proofpoint®

I'm Still Waiting For My $10 Million. How About You?

Dale "Dr. Z" Zabriskie, CISSP CCSK
Evangelist, Security Awareness Training

My Favorite Nigerian 419 Scam

I am Mr. Ibrahim Mustafa Magu the chairman of ECONOMIC & FINANCIAL CRIME COMMISSION (EFCC) here in Nigeria. We have been working towards the eradication of fraudsters and scam Artists in Western part of Africa With the help of United States Government and the United Nations and some corrupt official administrators Mr Ibrahim Lamorde has been sacked who happen to be the former EFCC chairman.

My Favorite Nigerian 419 Scam

We have been able to recover so much money from these scam artists. The United Nation Anti-crime commission and the United State Government have ordered the money recovered from the Scammers to be shared among 100 Lucky people around the globe.

My Favorite Nigerian 419 Scam

This email is being directed to you because your email address was found in one of the scam Artists file and computer hard disk in our custody here in Nigeria and with the information gartered from this Scam artist, you notice that you have been scammed of so much money and have decided to compensate you with a **little token** to recover the lost of your fund.

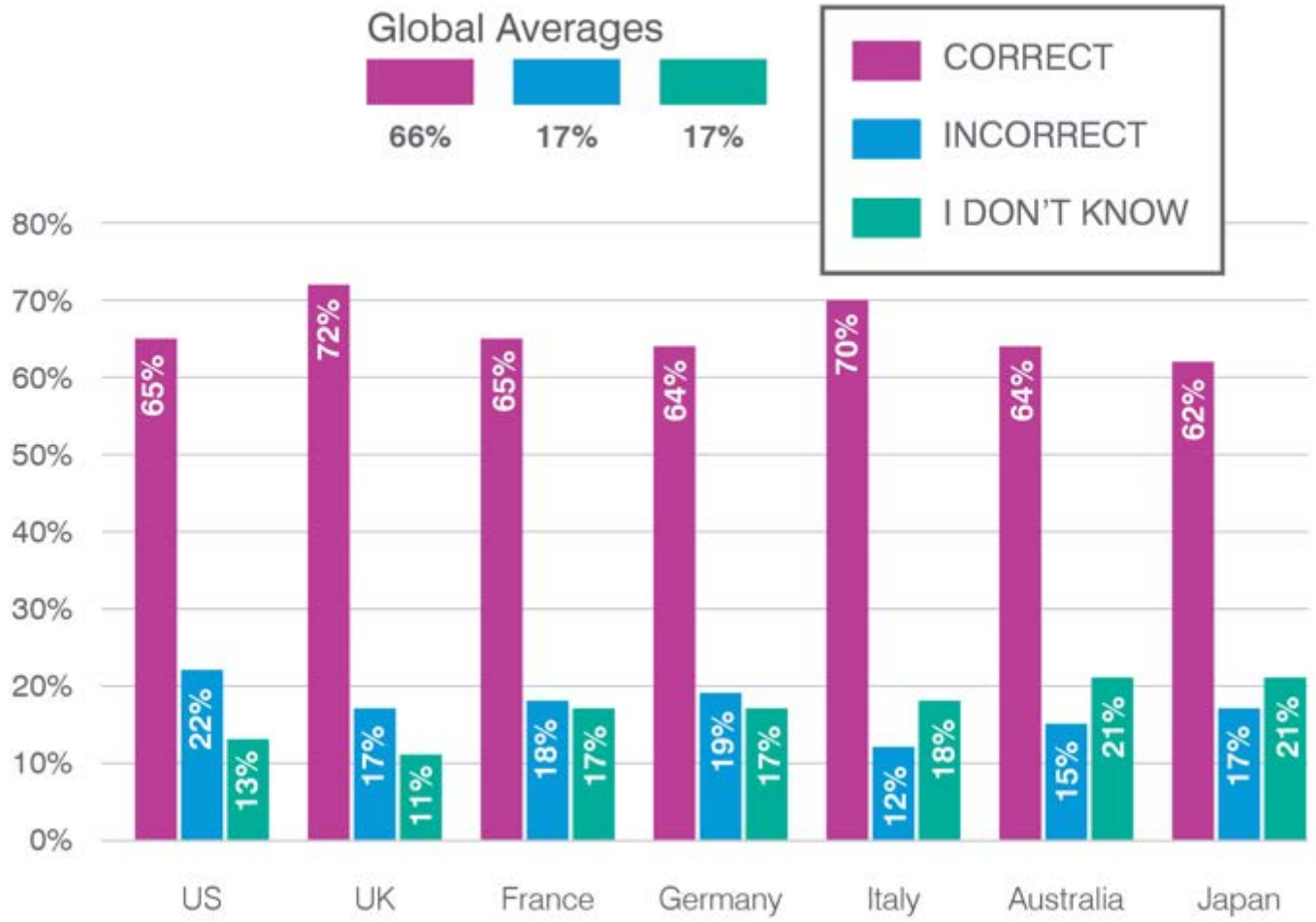
My Favorite Nigerian 419 Scam

You are therefore being compensated with the total sum

$ 2.5 Million Dollars.

Why are we on this journey?

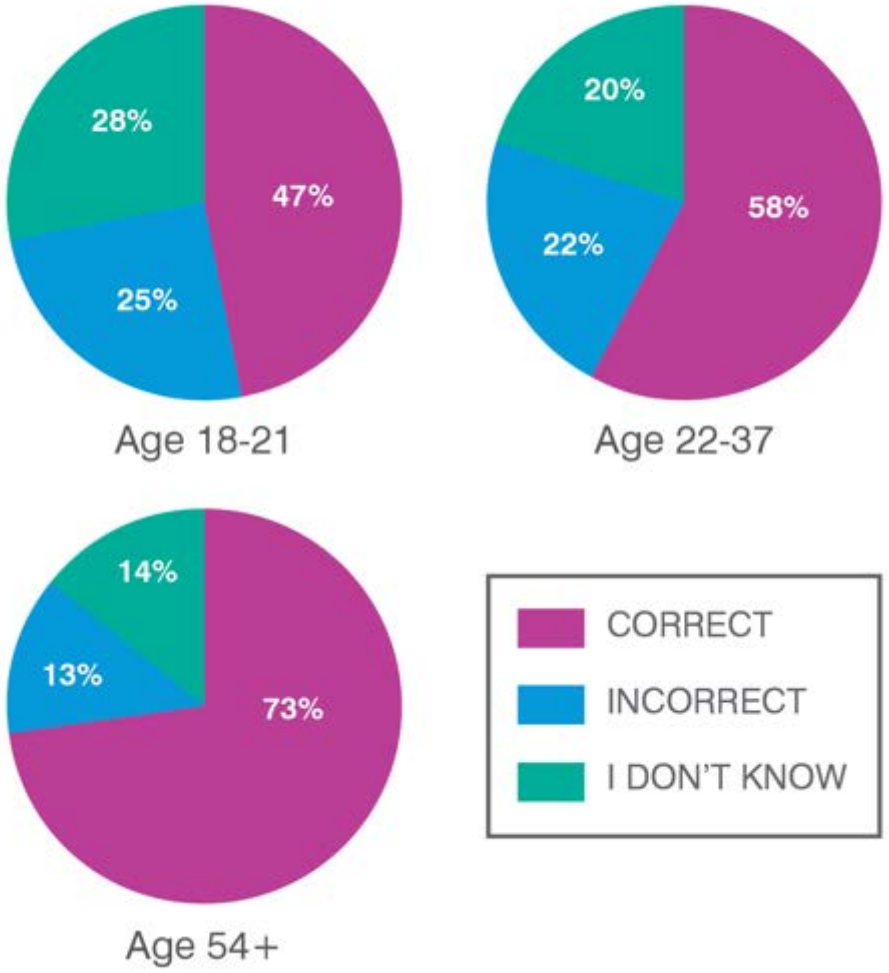
We Asked: What Is Phishing?



Between **30% and 40% of working adults** around the world were unable to identify the definition of phishing

proofpoint.

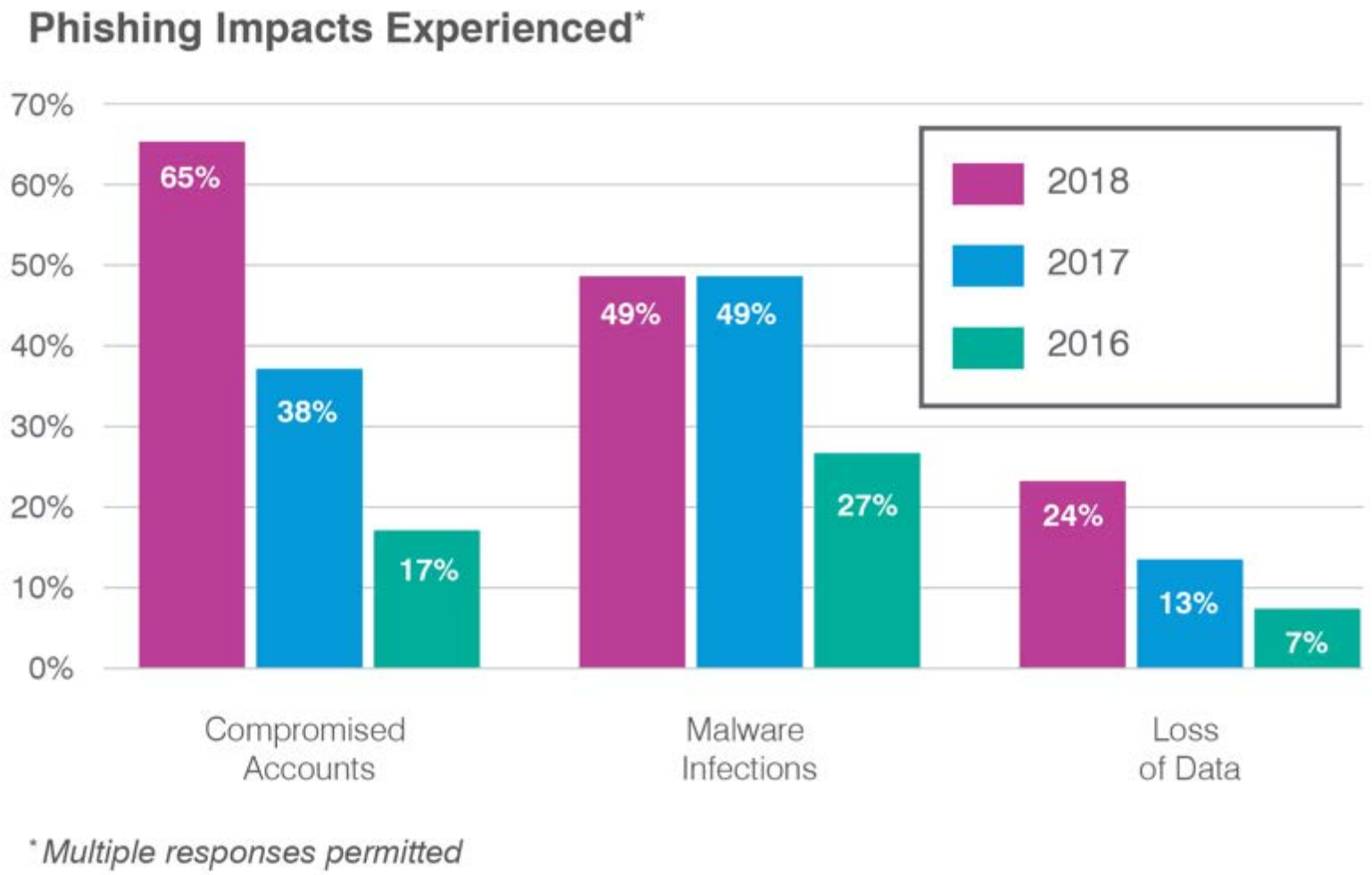
We Asked: What Is Phishing?



Baby boomers (54+) outperformed all others, including millennials (22-37)

proofpoint.

We Asked: What Impacts Are You Experiencing?



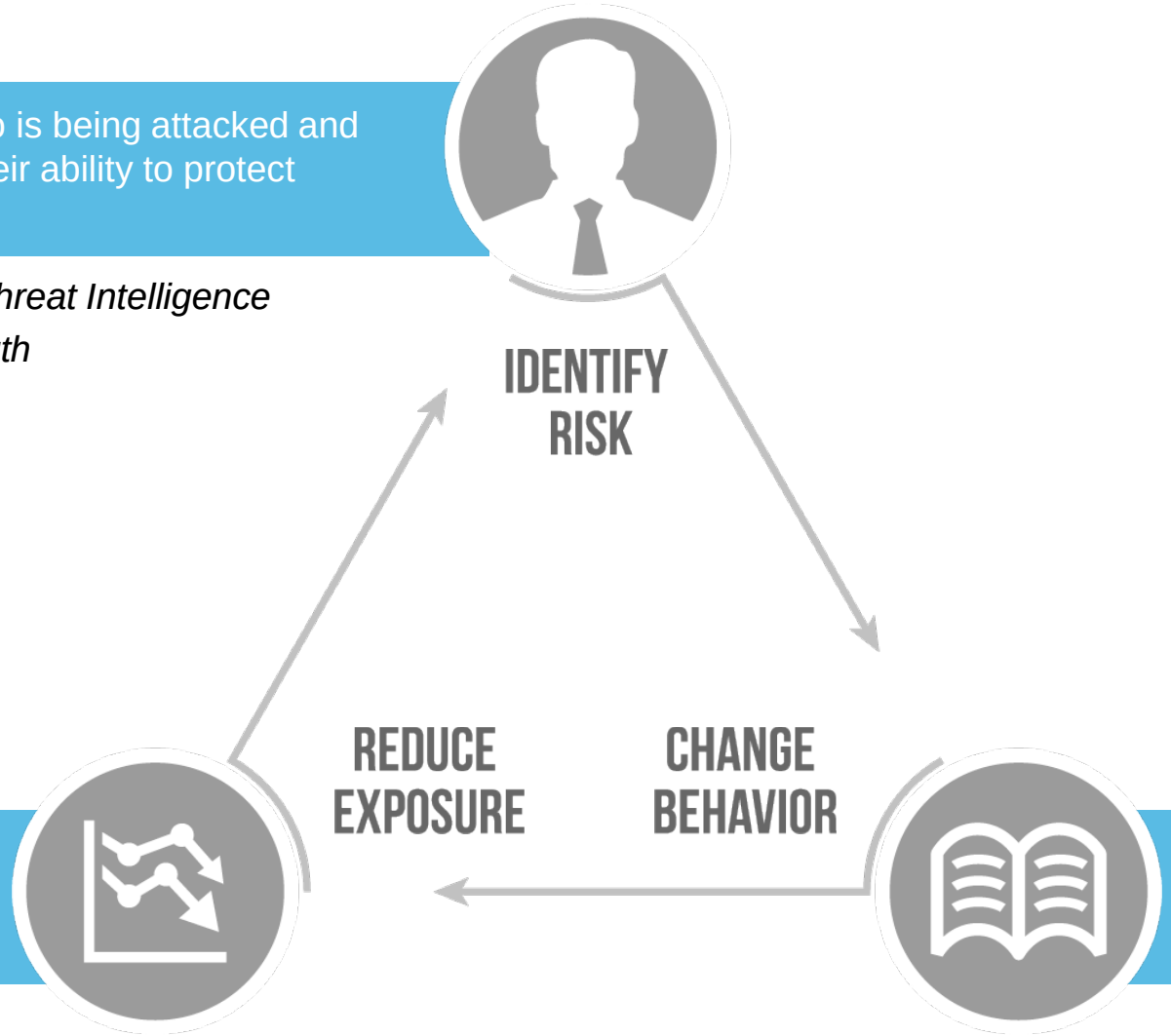
Credential compromise increased by **more than 280%** since 2016.

proofpoint.

People-centric Risk Reduction

Identify who is being attacked and evaluate their ability to protect themselves

Proofpoint Threat Intelligence
CyberStrength
ThreatSim



PhishAlarm
PhishAlarm Analyzer
Threat Response Auto-Pull (TRAP)

Knowledgeable end users report potential threats which reduces attack surface

Interactive Training
Awareness Videos and Materials

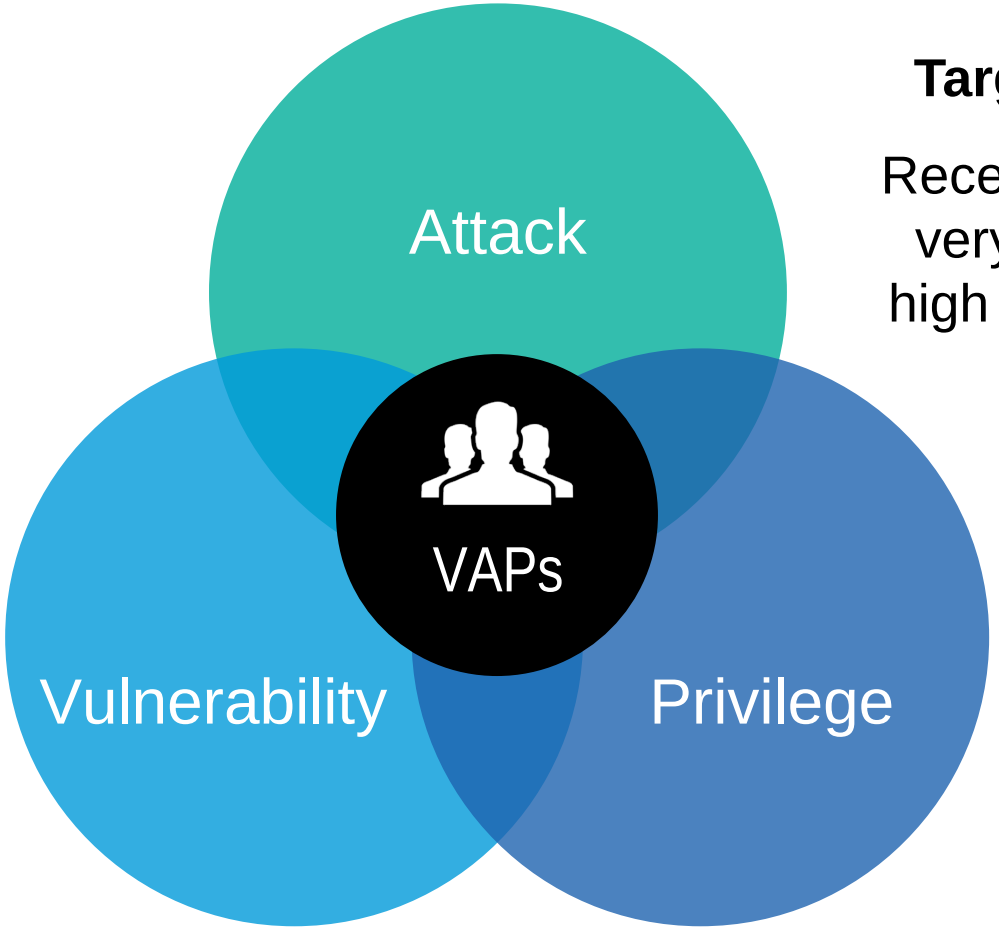
Deliver training based on actual threats, user behavior, and knowledge gaps

proofpoint.

Who are your VAPs?

Work in High Risk Ways

Clicks on malicious content, fails awareness training, or uses risky devices or cloud services



Targeted by Threats

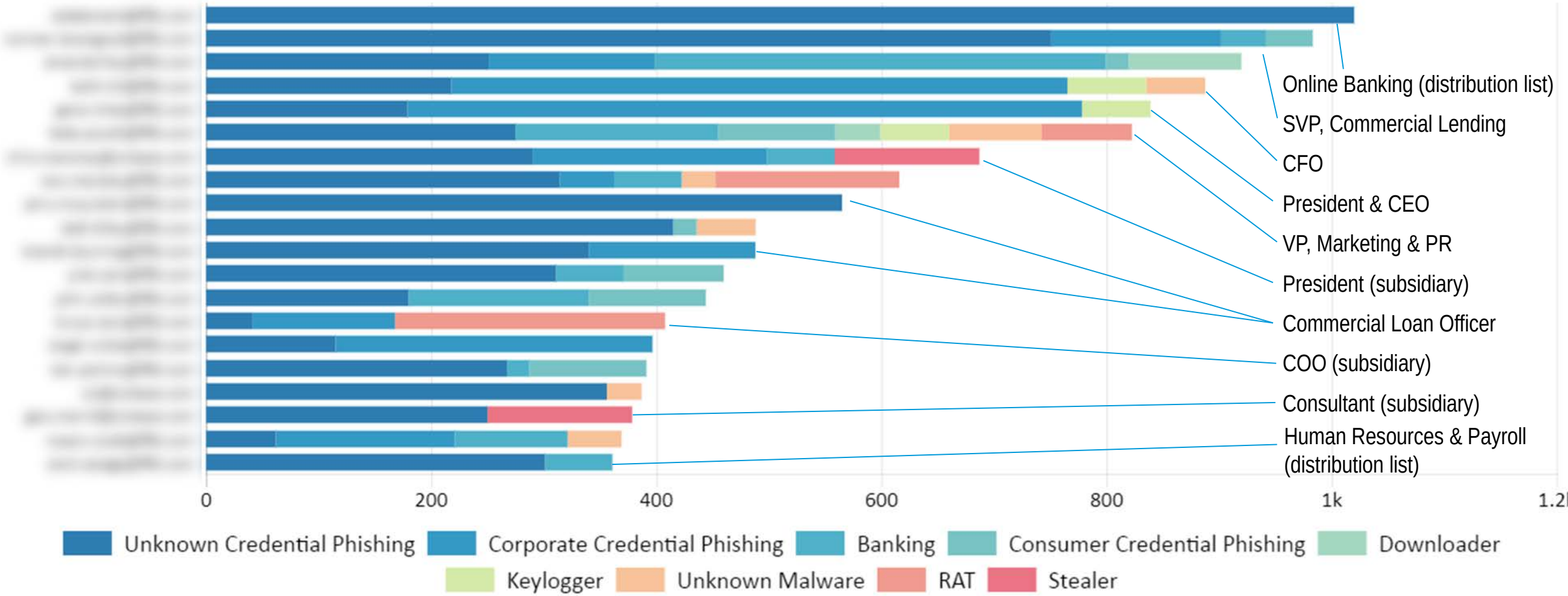
Receive highly targeted, very sophisticated, or high volumes of attacks

Access to Valuable Data

Can access or manage critical systems or sensitive data

Very Attacked People: Regional Bank

(Top 20 ranked by Attack Index)



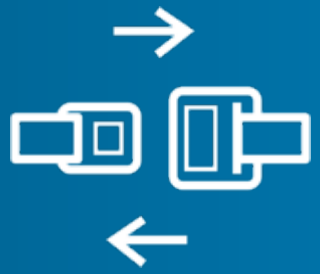
proofpoint.

Preflight Checklist

Effective Security Awareness Programs Include the Following:

- ✓Advanced discussions with stakeholders
- ✓Pre-launch testing and planning
- ✓Baseline vulnerability measurements
- ✓Introduction of cybersecurity training to employee base
- ✓Ongoing assessments
- ✓Clear, timely link between assessments and training
- ✓Regular, organization-wide education
- ✓Reinforcement of key messages and ongoing awareness activities
- ✓Consistent tracking and reporting
- ✓Clear communications and status updates
- ✓Motivational component
- ✓Culture of security

proofpoint.



Prepare for Takeoff

Prepare for Takeoff

- Why are you running a program?
  - Educating people to make them smart enough is NOT the purpose
  - Trying to trick people is NOT the purpose
- Asking the right questions is key – Don’t assume
- Know what your tools can and cannot do
- Share information about the program selectively
- Take a hard look at how you group and segment your users
- Determine the topics – Define the metrics

Down the Runway

Down the Runway

- Consider a Beta launch. It helps you…
  - Identify unforeseen issues
  - Provide benchmark data
  - Sell the program
- Start with “blind” Phishing Simulations
  - Choose a template or craft an email that is of moderate difficulty
  - Avoid language that could be concerning and is globally “neutral”
  - Keep the list of “those in the know” as short as possible.
  - Do NOT provide immediate feedback to the users that click. No “teachable moment”
- After the “blind”, communicate your results
- As you socialize the program, focus on benefits over features

In the Air

In the Air

- Plan for phishing simulations every four to six weeks
  - Determine what your culture can tolerate
- Start with a moderately easy phish and gradually increase the difficulty as your users improve
- Pair simulated attacks with a “teachable moment” that engages the user if/when they click.
- Give users a simple way to report suspected phishing attempts
- Use Auto-enroll capability to assign follow-up training for users that fail simulated attacks
- Reinforce the message with awareness materials
- Redo a “blind” periodically – Helps reset the baseline

proofpoint.

Adjusting your Pitch, Roll, and Yaw

Pitch, Roll, and Yaw: Corrections to stay on path

- Tracking and Reporting – Measurement is the key to success!
  - Numbers of active malware infections
  - Rates of successful external phishing attacks
  - Downtime hours for end users following a malware infection, successful phishing attack, or misplaced/stolen device
  - Hours and resources tied to remediation of devices following user mistakes
  - The quantity and quality of calls fielded by your IT helpdesk
  - Numbers of suspicious emails reported by your users
- Vary the approach to your simulations
  - Link based, attachments, credential, etc.
- Keep it fresh and relevant
  - Repurpose threats you are seeing in your own environment
  - Use current/company events as a phishing template e.g.: Tax season, Cultural, etc.
  - Consider introducing smishing and USB simulation

Pitch, Roll, and Yaw: Motivational Techniques

- Gamification can engage and motivate users
  - Competition between departments or groups
  - Offer rewards based on score or timeliness
  - Scale your gamification to your corporate culture
  - Look for champions in departments/groups
- Emphasize the value to users outside of work
  - Good personal security protects the enterprise

Pitch, Roll, and Yaw: Consequence Models

- Consequence Models
  - Be very thoughtful about using a consequence model
  - Include HR and legal teams
  - Gauge effectiveness
  - Above all, don’t make it negative

Wrap up – Dealing with Headwinds and Tailwinds

- Every end user interaction tells you something
- NOT clicking is a GOOD thing
- Reported phishes (real or simulated) are the best metric
- Be a marketeer

proofpoint®