



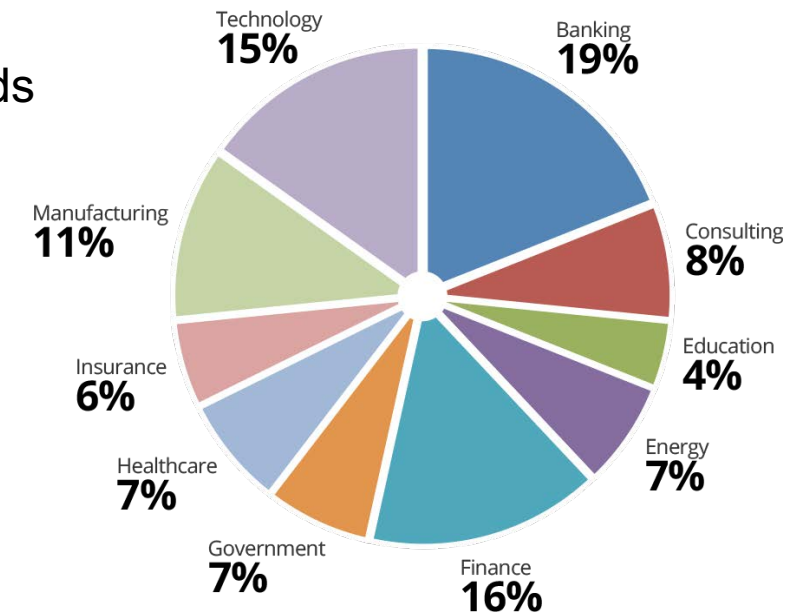
# Think Like a Hacker: Learn How to Use OSINT to Defend Your Organization

**Rosa L. Smothers**  
SVP of Cyber Operations



# KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



# Agenda

- Secure Set Up to Conduct OSINT Investigations
- Language and Culture
- How and Where to Conduct Searches
- Locations and Images
- Apps and Tools



# Safety First



# Secure Your Setup Before Any Investigation

Hardware/Software or Cloud-Based

- Dedicated Machine
- Disk Wiper
- Virtual Machine
- VPN
- Amazon Lightsail, MS Azure portal, Google Cloud, etc.
- Virtual Machine instance(s)
- VPN

# Personas



# All About the Bona Fides

Create Your Persona(s)

- Social Media profile
- Image
- Robust and Consistent Background
- Aged Profile

2,160,005 free AI generated photos

## Select Photos

- ☐ All 2,160,005 with current filter
- ☐ Random 100
- ☐ All 30 on this page

## Background Color

## Face

- ☒ All
- ☐ Natural NEW
- ☐ Beautified

## Head Pose

## Sex

## Age

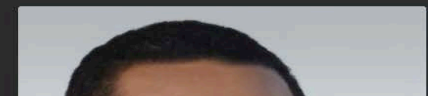
## Ethnicity

## Eye Color

## Hair Color

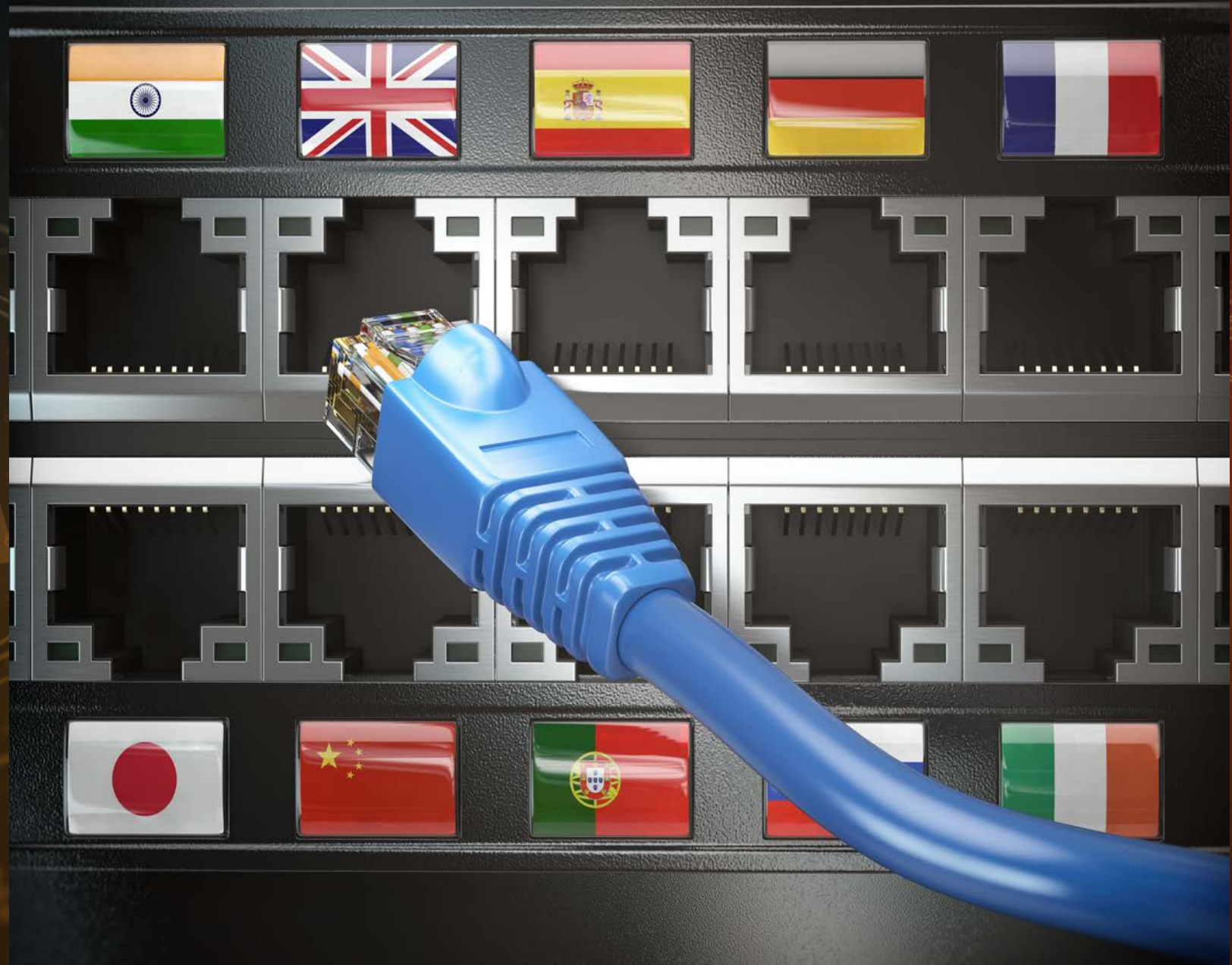
## Hair Length

## Emotion





# Think Like the Adversary

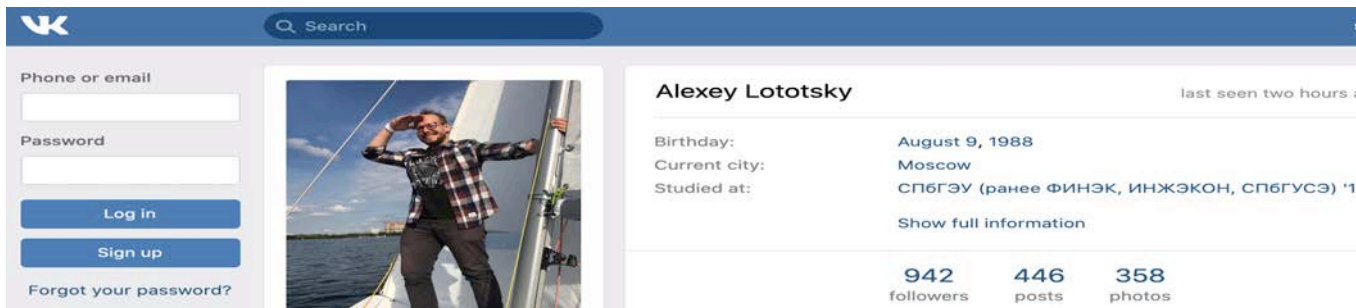




# “It’s What I’d Do/Say/Think...”

Avoid Mirror Imaging

- Social Media Platforms Based Upon Culture
- Persona’s Image
- Social Media Connections/Interest Groups



大家正在搜: 山西襄汾县... Q

weibo | 微博

精选

交友

企业

好莱坞

房产

旅游

时尚



# Watch Your Language

amaste مرحبا Willkomm Bem Vindo Selam  
Namaste Croeso Willkommen  
Bienvenue Bienvenue Welcome Bienvenidos وسهلا  
ut om nue  
venidos مرحبا Welcome Welkom Croe  
Nam  
atang أهلا وسهلا مرحبا  
ome  
Benvenuti Willkommen Selamat Datang Croeso Bem  
Benvenuti  
дошъл  
Καλώς ήλθατε

# The ABCs (or АБВЫ or اَبْت...) of Investigating Accounts

Linguistic and Cultural Context is Key

- Social Media Platforms Based Upon Culture
- Persona's Image
- Use of Language

vputin@yandex.ru ≠ впутин@яндекс.ру

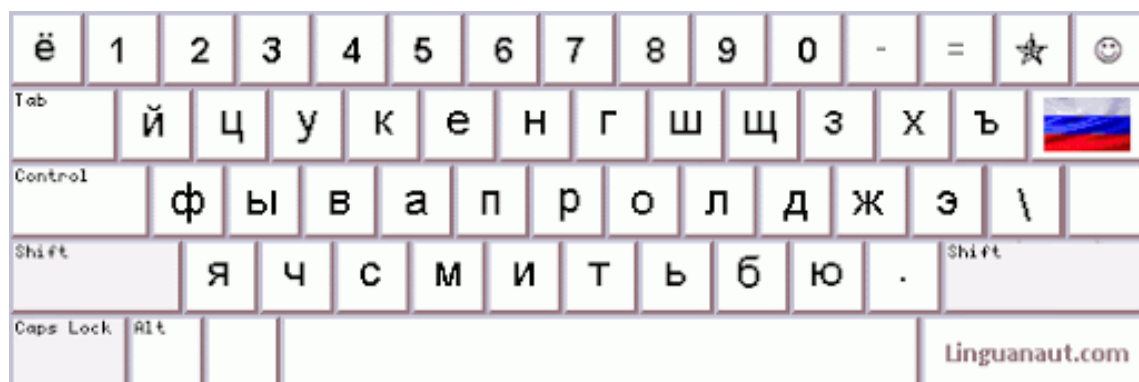
balassad@syriantelecom.com.sy ≠ بشار الأسد@syriantelecom.com.sy



# The ABCs (or АБВЫ or اَبْت...) of Investigating Accounts

Linguistic and Cultural Context is Key

- Usernames are often a “tell”



Jabwthac,@yandex.ru

Офицерфсб@yandex.ru



Hojvhrq;@zain.com

اختر اقلك@zain.com

# The ABCs (or АБВЫ or اَبْت...) of Investigating Accounts

## Username

























- Naming Conventions
- Numbers in a username often birthdate of user or their children
- Can indicate interest (sports or pop culture reference)

Domain Search

hunter.io Hunter ↗ 🔍

☒ All ☐ Personal ☐ Generic 8 results [Export in CSV](#)

Most common pattern: {first}@hunter.io 🔍 Find someone...

Giovanni Lepori Customer Success 	  3 sources 
<b>giovanni@hunter.io</b> 	
Mirko Rakic Software Engineer	  3 sources 
<b>mirko@hunter.io</b> 	
Bastien Libersa Software Engineer 	  3 sources 
<b>bastien@hunter.io</b> 	
Francois Grante Cofounder 	  8 sources 
<b>francois@hunter.io</b> 	
Antoine Finkelstein Cofounder 	  7 sources 
<b>antoine@hunter.io</b> 	

# Pattern of Life

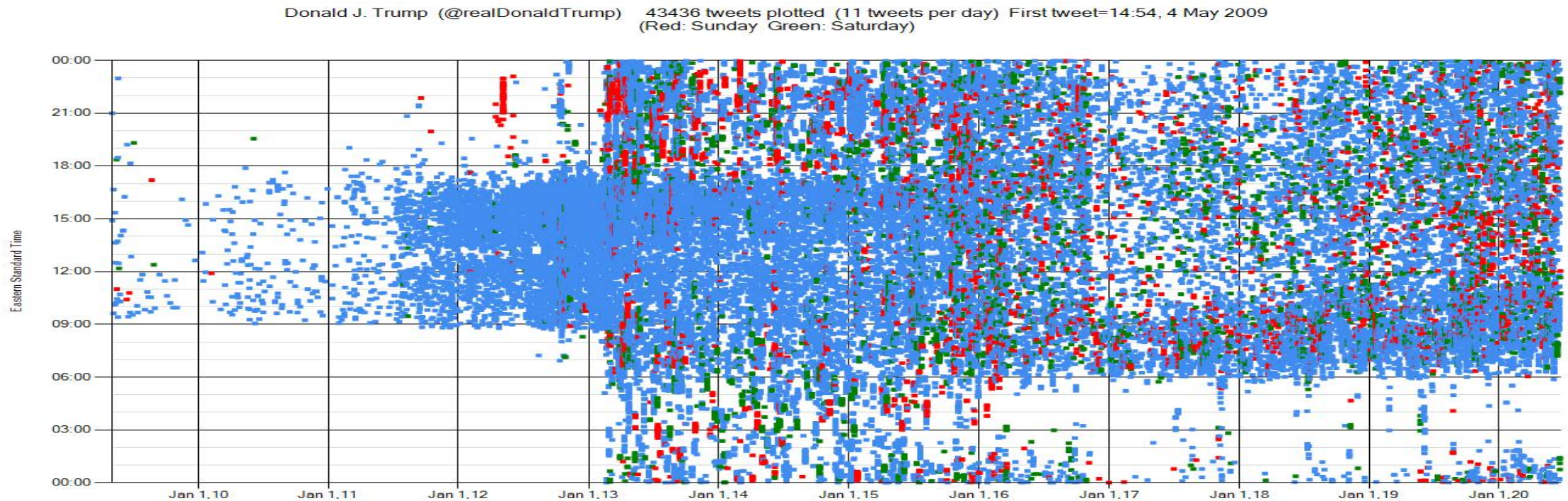




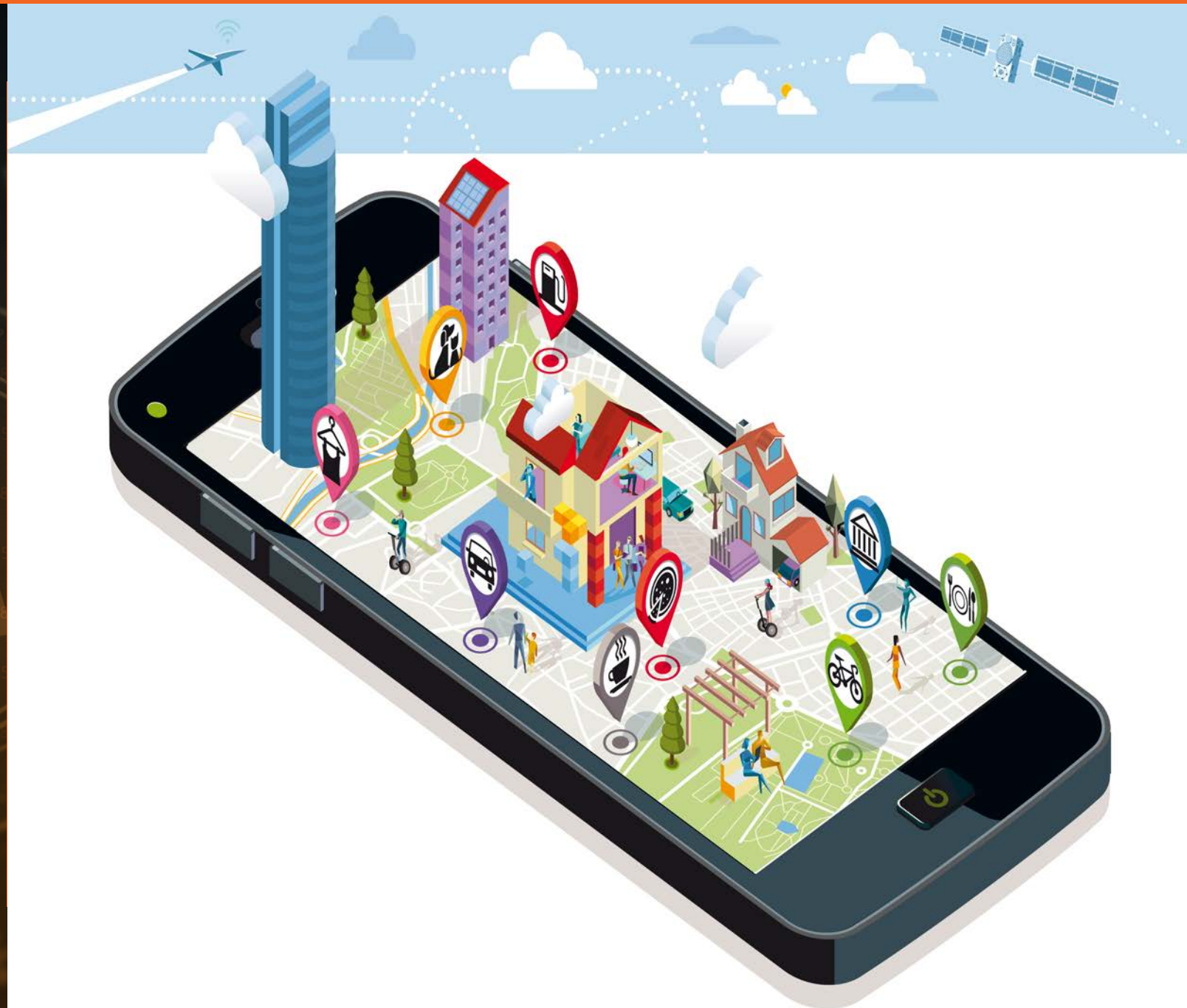
# Time After Time

Date and Time is an Indicator

- **Pattern-of-life analysis** is a method of observation specifically used for documenting or understanding a subject's habits



# Locations & Images





# Location, Location, Location

- Aerial Analysis

What time is it?

What is today?

What season is it?

What can be expected tomorrow?

What type of industry drives this economy?

Where are we?





# A Photo Says a Thousand Words

- Photo Analysis

Meta data

Clone detection

Magnification/Zoom to detect miniscule details

Principal Component Analysis (PCA)



\*[https://www.cia.gov/kids-page/games/games\\_aerial\\_analysis.html](https://www.cia.gov/kids-page/games/games_aerial_analysis.html)

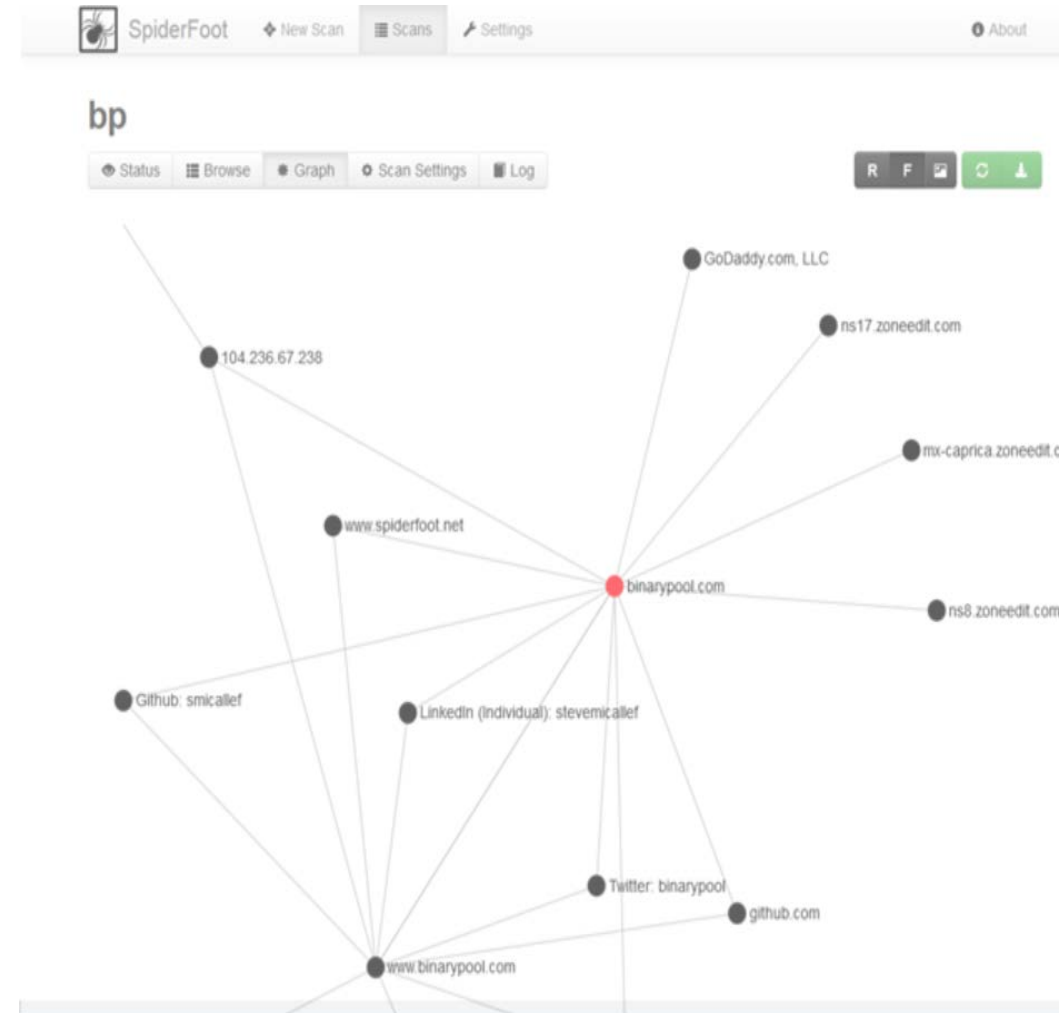
# Apps & Tools



# The Right Tool for the Right Job

Plenty of Options, Some Only Dependent upon OS of Choice

- Multiple Search Engines
  - Google Hacking DB
  - Shodan – device discovery
  - Contextualwebsearch.com
- Public Databases
  - Property Records
  - Open S3 Buckets
- Dark Web Data Breaches
- Data Visualization
- GitHub (.py)
  - PaGoDo, Tweepy,





# The KnowBe4 Security Awareness Program WORKS



## Baseline Testing

Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.



## Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.



## Phish Your Users

Best-in-class, 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!



# Security Awareness Training Program That Works

- 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)

## Visible Proof the KnowBe4 System Works



# Resources

## Free IT Security Tools



Domain Doppelgänger



Awareness Program Builder



Domain Spoof Tool



Mailserver Security Assessment



Phish Alert



Ransomware Simulator



Weak Password Test



Phishing Security Test



Second Chance



Email Exposure Check Pro

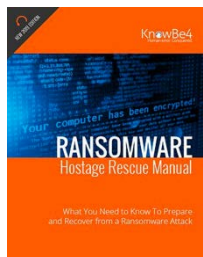


Training Preview



Breached Password Test

## Whitepapers



### Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.



### CEO Fraud Prevention Manual

CEO fraud is responsible for over \$3 billion in losses. Don't be next. The CEO Fraud Prevention 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.



### 12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

» Learn More at [www.KnowBe4.com/Resources](http://www.KnowBe4.com/Resources) «





# TIME FOR QUESTIONS



**KnowBe4**  
Human error. Conquered.

**Know more about KnowBe4.**

**Contact: Rosa L. Smothers**  
(727) 748-4199  
[rosas@knowbe4.com](mailto:rosas@knowbe4.com)



Thank You!

**KnowBe4**  
Human error. Conquered.

**Know more about KnowBe4.**

**Contact: Rosa L. Smothers**  
(727) 748-4199  
[rosas@knowbe4.com](mailto:rosas@knowbe4.com)