RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **HUM-R08V**

Getting Engagement in the Midst of Chaos

Javvad Malik

Security Awareness Advocate
KnowBe4
@J4vv4D

Erich Kron

Security Awareness Advocate
KnowBe4
@ErichKron

Erich Kron

Security Awareness Advocate

@ErichKron

About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)2
- A veteran of IT and Security since the mid 1990's in manufacturing, healthcare and DoD environments
- Hero to Javvad

CISSP® Certified Information Systems Security Professional

CISSP® Certified Information Systems Security Professional

ISSAP® Architecture

Microsoft® CERTIFIED IT Professional

Javvad Malik

Security Awareness Advocate

@J4vv4D

About Javvad Malik

- 20 years in computer security
- IT Security Operation
- Infosec Consultant
- Analyst at 451Research
- Security Advocate at KnowBe4
- YouTuber
- Podcast Host
- Blogger
- Hero to millions

Agenda

- Disruptions Abound
- Attacks Against Home Workers
- Engagement in the Defense

RSAConference2020 APJ

A Virtual Learning Experience

Disruptions Abound

Habits Were Quickly Changed

April 9, 2020: The same intersection just six weeks later—a 62 percent drop in traffic.

- Habits have changed and life had been disrupted.
- Travel, even locally, dropped significantly in a very short amount of time.
- Leaving the house quickly became a novelty as opposed to daily life

Source: https://www.csis.org/analysis/japans-response-covid-19-work-progress

Attacks Spiked

- Attacks took off as people transitioned to working from home
- March 8-14 = 16 New Templates
- March 15-21 = 36 New Templates
- March 22-28 = 94 New Templates

The Growth & Development of COVID-19 Phishing Templates

Week	New Templates
Jan. 19 - Jan. 25	0
Jan. 26 - Feb. 1	1
Feb. 2 - Feb. 8	5
Feb. 9 - Feb. 15	6
Feb. 16 - Feb. 22	5
Feb. 23 - Feb. 29	3
Mar. 1 - Mar. 7	16
Mar. 8 - Mar. 14	16
Mar. 15 - Mar. 21	36
Mar. 22 - Mar. 28	94

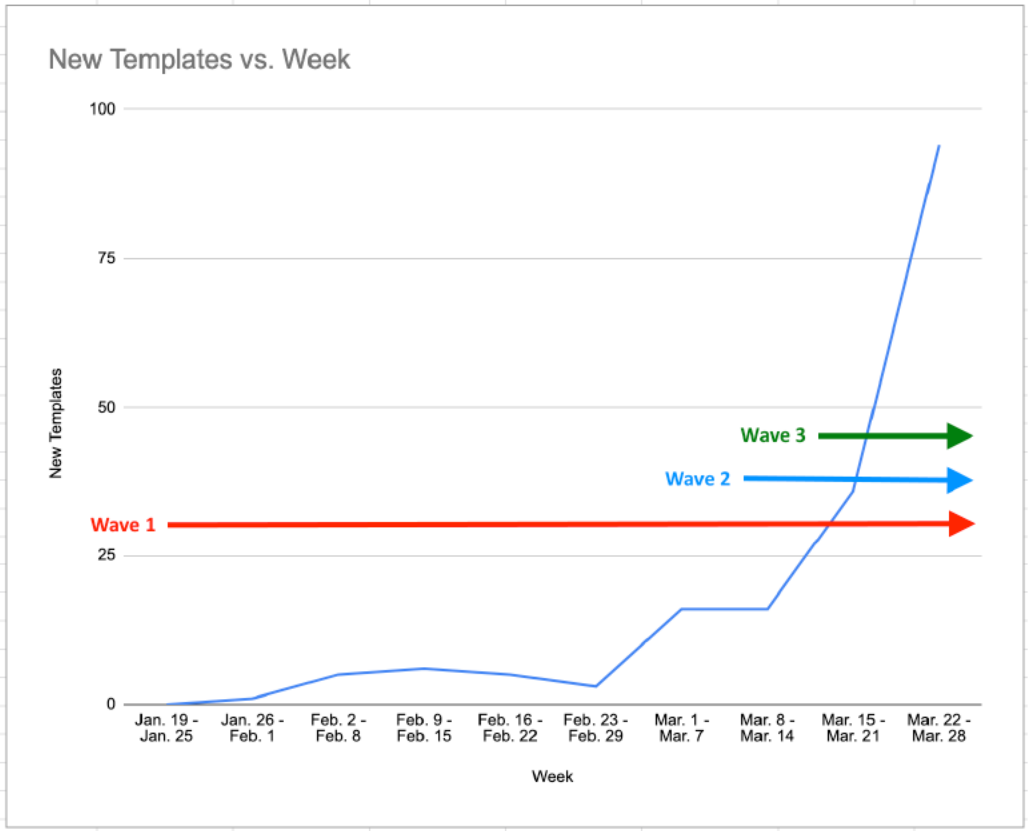
Note: "New Templates" means new and unique COVID-19 phishing templates encountered for the first time. Templates can be considered "new and unique" even if they are minor variations of earlier templates. Templates classified as "spam / scam" are not considered or included in this number.

The Three Waves of Templates

Wave 1: Spoofs of authoritative sources of information (CDC/WHO/HHS/HR) purportedly offering information and updates on the outbreak.

Wave 2: New and novel templates designed exclusively for COVID-19 that move beyond merely offering new information on the outbreak.

Wave 3: Re-purposed older templates and social engineering schemes modified and updated to include a COVID-19 theme or angle.



The World Adjusts

- All levels of life and work have been disrupted including the shutdown of sports. People are hungry for information
- In many cases organizations and government entities have had to provide incomplete information to employees and the public

Tokyo Olympics in 2021 at risk of cancellation admits Japan's PM

- **Staging Games 'difficult' if pandemic not contained**
- **IOC's Bach warns proliferation of events may need review**

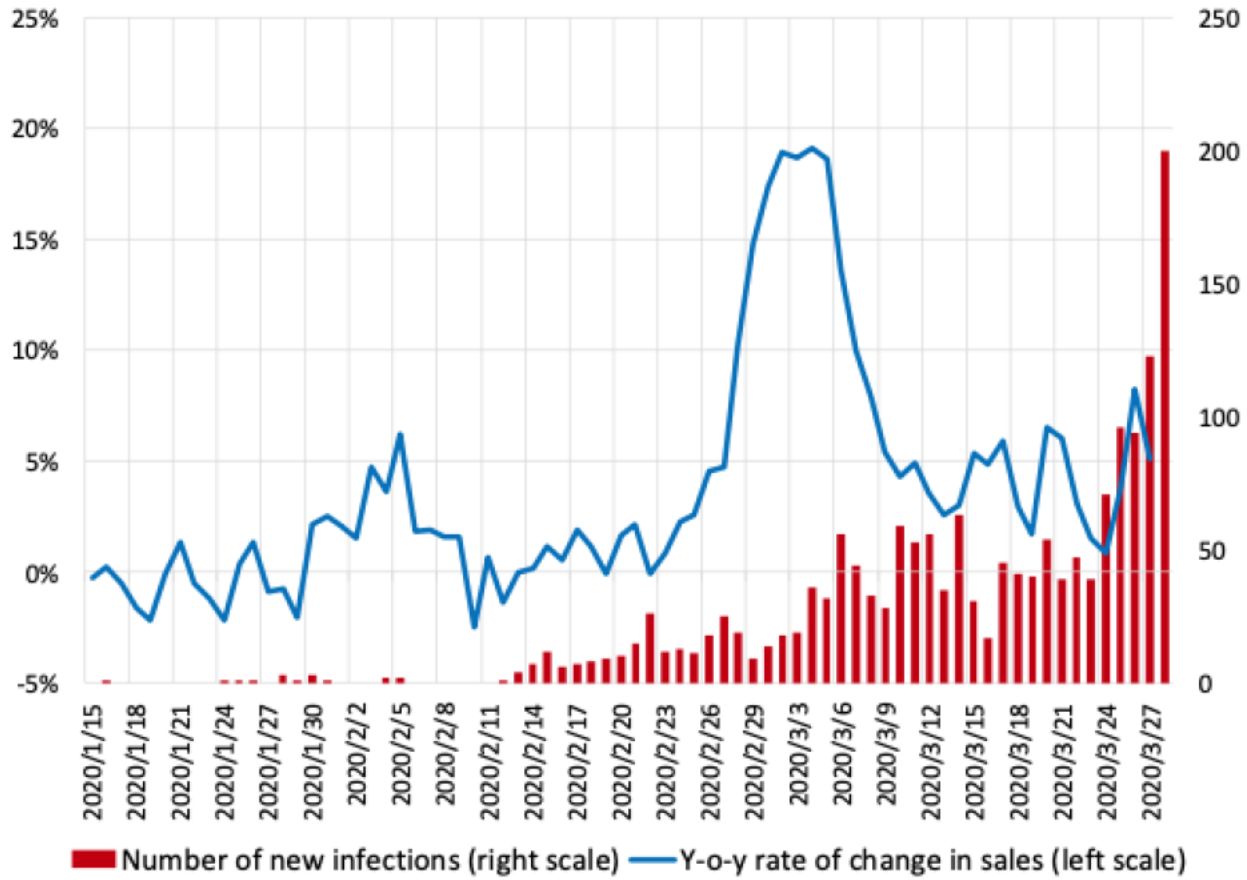
▲ The Tokyo Games, originally set to start in July this year, have been rescheduled for 2021. Japan has spent $13bn on preparations. Photograph: Kim Kyung Hoon/Reuters

Japan's prime minister, Shinzo Abe, has given the starkest warning yet that the rearranged Tokyo Olympics next year might have to be cancelled completely, saying it would be difficult to stage them if the coronavirus pandemic is not contained.

Uncertainty Drives Concern

- Economic changes have impacted everyone and panic buying/shortages have become normal
- Disruptions in the supply chain and unanticipated demand for products has created panic buying, leaving vendors scrambling

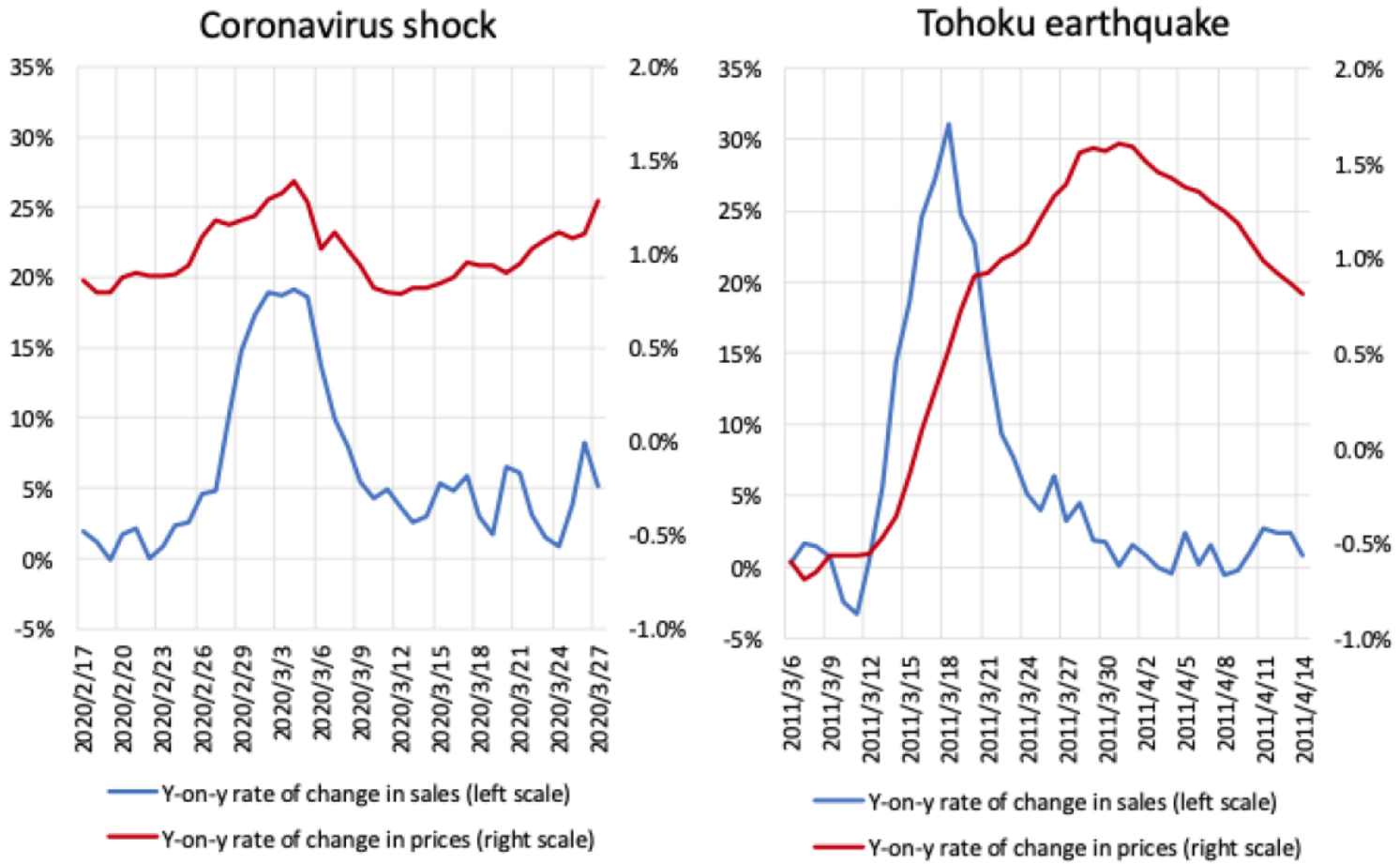
The number of new infections in Japan and supermarket sales



Sources: Nowcast Inc., "Nikkei CPINow." NHK News Web

It Has Happened Before

- Natural and unnatural events happen with impacts on economy and spending
- Anxiety and uncertainty drive panic buying and price hikes on low supply



Source: Nowcast Inc., "Nikkei CPINow."

Unexpected Supply Chains

Wuhan

Lockdown

Cargo planes

Cartels

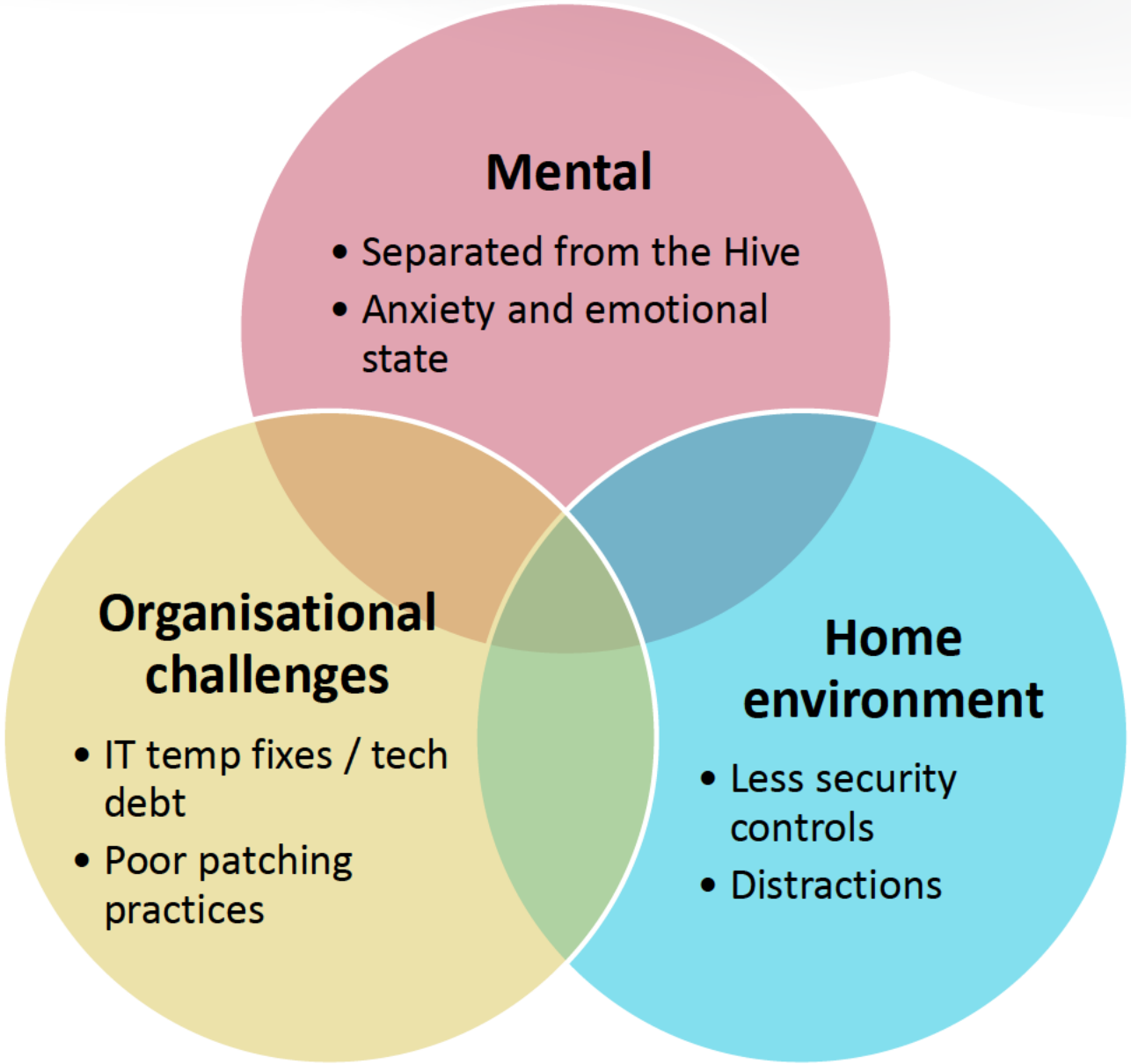
Border shutdown

Fentalyn pills in San Diego increase from $5 to $7

RSAConference2020 APJ
A Virtual Learning Experience

Attacks Against Home Workers

Why Attack Homeworkers?

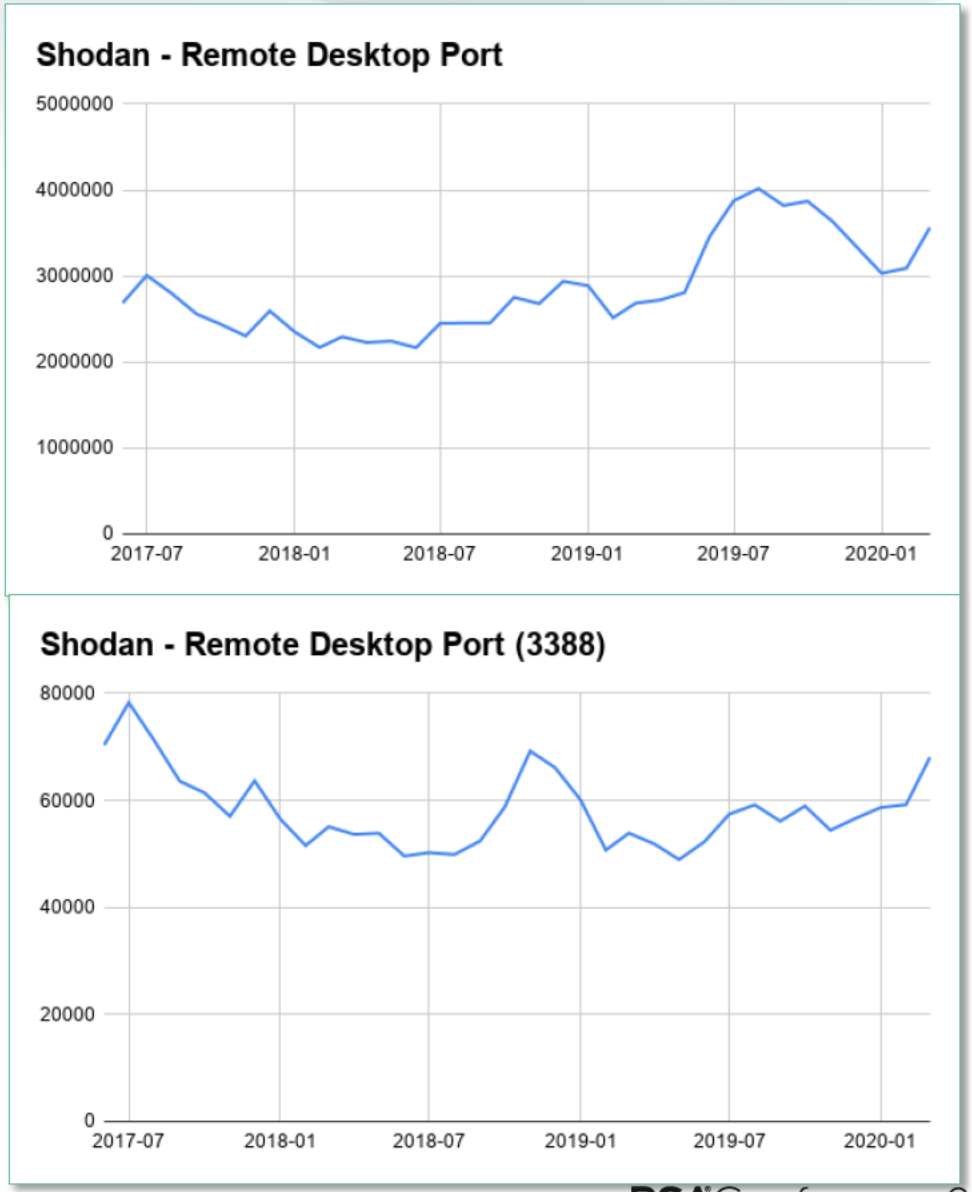


Criminals are sharks…

… this is what homeworkers look like to them

Quick Changes Were Made

- Technical debt is being accumulated as “quick fixes” are implemented to get people working and productive
- This is not unusual or specifically bad, but it there will be a reckoning

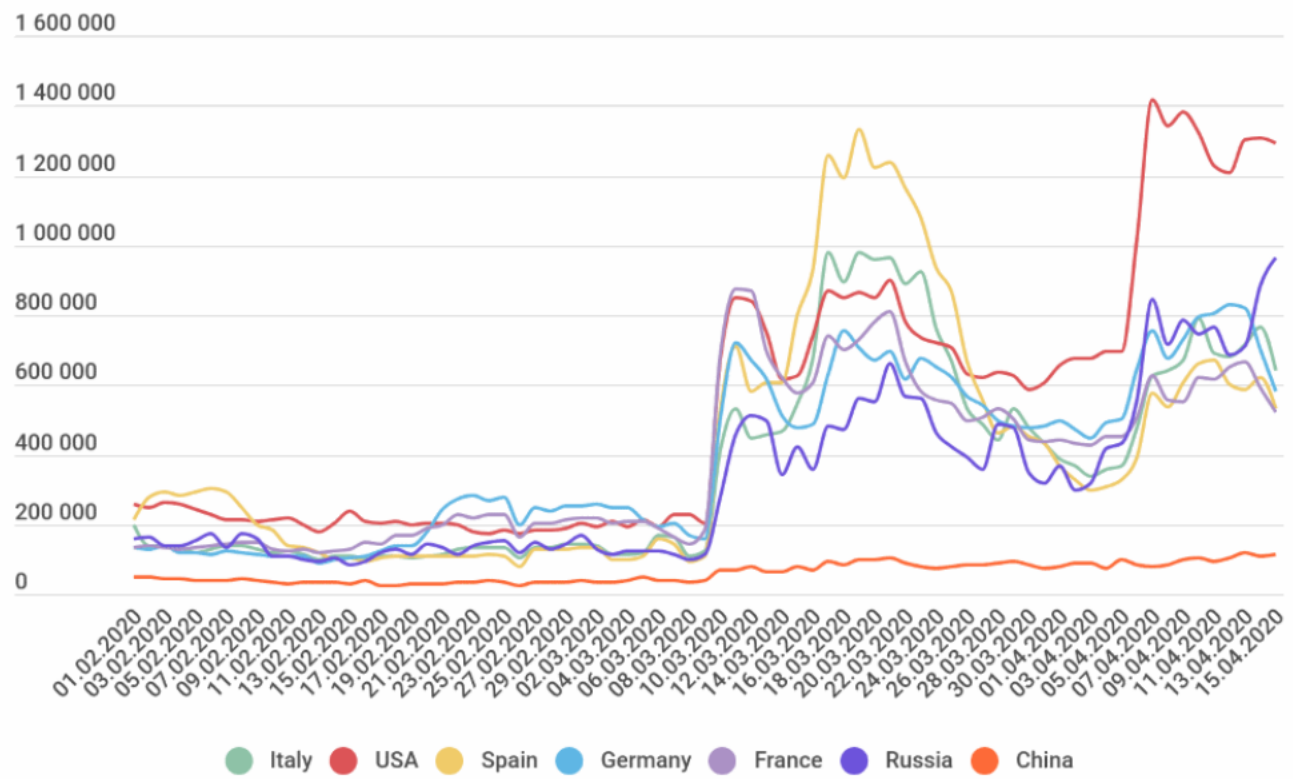


Open RDP = Brute Force Attacks

- The new RDP attack surface is being exploited through credential stuffing and password spraying
- Are small or medium, organizations monitoring against brute force attacks?

Kaspersky: RDP brute-force attacks have gone up since start of COVID-19

RDP brute-force attack numbers rose in mid-March as quarantines were being imposed over the globe.



Remote Working = New Tools

- Zoom and other collaboration platforms are being heavily targeted
- People are unfamiliar with the technology and liable to make errors

Apple Founder Zoom-Bombs Meeting To Thank COVID-19 Scientists

John Cumbers Senior Contributor
Manufacturing
Synthetic biology & space settlement connector, founder and investor.

Steve Wozniak, co-founder of Apple with Steve Jobs, thought he had coronavirus. His quest for the test reveals the progress we've made—and the work to be done.

Steve Wozniak, co-founder of Apple with Steve Jobs, thought he had coronavirus. His quest for the ... [+] SYNBIOBETA

Zoom buys security company, aims for end-to-end encryption

Intel report: Zoom could be vulnerable to foreign surveillance

Two new massive Zoom exploits uncovered

500,000 Zoom accounts sold on hacker forums

Singapore teachers banned from Zoom

Taiwan bans Zoom from government use

Attackers Use Psychology

Our brains' job to filter, interpret, and present 'reality'

Social Engineering

Are You Being Manipulated?

-- understand the lures --

Greed	Curiosity	Self Interest
Urgency	Fear	Helpfulness

Social Media

- Social media is being used to spread misinformation at an incredible rate
- This causes more anxiety and mental fatigue

GEORGE FLOYD · Published June 5

More than half of social media posts about George Floyd, police brutality, are from fake accounts: study

By Hollie McKay | Fox News

Hollywood ramps up calls to defund police amid riots and looting

Fox Nation host David Webb pushes back on the 'dangerous' rhetoric of the Hollywood elites amid the George Floyd unrest.

As both peaceful protests and violent rioting continue to unfold across much of the country following the May 25 death of George Floyd while in Minneapolis police custody, an extensive social media assessment has found that the unrest has been significantly amplified by the monthslong coronavirus lockdown and that more than half the online narrative is being driven by fraudulent accounts and bots.

Source: https://foxnews.com

THE CORONAVIRUS CRISIS

Researchers: Nearly Half Of Accounts Tweeting About Coronavirus Are Likely Bots

May 20, 2020 · 10:19 PM ET

BOBBY ALLYN

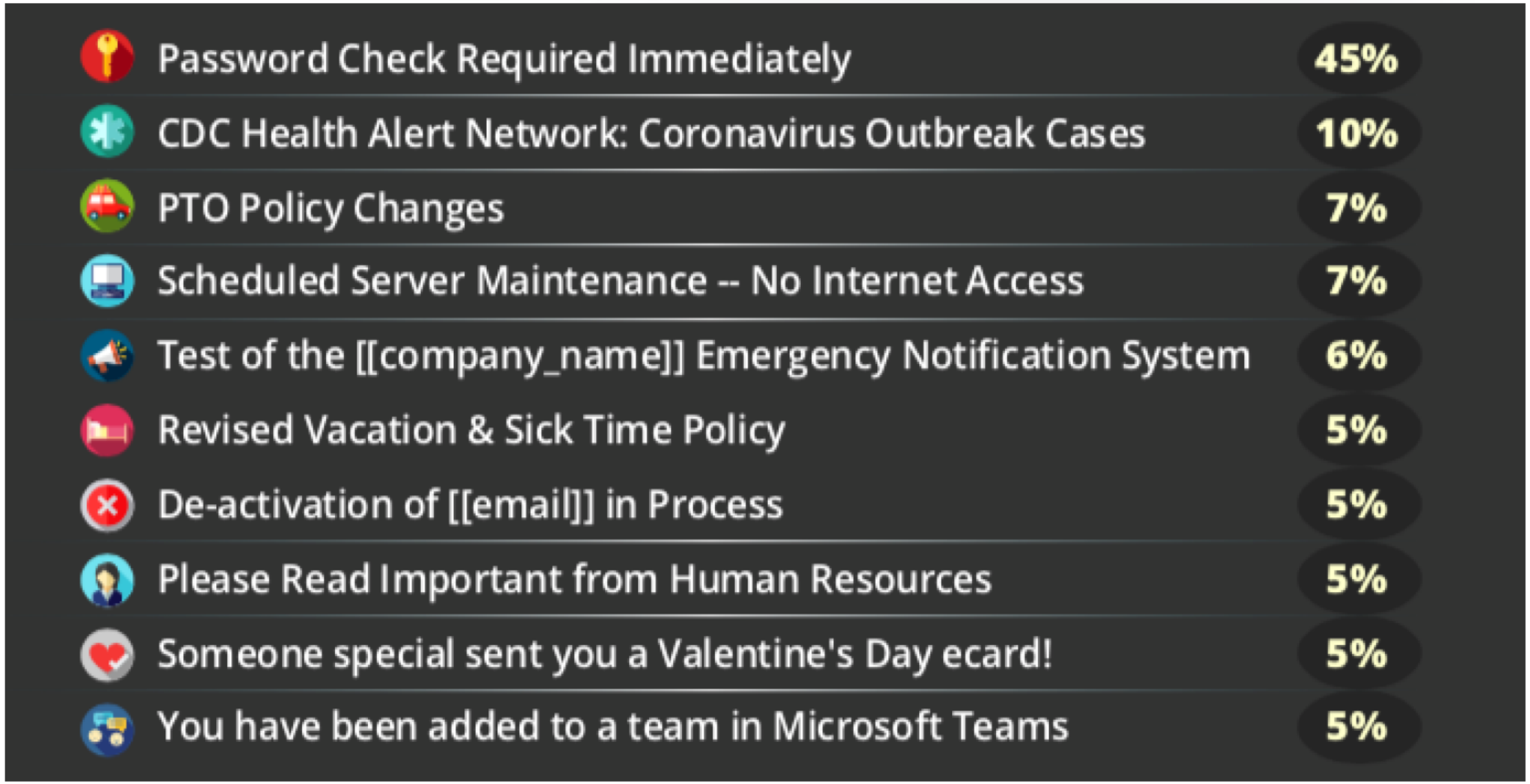
Researchers from Carnegie Mellon University say nearly half of all accounts tweeting about the coronavirus appear to be bot accounts.

Updated at 7:55 p.m. ET

Nearly half of the Twitter accounts spreading messages on the social media platform about the coronavirus pandemic are likely bots, researchers at Carnegie Mellon University said Wednesday.

Source: https://www.npr.org/

Top 10 General email subjects Q1 2020



RSAConference2020 APJ

A Virtual Learning Experience

Engagement in the Defense

Awareness itself does not result in secure behaviour

"Everybody has a plan
until they get punched
in the mouth."
- Mike Tyson

http://articles.sun-sentinel.com/2012-11-09/sports/sfl-mike-tyson-explains-one-of-his-most-famous-quotes-20121109_1_mike-tyson-undisputed-truth-famous-quotes

What Is Your Focus?

Ask yourself

Do you care more about what your people know or what they do?

Have Realistic Goals

You can't effectively train on everything…

If your goal is behavior change,

focus on 2 to 3 behaviors at a time

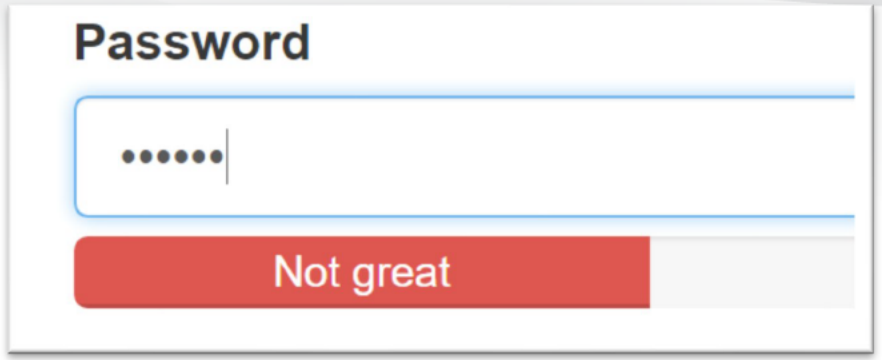
Think Like A Marketer

Bunmeido Sponge Cake

" Our egg yolk is different from other places. We raise chickens in natural valleys with organic grass and corn to make the yolks have a fresh color and intense taste."

"We have kept our original, traditional manufacturing method through more than 100 years of research and experiences of making the best castella."

Nudge them in the right direction



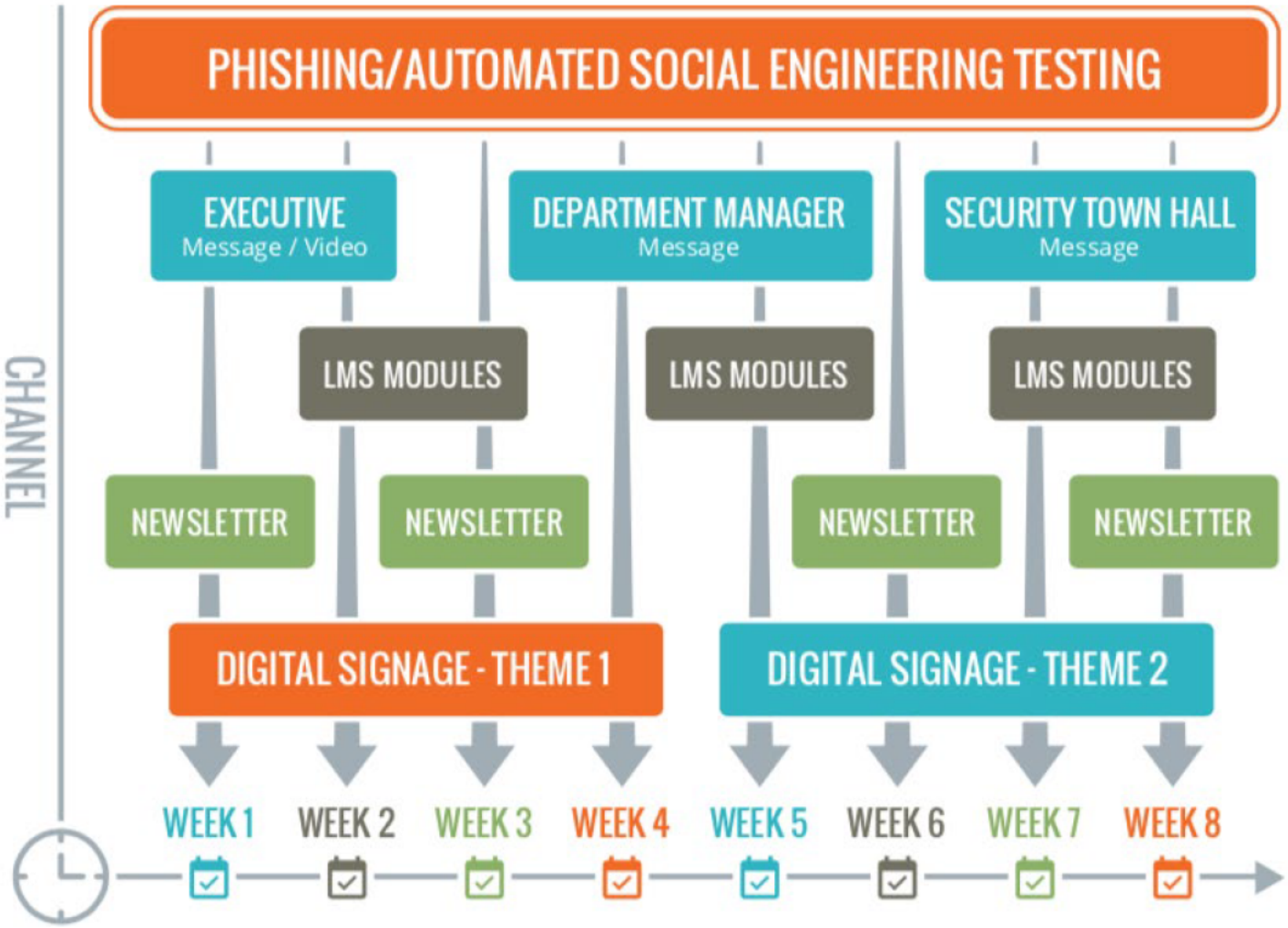
Building engagement and learning techniques

- Establish a baseline and work from there
- Determine where you are now through testing
- Make the lessons relatable
- Recruit leadership and some internal advocates to spread the message
- Have entertaining material that holds attention

Building engagement and learning techniques

- Phish and test people
- Use gamification to create a sense of competition and fun
- Review the Results
- Look for trends and areas that need improvement or that you want to emphasize

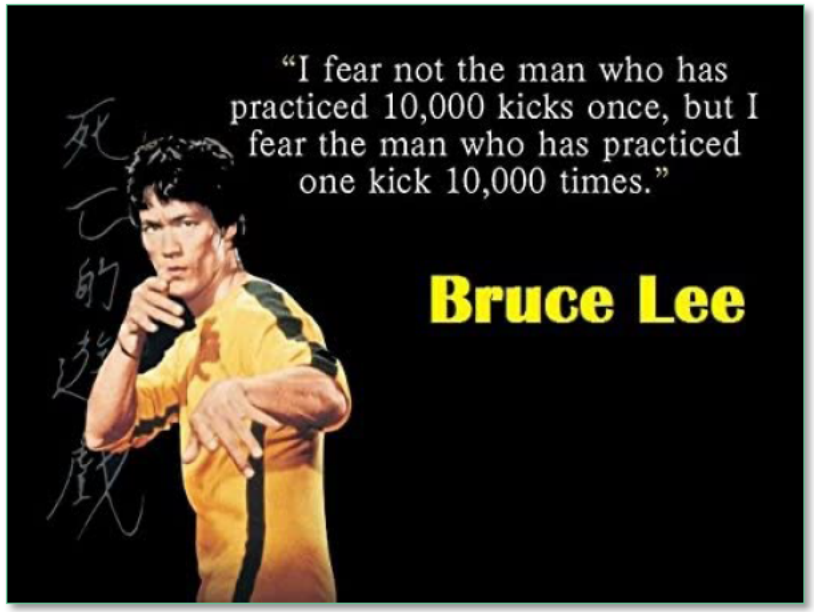
Coordinate Campaigns

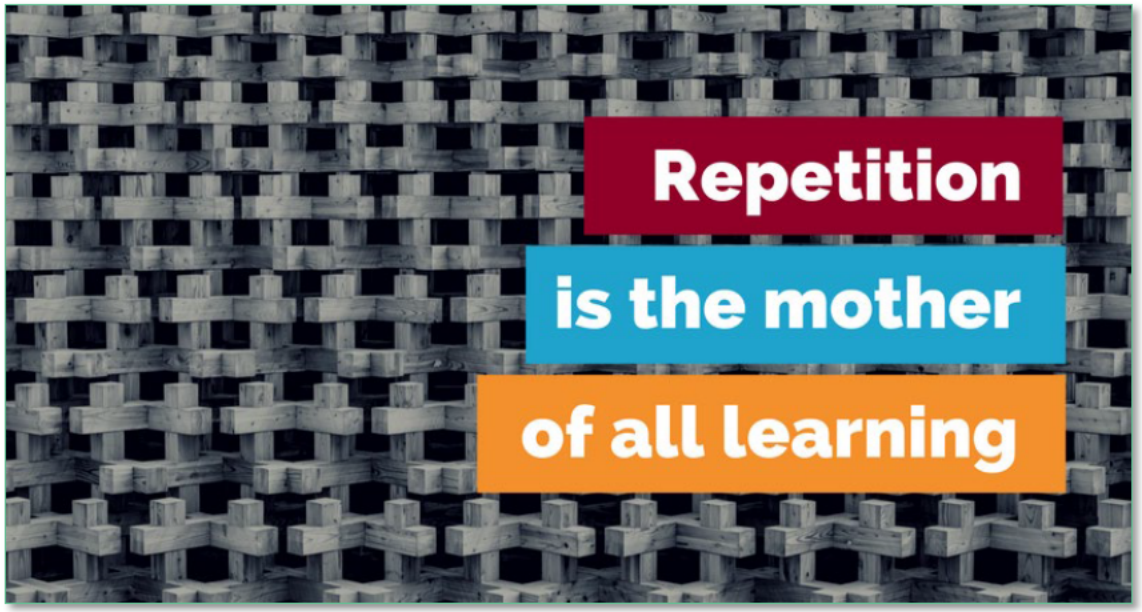


Run your security awareness program like a marketing campaign

Continuous testing while delivering targeted educational messages, training modules, and internal newsletters and digital signage will reinforce new behavior so your users become an effective last line of defense.

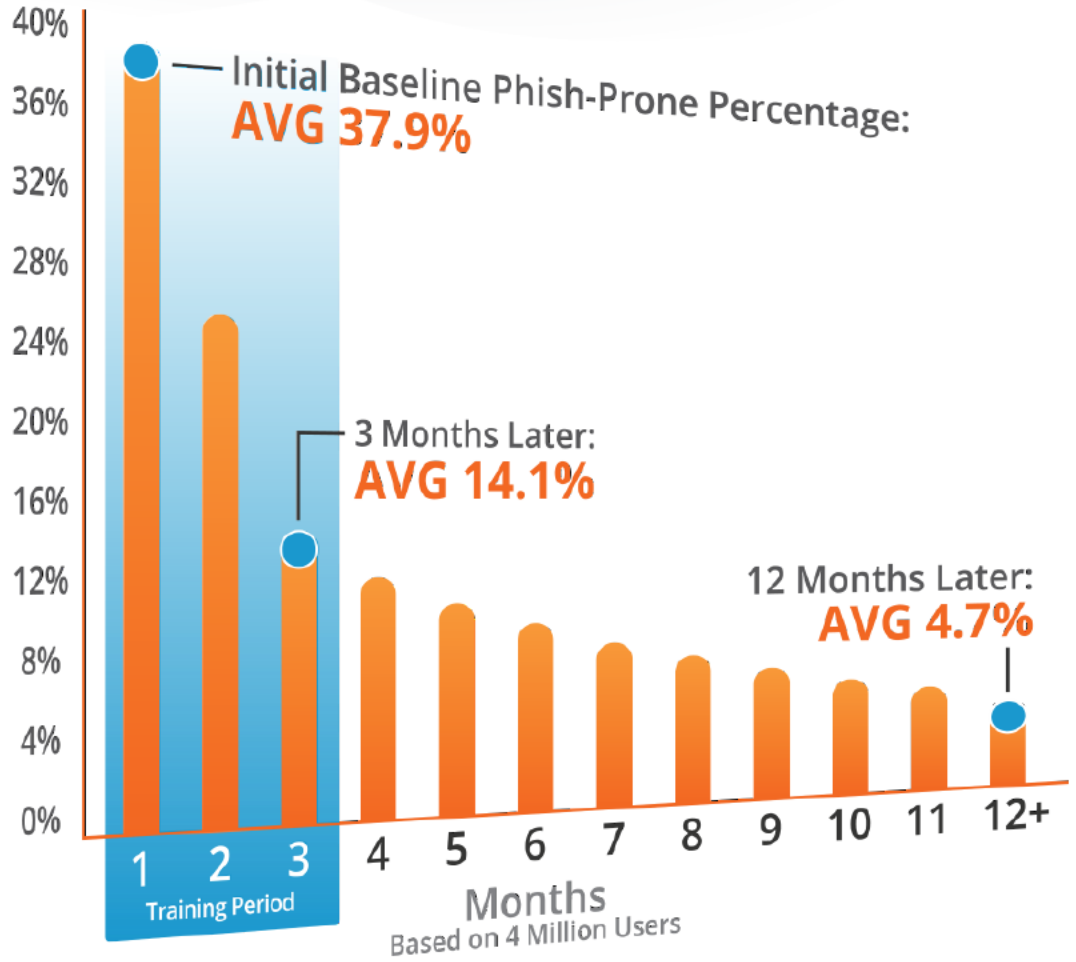
Repeat A Relevant Message





Understand What To Expect

- Expect a significant reduction at first followed by a gradual improvement
- Prepare a continuous campaign
- Don’t expect perfection, but deal with accidental clicks with grace



Takeaways

- Immediate
  - If you are not doing a formal awareness program, start one
  - Ask employees if there are any scams that concern them and include tips for avoiding falling victim- make the security team approachable
- Midterm
  - Work with marketing and HR groups to make the message relevant
  - Concentrate on attacks you are seeing
- Long Term
  - Make sure you are measuring progress so you can focus on results

Thank You!

Erich Kron – Security Awareness Advocate
ErichK@KnowBe4.com | @ErichKron

Javvad Malik – Security Awareness Advocate
JavvadM@KnowBe4.com | @J4vv4D