RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: HUM-R04

COMPROMISING FORTUNE 500 BUSINESSES WITHOUT HACKING A THING!

Rachel Tobac

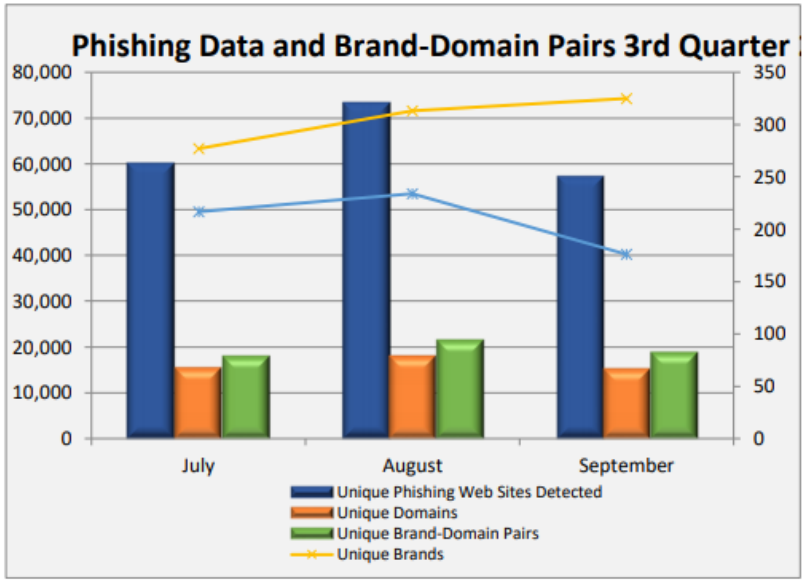
CEO, SocialProof Security
UX Research, Course Hero
@RachelTobac / @socialproofsec

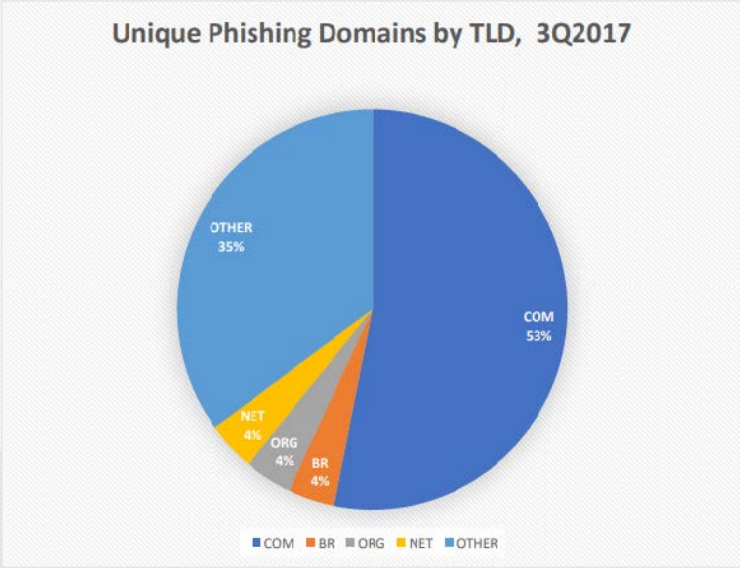
Joe Gray

Senior Security Architect, IBM
@C_3PJoe / @advpersistsec /
@hackingglass

The Cold Hard Facts

Phishing Statistics





Source: APWG 3Q2017 Report

Statistic Highlights

Statistical Highlights for 3rd Quarter 2017

	July	August	September
Number of unique phishing websites detected	60,232	73,393	57,317
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	99,024	99,172	98,012
Number of brands targeted by phishing campaigns	277	313	325

Source: APWG 3Q2017 Report

About Rachel @RachelTobac

SOCIAL PROOF SECURITY

@RachelTobac

About Joe

DERBYCON VII (2017) CLOSING CEREMONY

Chris Hadnagy presenting me with the Trophy

Apply! What will you learn today?

- OSINT concepts and how they lead to social engineering (SE) attacks
- Common social engineering attack methods
- How we won SECTFs
- Examples of what social engineering sounds like
- How to get your organization prepared for SE

HOW WE DO OPEN SOURCE INTELLIGENCE

OSINT against the business and its users

Advanced Persistent Security

What is OSINT?

Publicly available material:

- The Internet
- Traditional mass media
- Specialized journals, conference proceedings, and think tank studies
- Photos
- Geospatial information
- Social media

What OSINT info do SEs target?

- VPN
- ESSID name
- Make and model of computer
- OS info + service pack/version
- PDF reader
- Browser and version
- Mail client
- Disk encryption
- Any/all software/versions

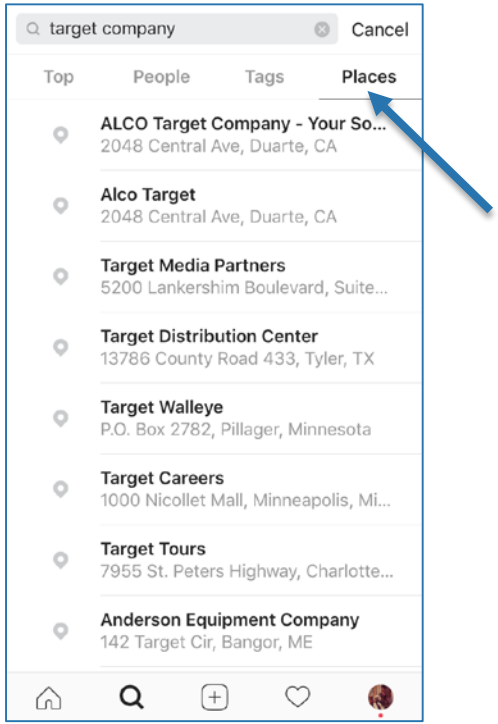
How I use social media for most OSINT

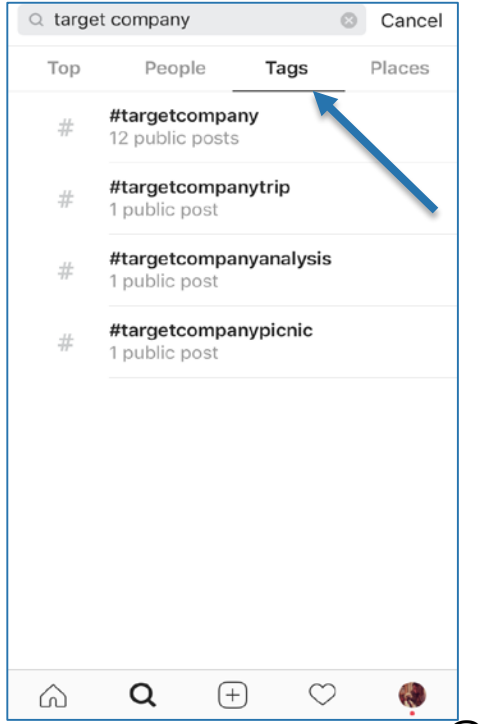





SOCIAL PROOF SECURITY

Instagram OSINT Example

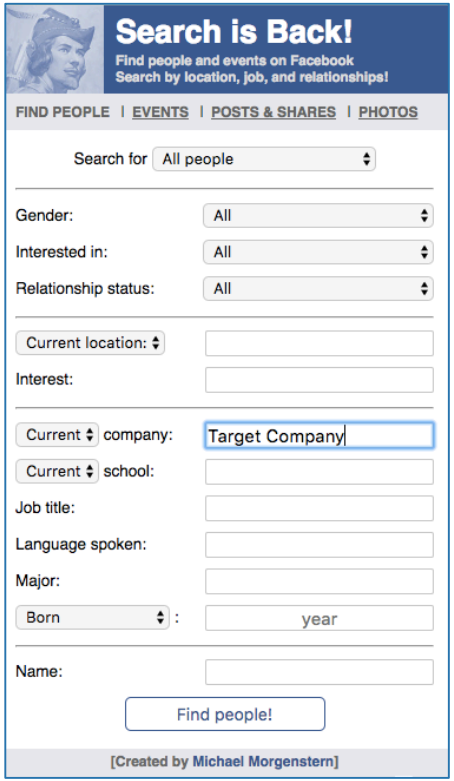


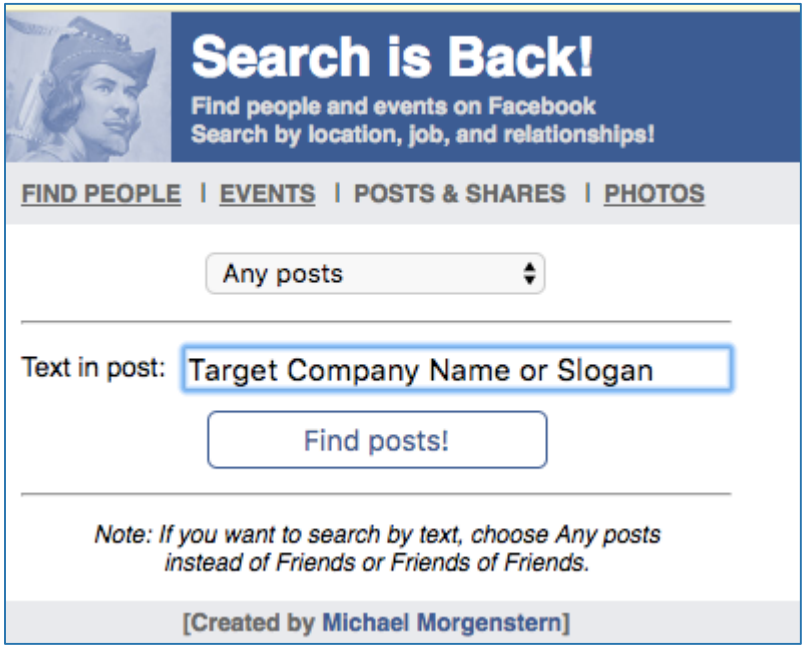


SOCIAL PROOF SECURITY

@RachelTobac

Facebook OSINT Example

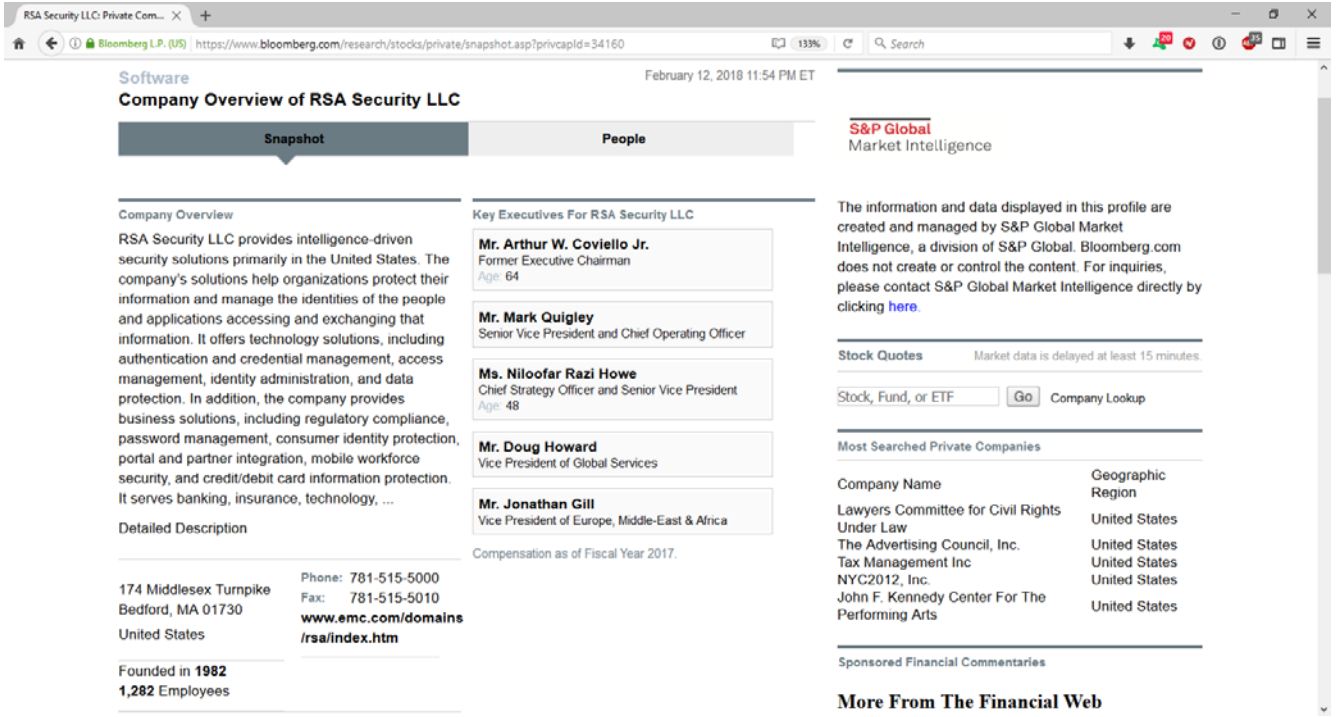




SOCIAL PROOF SECURITY

@RachelTobac

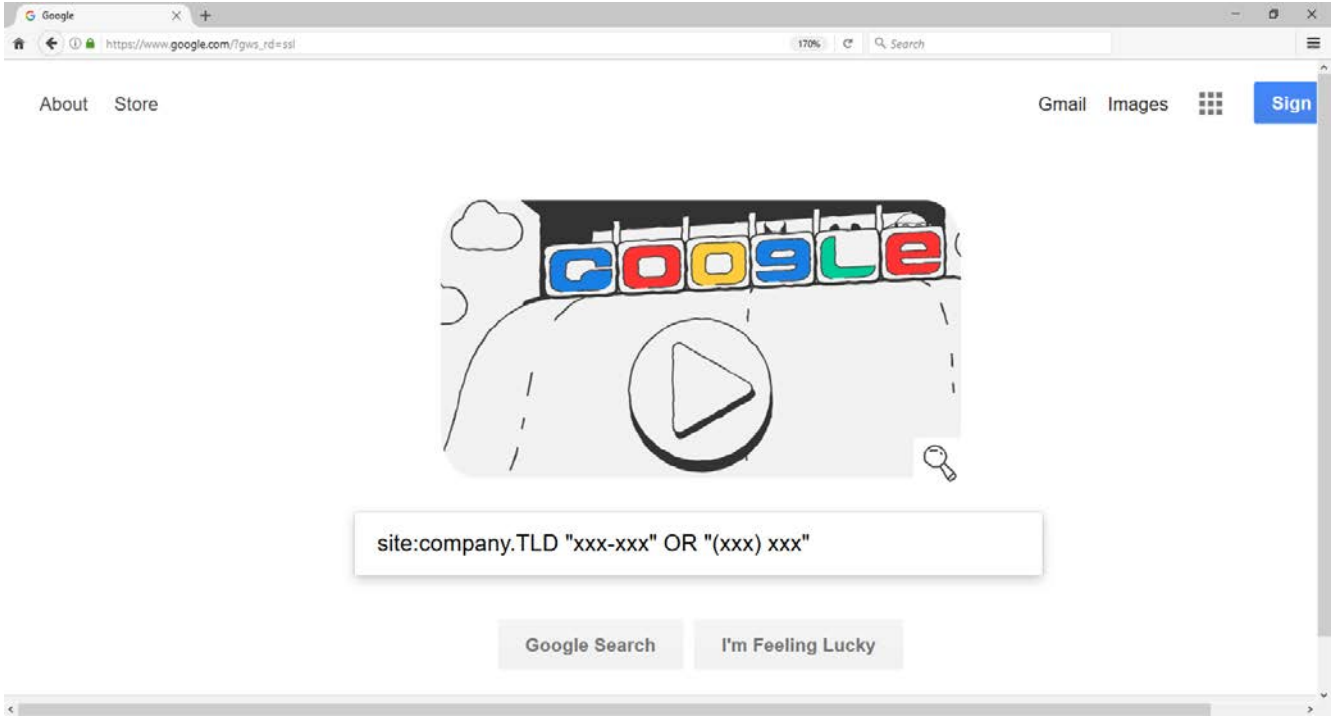
Gaining Initial Information



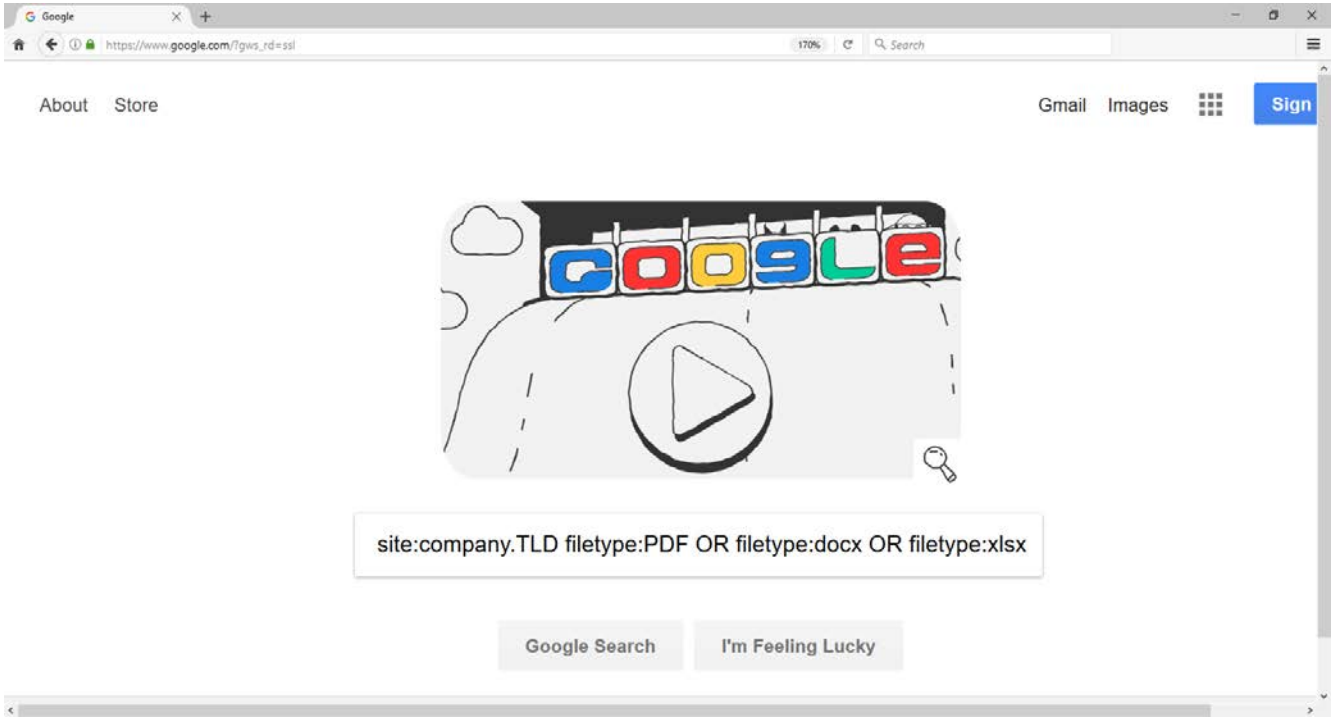
OSINT for Phone Numbers

- Block your number and sweep the organization
- Call outside hours to get names from voicemail
- If you find the directory, search for common last names

Google-Fu


Google
https://www.google.com/?gws_rd=ssl
170%
Search
About
Store
Gmail
Images
Sign
site:company.TLD "xxx-xxx" OR "(xxx) xxx"
Google Search
I'm Feeling Lucky

Google-Fu Next Step



Finding Info on People

- Build a repository of people
- Enumerate the people

Finding Info on People Continued

- See what user names they use
- Look for goldmines
- Use this data to build dossiers and leverage it to build rapport

About the domains

- Enumerate information about domains
  - Subdomains
  - MX records
  - SPF
  - Technologies used
    - Remote.target.tld
    - VPN.target.tld

We Take a Tour

How do SEs use these data points later?

SOCIAL PROOF SECURITY

SOCIAL ENGINEERING

Any act that convinces someone to do something that may or may not be in their best interest.

@RachelTobac

Picking Targets

- I vish the phone numbers I can find
- 3rd party vendors posting and tagging you
- You help people? You're getting a call
- You posted on social media about your company

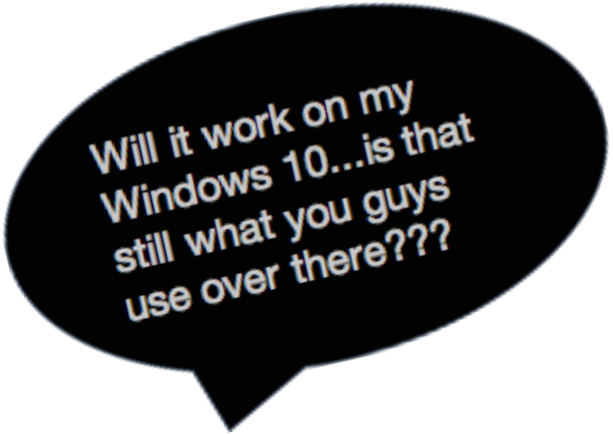
Picking Pretexts

SOCIAL PROOF SECURITY

Why does SE work on people so well?

- **Cialdini's 6 Principles of Persuasion:**
  - Reciprocity
  - Commitment & Consistency
  - Social Proof
  - Liking
  - Authority
  - Scarcity

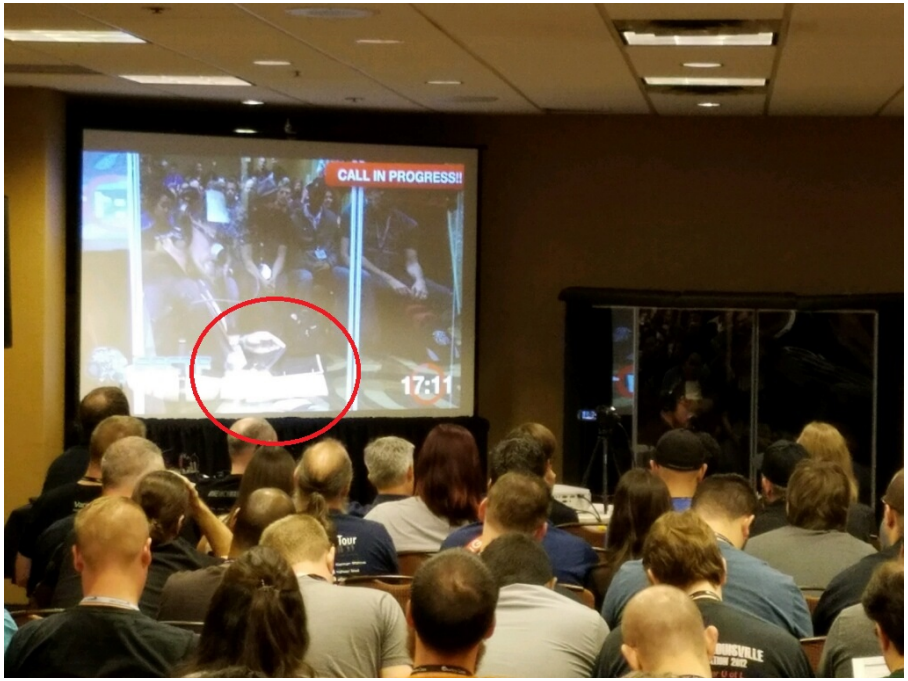
DEFCON SE calls



SOCIAL PROOF SECURITY

@RachelTobac

Derbycon SE Calls



Props

- Office Noises
- Uniforms
- Toolboxes
- Ladders
- Donuts and/or Coffee
- Badges

BRINGING IT ALL TOGETHER: NEXT STEPS

Emoji Takeaways

SOCIAL PROOF SECURITY

Training should be timely

Tips for Training

- Do more than the annual training for compliance purposes
- Employ role based training
- Integrate into Incident Response Plan
- Use automated solutions or external contractors to attempt attacks
- Ensure social engineering (specifically phishing, pretexting, and vishing) are included in your penetration tests

Applying what you've learned

- Next week you should:
  - OSINT survey on your company
  - talk with management about SE
  - talk with IR team for integration
- In the first three months following this presentation you should:
  - quarterly training scheduled in a shorter format
  - baseline phishing simulation
- Within six months you should:
  - adapt training to current trends and testing results
  - have a second training session
  - OSINT survey and Social Engineering pentest

Resources

- https://github.com/jocephus/RSAC_Resources/

QUESTIONS?

@racheltobac
@C_3PJoe