Social Media Best Practices

NCMS Brown Bag Seminar

Best Practices Committee

December 9, 2015

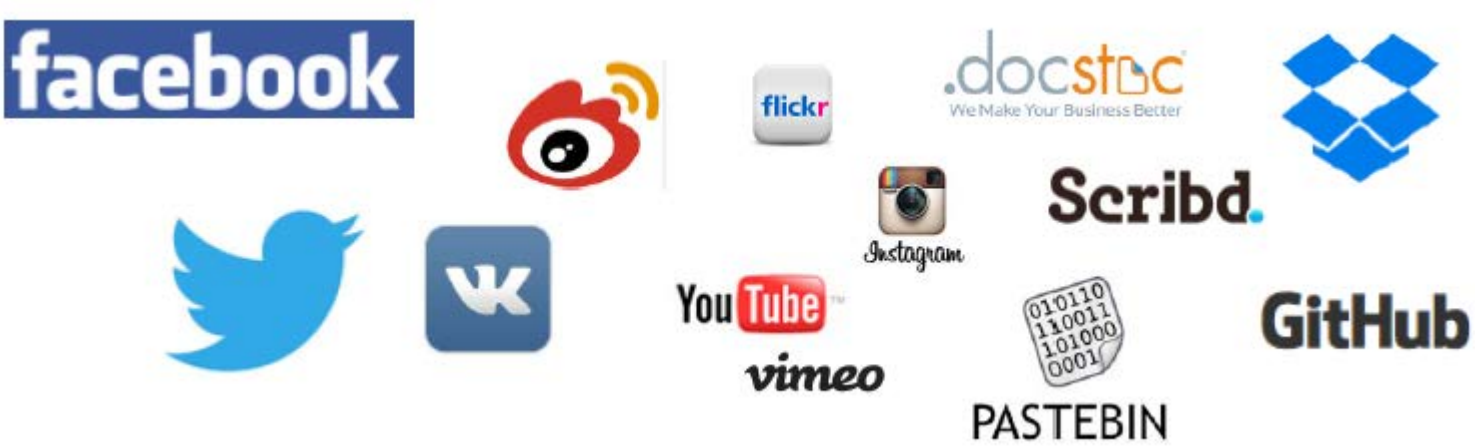
Objectives

- Recent Headlines
- Breadth & Depth of Social Media Today
- Spying on the Internet and the Threat of Social Media
- Case Studies
- What should I do?
- Resources
- Questions

The Social Media Revolution

""We want to connect everyone in the world and give people the tools to share whatever they want"

-- Mark Zuckerburg, Facebook CEO, Sept. 2013



How much of a priority is security when you are "connecting" everyone in the world?

Recent Headlines

China reportedly compiling 'Facebook' of U.S. government employees

By Catherine Herridge, Matthew Dean Published September 16, 2015
FoxNews.com

LinkedIn Sockpuppets Are Targeting Security Researchers

25 million affected by OPM hack, sources tell ABC News

BY JENNIFER DONELAN, ABC NEWS | THURSDAY, JULY 9TH 2015

LinkedIn serves up resumes of 27,000 US intelligence personnel

A new transparency project has mined LinkedIn to create a database of the US intelligence community, complete with codewords.

By Rob O'Neill | May 6, 2015 -- 21:14 GMT (14:14 PDT) | Topic: Security

U.S. investigating report email account linked to CIA director hacked

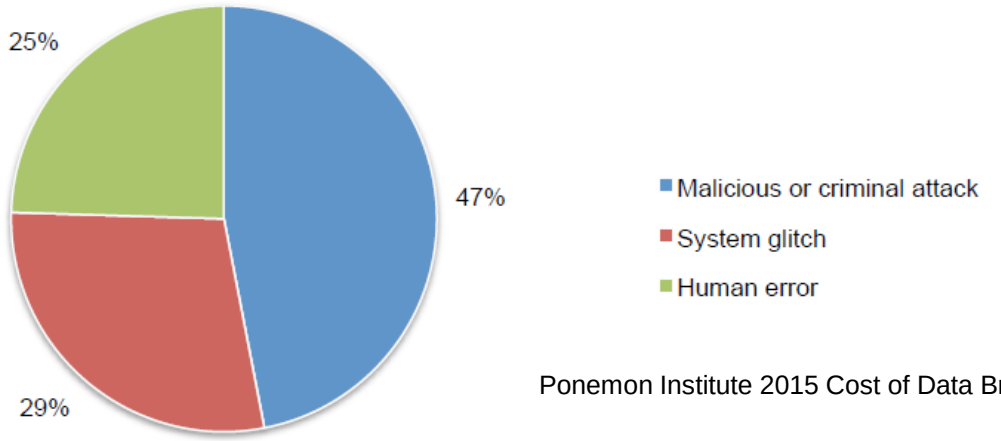
By Evan Perez, Tal Kopan and Shimon Prokupecz, CNN
Updated 8:48 AM ET, Tue October 20, 2015

CENTCOM Twitter Account Hacked By Individuals Claiming To Be Part Of ISIS

The Huffington Post | By Paige Lavender

Social Engineering = Breaches

- 47% of data breaches from malicious or criminal attack
- The most common type of these ***include phishing/social engineering*** and ***malware infections***



Ponemon Institute 2015 Cost of Data Breach Study.

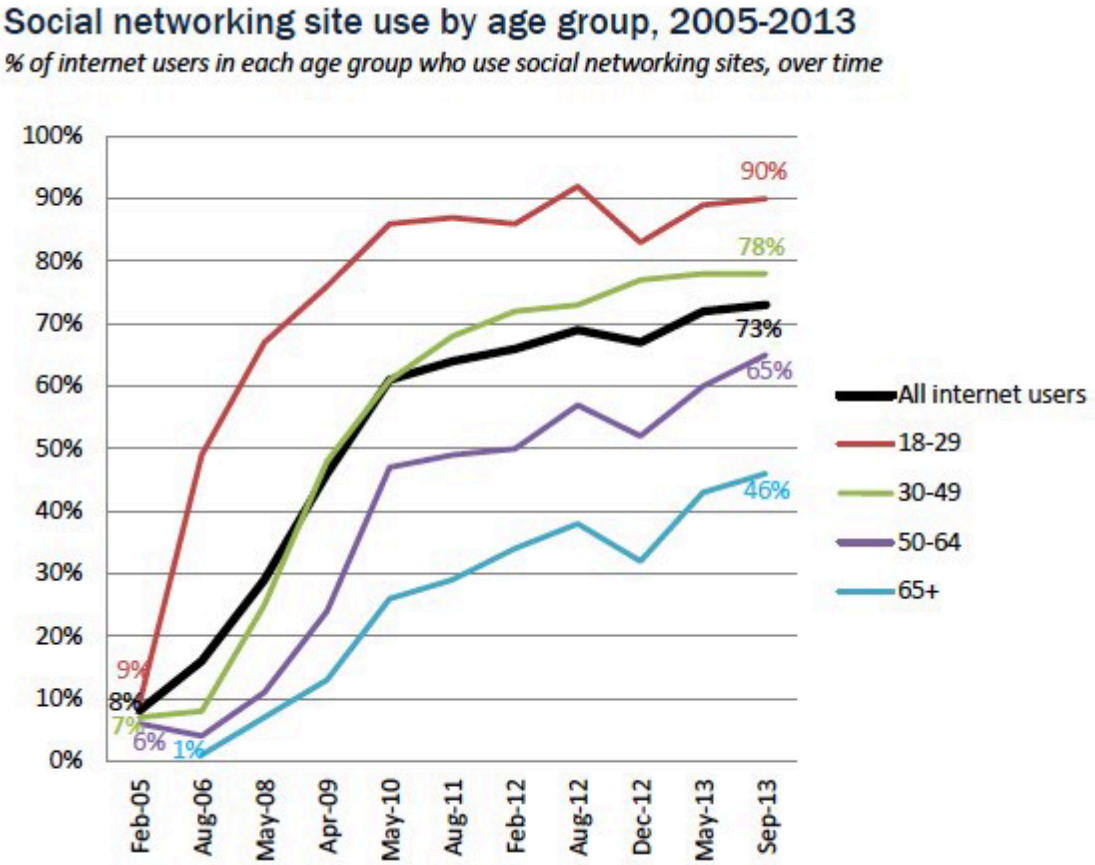
"We analyzed APT-related spear-phishing emails collected…we found that 91% of targeted attacks involve spear-phishing emails, reinforcing the belief that spear phishing is a primary means by which APT attackers infiltrate target networks." -- Trend Micro Incorporated Research Paper

Some types of social media risks

- Reputation/Brand as an asset
  - Social media shapes opinion
- Data Loss
  - Proprietary data, PII
- Piracy Infringement
  - Utilizing protected info w/o permission, be careful
- Corporate Espionage
  - Stealing sensitive data and IP
- Reconnaissance
  - Social media creates exposure points, forums, blogs
- Information Leakage
  - Unintentional disclosure, incorrectly released

Who uses Social Media?

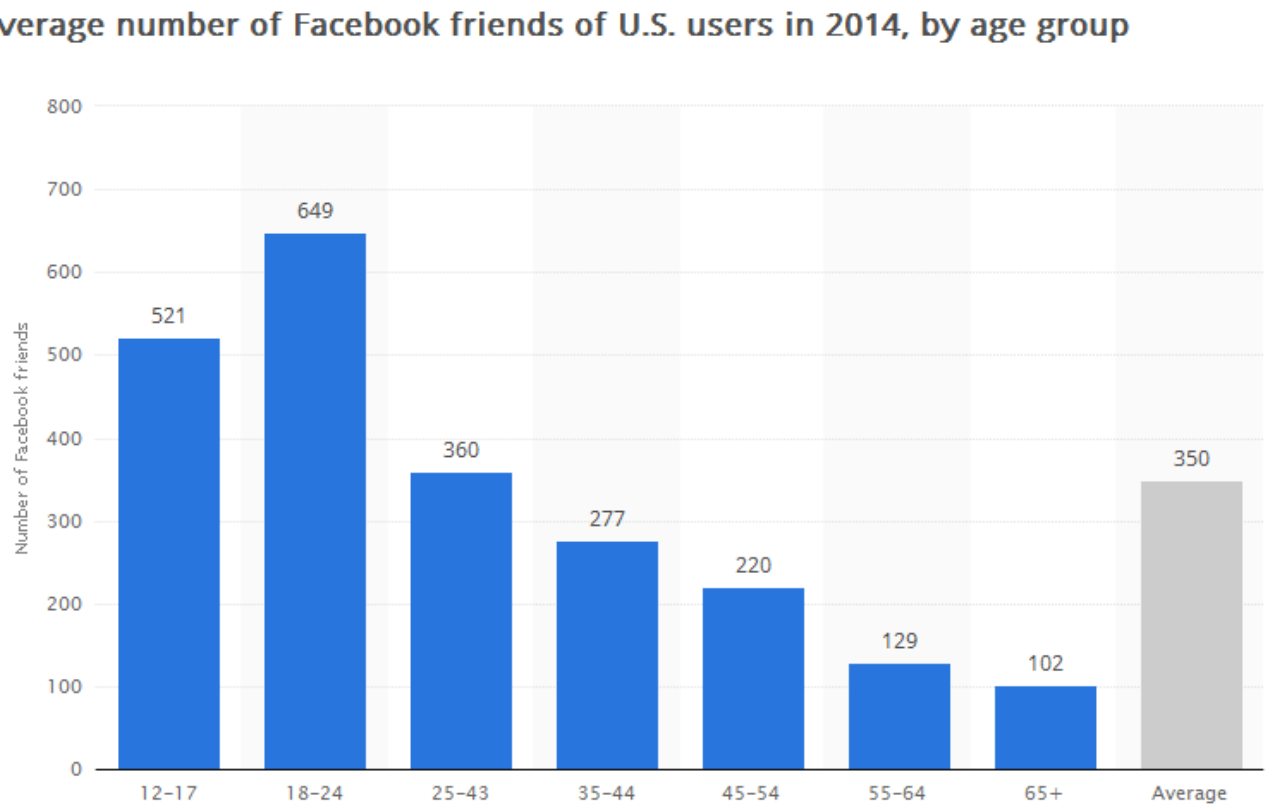
- Social media has gone from nothing to a majority of users in less than 10 years, reports Pew Research
- Only group where it is not a majority of users is age 65+, and that's at 46%
- Mobile devices contribute to the increase of social media popularity as users share their experiences on the go



Source: Pew Research, 2013

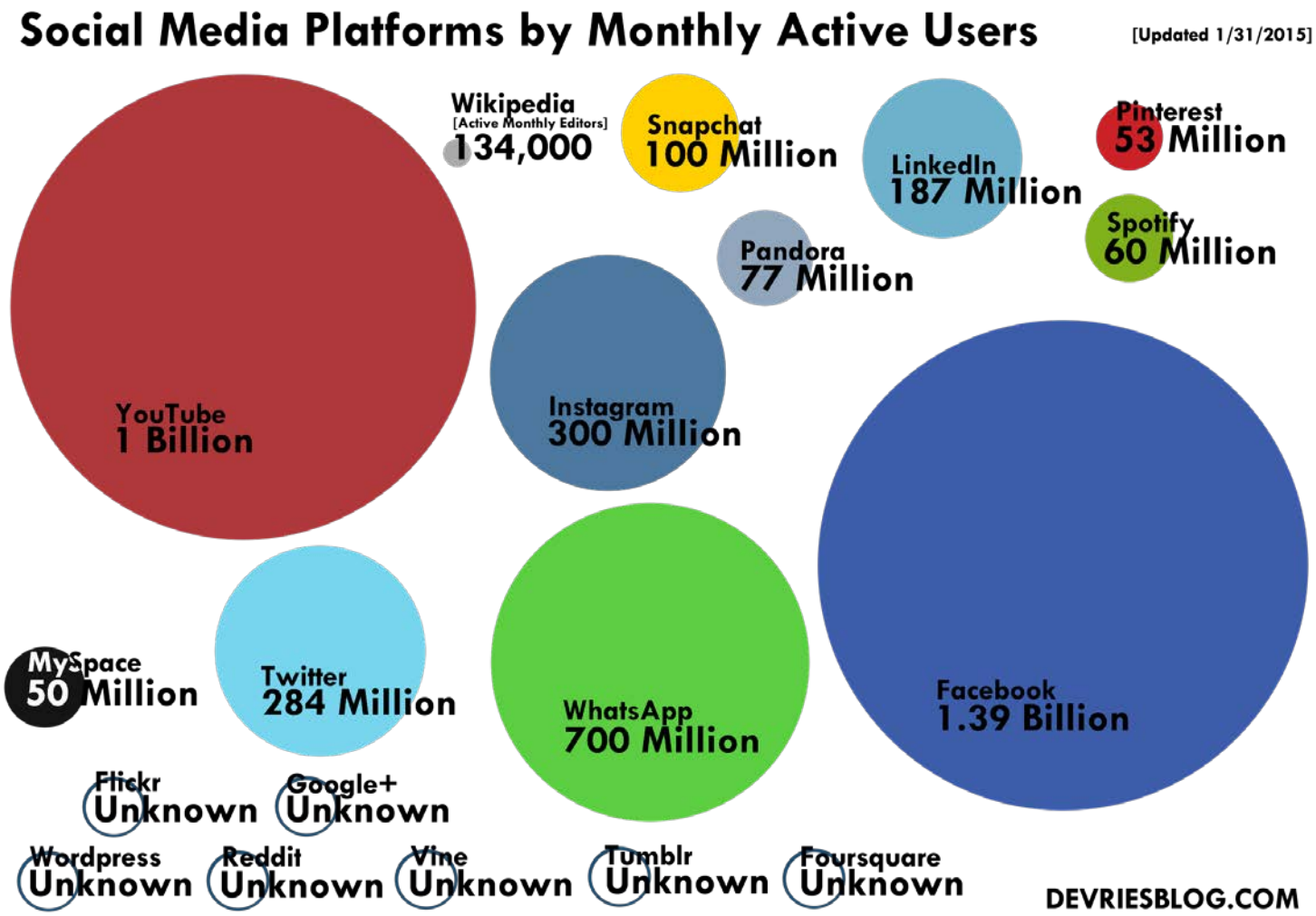
Social Media and Age Groups

- The average 18-24-year old has 649 Facebook Friends
- How well do they "know" these people?



Source: Statista, 2014

By the Numbers



What does Social Media Spying Look Like?

- Unfortunately, it looks a lot like deliberate friendships and business relationships!
  - Want to be your friend, or in your network, or follows you on Twitter
  - Wants to network with your connections
  - Seems genuinely interested in what you do and where you work
  - Asks you to share papers and presentations – “elicitation”
  - Sends you links to articles or web sites

- ***Social media spies are just like real spies, only you never meet them***
- ***Sometimes, they actually ARE real spies***

Why is this Important to us?

- Our companies are part of the American Defense Industrial Base (DIB), an integral part of national security.
  - The DIB has been referred to as “the soft underbelly” of national security.
  - Defense contractors face the same Intelligence threats that American soldiers, diplomats and spies face, every day.
- In a post-Cold-War era, the threats to national security are greater than ever:
  - Our enemies spy on us to learn what we will do, steal our technology, and deny us the ability to resist should war occur.
  - Our allies spy on us to understand our intentions and the limitations of our friendships.
  - Our competitors spy on us to steal our technology, and our people.
  - Terrorists and criminals attack us to steal, undermine, discredit or destroy that which we build.

Spying & Espionage Online

- Each year US Industry loses $100s Billions to cyber crime whether from terrorists, hacktivists, criminals, or foreign intelligence services
- There are many threats to contend with:
  - Spies who deliberately target our employees
  - Viruses and botnets that send our data to other agents.
  - Agents who buy information from other agents to target us, our families and friends.
- There is an entire marketplace involved in buying and selling your information:
  - Used extensively by criminals, but spies play there too.
- The social network makes spying 100x more efficient:
  - Much easier and cheaper to connect to people online than in person.
  - They don't generally distinguish between "family", "friends" or "acquaintances". Everyone you're connected to can see everything.

Case Study: Robin Sage

Meet Robin Sage:

- 25 years old, with a degree from MIT and 10 years of work experience.
- Accounts on Facebook, LinkedIn, Twitter, others.
- In 2009, she appeared in social media and contacted nearly 300 people in security, military, intelligence and defense contractors.
- She received invitations to do consulting work, dinners and conferences.
- She obtained access to email addresses, bank accounts and locations of military units from Facebook photos.

Case Study: Robin Sage

Who is she really?

- White hat hacker Thomas Ryan.
- Her name is taken from the “Robin Sage” training exercise for Special Forces candidates.
- Her home address was at the Blackwater main office.
- Ten years in the industry at 25 … hmmm.

Case Study: Robin Sage

- Ryan presented these findings at the Black Hat conference as an example of the threat of social networking.

- His experiment exposed the weaknesses of the human element, even in national defense and intelligence communities.

Case Study: "Newscaster"

- Iranian project "Newscaster"
  - Campaign conducted from 2011 until 2014
  - Revealed by ISIGHT Partners in May, 2014
  - Created more than a dozen fake personas on social networking sites.
  - Used Facebook, Twitter, LinkedIn, Google+, YouTube, others.
  - Targeted more than 2,000 people in US military, diplomats, Congress, journalists, US think tanks and defense contractors.
  - Created legitimate-looking web sites to support the ruse.
  - Sent targets to web sites that stole their logon credentials and installed malware on their computers.

LinkedIn Sockpuppets

- On September 3rd 2015, F-Secure reported that multiple LinkedIn accounts targeted numerous security specialists in an attempt to map their social graphs.

- Each recruiter account is focused on a particular type of Security Specialist.

- Jennifer and the other recruiter accounts have since been deleted.

LinkedIn Sockpuppets

Jennifer White 3rd

Mobile Security Talent Acquisition at Talent Src

London, United Kingdom | Staffing and Recruiting

Previous H&M

Education The University of Edinburgh

Send Jennifer InMail

500+ connections

https://uk.linkedin.com/pub/jennifer-white/b4/437/35

Background

Summary

Our mission is simple.
We establish trusting and healthy relationships with the best talents in the world.

I focus on Mobile Security profiles, Android, iOS technologies, working on malware, HCE, Apple Pay.

Contact & CV : jen@talent-src.com

Some areas of interest are
Internet of Things (IoT) security
Advanced state-sponsored malware reverse-engineering
Vulnerability research and exploitation
Penetration testing and security assessment
Malware analysis and new trends in malicious codes
Forensics, IT crime & law enforcement
Privacy issues
Low-level hacking (console security & mobile devices)
Risk management and ISO 27001
BYOD
Social Engineering

LinkedIn Sockpuppets

Talent Src
Staffing and Recruiting
11-50 employees

Home

Our mission is simple.
We establish trusting and healthy relationships with the best talents in the world.
Through our network of researchers, mining anything from scientific publications, patent databases, social networks, OSINT with a pinch of our secret recipes, we identify who is going to be driving the most fascinating organisations thanks to their in-demand talents.

We exclusively focus on bleeding edge technological challenges, and micro-niches skills and leaders.

Whether you can design an artificial eye implant, hack a bank card using lasers, or take an organisation to true new places ...

Expect to hear from us

Specialties
Cyber Security, Penetration Testing

Website
http://www.talent-src.com

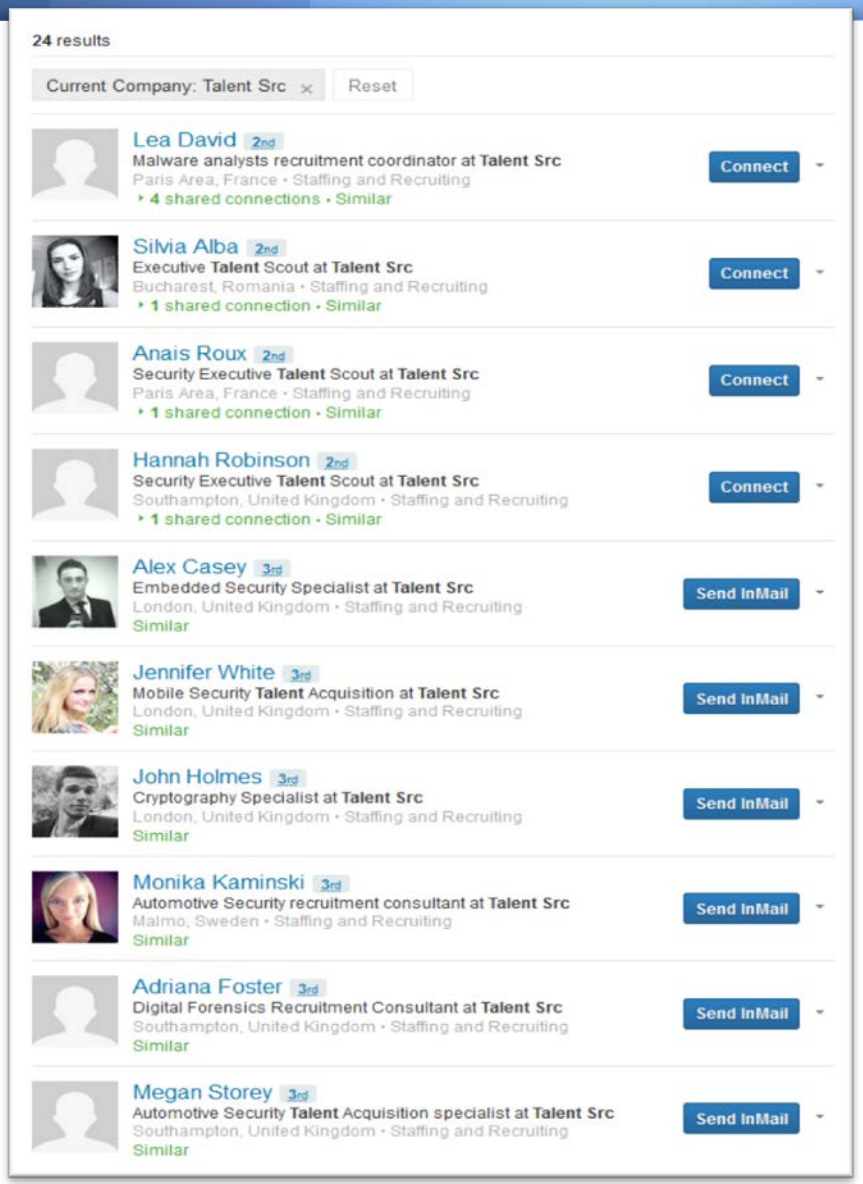
Industry
Staffing and Recruiting

Type
Privately Held

Company Size
11-50 employees

Founded
2015

LinkedIn Sockpuppets



Case Study: CentCom Social Media

- On January 11, 2015 the United States Central Command- CENTCOM – had their social media home page on Twitter and YouTube.
- The webpages were “Hacked” for around 30 minutes
- The webpages were eventually taken down for several hour.
- During the hack, tweets contained what appeared to be military plans and contact information for military officials -- one posting even showed what appeared to be an image from a computer webcam in a military facility.

CyberCaliphate

Case Study: CENT Social Media

- The “Hack” happened due to weak password authentication.
- CENTCOM had multiple system administrators for their social media accounts
- No Classified material was compromised
- Although it was embarrassing to CENTCOM, the hack had little to no affect on operations.

Case Study: OPM Hack

- The OPM Hack started in 2013 and lasted well over a one year period.
- It was originally reported that the breach released the Personally Identifiable Information of 4.2 million current and former federal employees.
- ABC News later reports that 25 Million people have been compromised in the OPM hack.
- OPM later puts the total # affected at 21.5 Million because some people were hacked twice.
- 21.5 million equates to around 9% of the adult population of the U.S.
- The breach exposed SF-86 information including Foreign Contacts, Foreign Travel, Names and Details of relatives, arrest Records, Psychiatric and mental health issues, Financial issues, Infidelity or other transgressions.

Case Study: OPM Hack

- What can our adversaries do by combining the OPM breach data, with information shared on social media?
  - Greatly increase social engineering opportunities
  - Likely will target users home computers
  - Use much more sophisticated spear-phishing schemes
  - Better understand your more recent personal habits
  - Combine this data with medical data obtained from recent Anthem attack targeting federal employees
  - Target subjects for blackmail

"We analyzed APT-related spear-phishing emails collected…we found that 91% of targeted attacks involve spear-phishing emails, reinforcing the belief that spear phishing is a primary means by which APT attackers infiltrate target networks." -- Trend Micro Incorporated Research Paper

What can I do?

- **Remember that social media is a potential threat:**
  - Your online activities may inadvertently expose excessive information about your identity, location, relationships, and affiliations, creating an increased risk of identity theft, stalking, or being targeted.
  - The threats are the same online as they are in-person.
  - But online those threats are easier, faster, bigger and cheaper than in-person.
- **Use good sense:**
  - An embarrassing comment or image will come back to haunt you… one day…when you least expect it…at the least opportune time.
  - Treat online posts as if they were completely public.
  - Choose your online "friends" as carefully as your in-person friends.
  - Review your social media privacy settings frequently
- **Always be cautious:**
  - Remember that "bad guys" are out there and targeting people like us.
  - Guard your credentials, and remember that your friends' credentials can be stolen and used to target you, as well.
  - As Ronald Reagan said, "Trust … But Verify."

Recommendations:

Do not:

- Post anything you would be embarrassed to see on the evening news.
- Post Smartphone photos (GPS) and don't use your face as a profile photo, instead, use cartoons or avatars.
- Accept friend/follower requests from anyone you do not know; independently verify identities.
- Post personally identifiable information (PII).
- Allow others to tag you in images they post.
- Use third-party applications; if needed, do not allow them to access your social networking accounts, friends list or address books.
- Use the save password, remember me or keep me logged in options.
- Use the same password for all of your accounts. Make sure the passwords for your financial sites are not permutations of your other passwords.

Recommendations:

Do:

- Be cautious when accessing online accounts from public Wi-Fi connections.
- Use strong, unique passwords. Consider passphrases for an additional level of safety.
- Keep anti-virus software current.
- Be cautious about the images you post. What is in them may be more revealing than who is in them. Images posted over time may form a complete mosaic of you and your family.
- Cover your camera when not in use.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Report contact with foreign nationals.

Resources

- NCMS Best Practices Committee Portal
  - https://www.classmgmt.com/MembersOnly/bp_committee.asp
- Social Media Policy Template
- U.S. Army Cyber Crime Prevention Flyers & Tip Cards
- Social Networking V1.0
  - CDSE Course
- Guide to Keeping your Social Media Accounts Secure
  - defense.gov
- Social networking privacy: How to be safe, secure, and social
  - Privacy Rights Clearinghouse privacyrights.org
- DHS ST06-003 Staying Safe on Social Media Sites
  - https://www.us-cert.gov/ncas/tips/ST06-003
- Subscribe to a social media management service provider to better analyze and understand social media conversations
- Report Incidents
  - http://www.ic3.gov

Questions?

Contact Information: