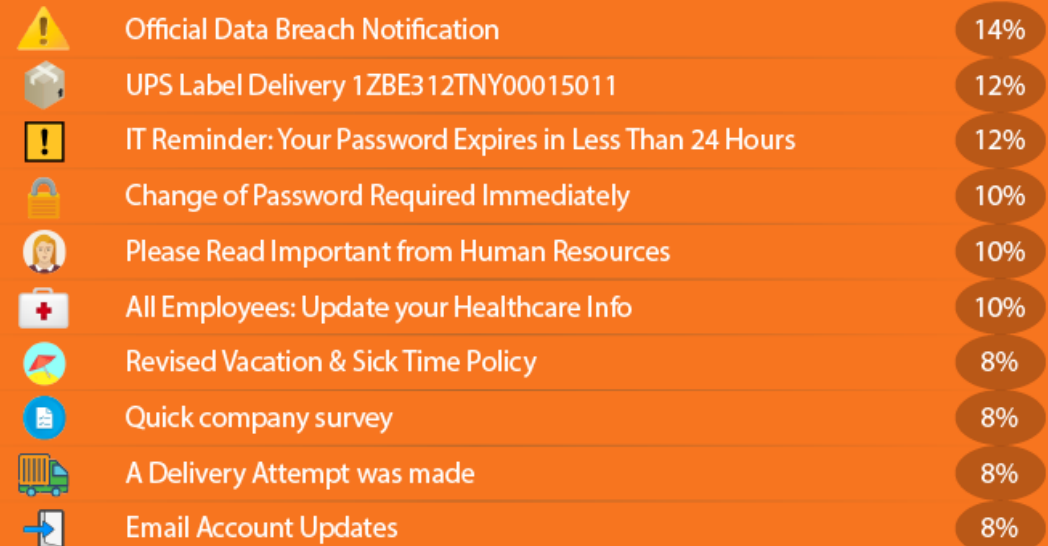
TOP-CLICKED

PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS




KEY TAKEAWAY



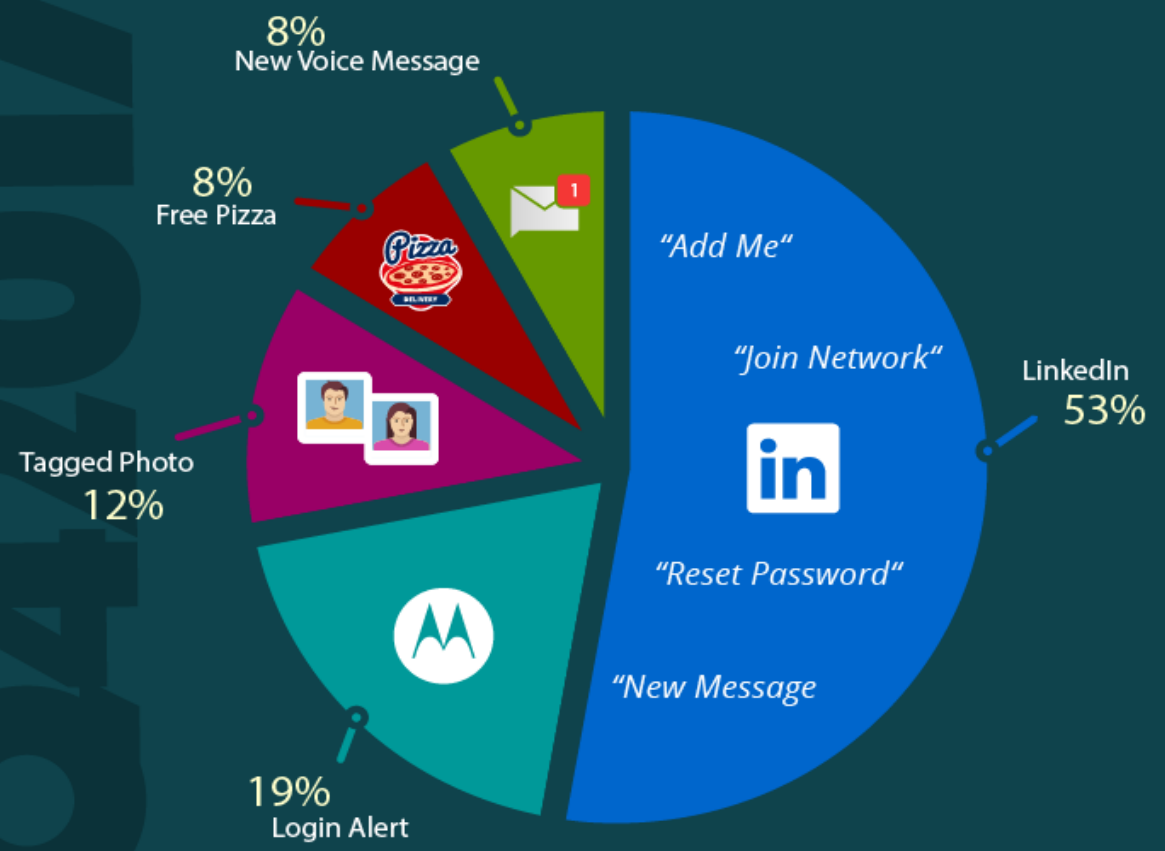
Email is an effective way to phish users when disguised as legitimate email. These methods allow attackers to craft and distribute enticing material for both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.

COMMON "IN THE WILD" ATTACKS

- 
- LinkedIn: Important Security Update
 - Amazon: Kindly update your account with Amazon to avoid shutdown
 - Email account will be closed
 - Office 365: Incoming mail on hold
 - We have created your ticket for server upgrade
 - Credit Card Details Follow Up
 - USAA: E-Money Pending Approval
 - PayPal: Problem with Account ID
 - Synchrony Bank/Walmart: Account Alerts
 - COURT NOTICE FILED AGAINST YOU

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS

	A Delivery Attempt Was Made	18%
	UPS Label Delivery 1ZBE312TNY00015011	16%
	Change of Password Required Immediately	15%
	Unusual sign-in activity	9%
	Happy Holidays! Have a drink on us.	8%
	Join my network on LinkedIn	7%
	Staff Review 2017	7%
	All Employees: Update your Healthcare Info	7%
	Psst. PSL is B-A-C-K!	7%
	Invitation: Performance Review	6%

KEY TAKEAWAY

i Email is an effective way to phish users when disguised as legitimate email. These methods allow attackers to craft and distribute enticing material for both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.



COMMON "IN THE WILD" ATTACKS

- Microsoft Drive: Invoice&payment21.pdf
- ID Suspension
- Your domains have been blocked
- Microsoft Office 365 Upgrade Test
- Facebook: Secure your Account
- PayPal: Your account was recently logged into from a new browser or device
- HR: End of year payroll Adjustment
- Alibaba.com: Lisa Witt has sent you an inquiry
- Microsoft Outlook: Inbound Activity Error: Failure receiving mail [Case ID: 39900801]
- Your iCloud account was used to login from a new device and location



Social Engineering

-- effective phishing lures --

Greed

Curiosity

Self Interest

Money

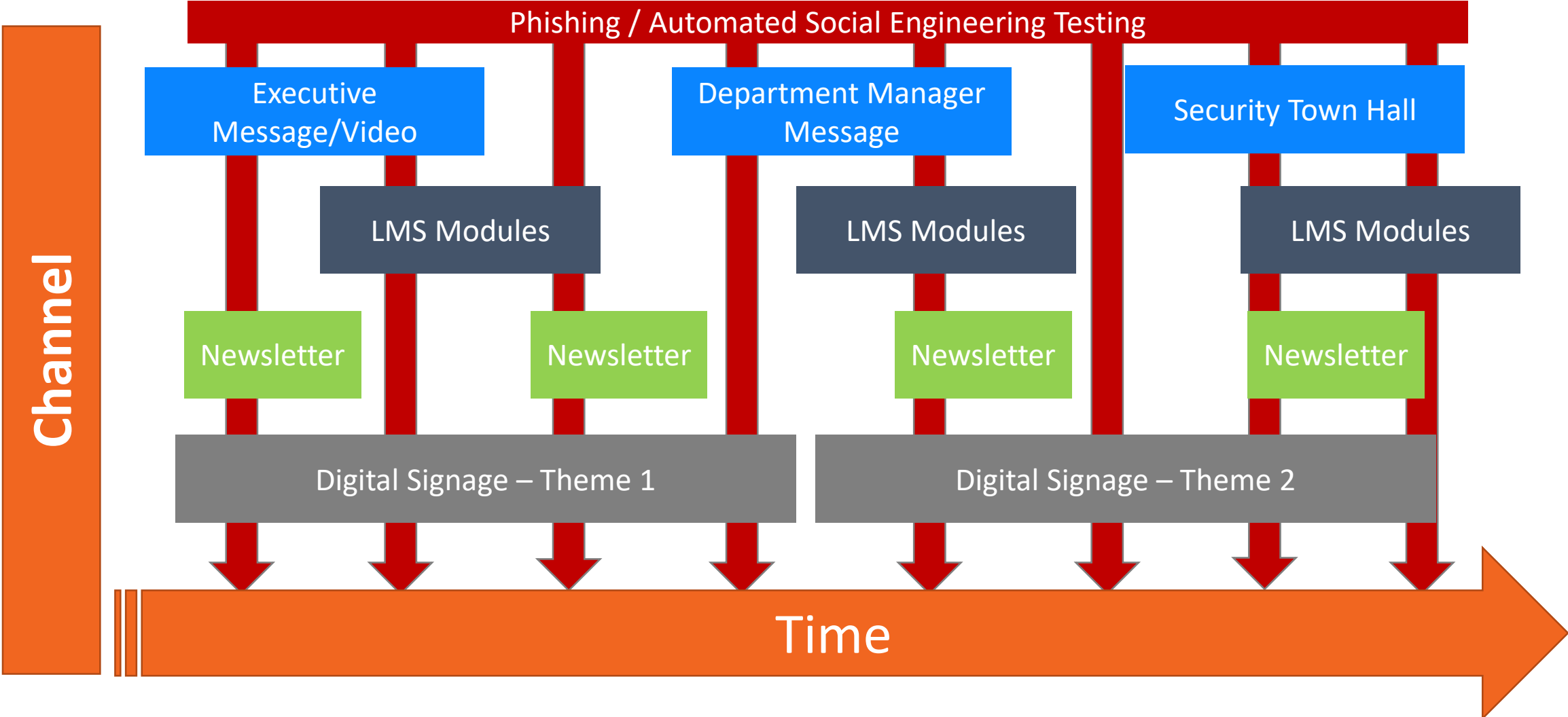
Urgency

Fear

Helpfulness

Hunger

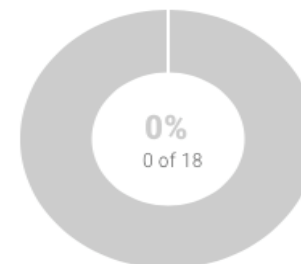
Plan like a Marketer. Test like an Attacker.





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.



Task List

Calendar

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

Final Thoughts

- Humans are the de-facto top choice for cybercriminals seeking to gain access into an organization.
- Security Awareness and frequent simulated social engineering testing is a proven method to dramatically slash your organization's phish prone percentage.
- Effectively managing this problem requires ongoing due diligence, but it *can* be done and it isn't difficult. We're here to help.

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.