Security Awareness

Summit & Training

SANS

Summit: Dec 3–4
Training: Dec 1–2
Live Online

sans.org/SecAwareSummit

Security Awareness
Summit & Training

Facilitated Social Engineering Sessions: Build Your Own!

Jen Fox, Domino's Pizza

Who am I?

- DEF CON 23 black badge, Social Engineering CTF
- Security Consulting
- Security Awareness @ DPZ!

Agenda

- Presentation & Exercise
- How-To & Variations

[Your Org's] Facts

# of places

# of people

 # customer data

$$$ revenue

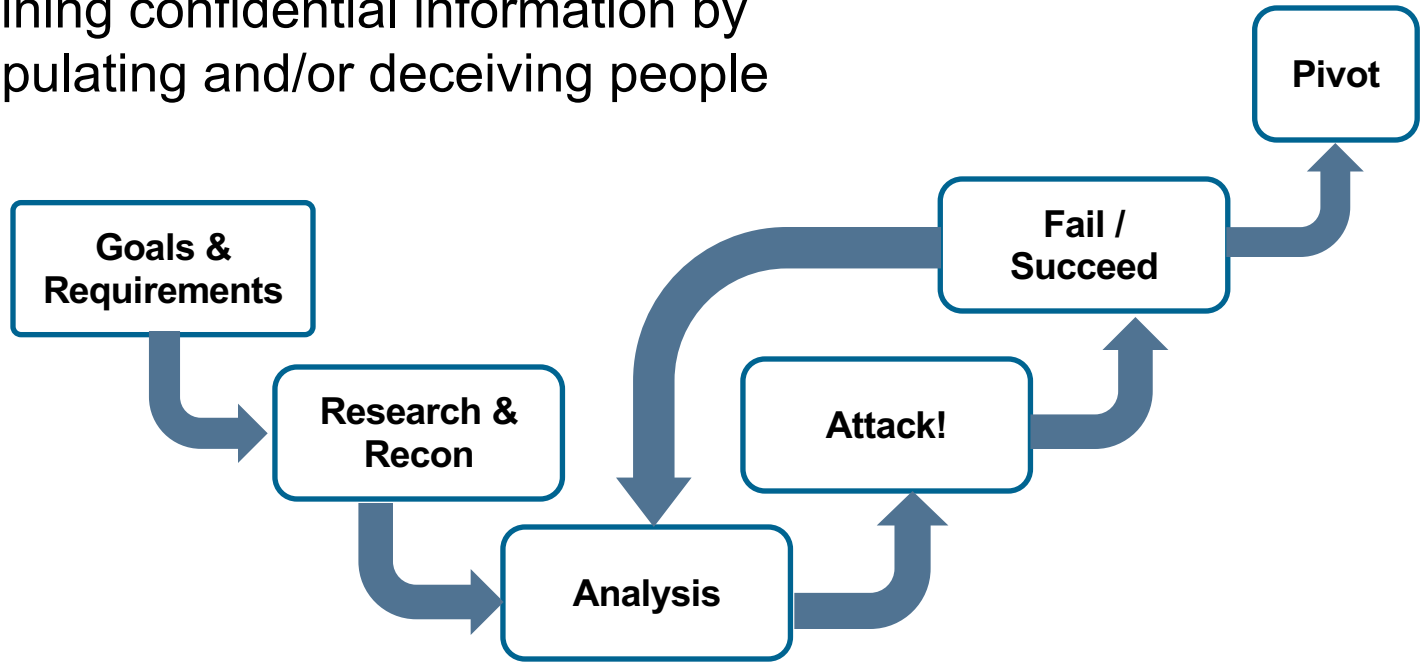
Humans are … human

- Emotions can be used to trick us
  - Urgency
  - Fear
  - Heartstrings for others
  - Curiosity
  - Wanting to be included
- We are better at detecting truth than lies
  - “Truth Default Theory”

Are there enough red flags…

Social engineering is an organized process…

Obtaining confidential information by manipulating and/or deceiving people



We do our homework

- Timeliness
- Credibility
- Language

Pretexts are engineered for…

- Probability –
  - Not everyone has to “bite”
    - The most effective pretexts are the ones that have the best odds of working.
- Forgettability –
  - Requests or pretexts are often mundane or behave in a way that we can shrug off as a simple error
    - It’s easy for us to believe we’ve simply mis-keyed something or that a site isn’t working properly

United Hope

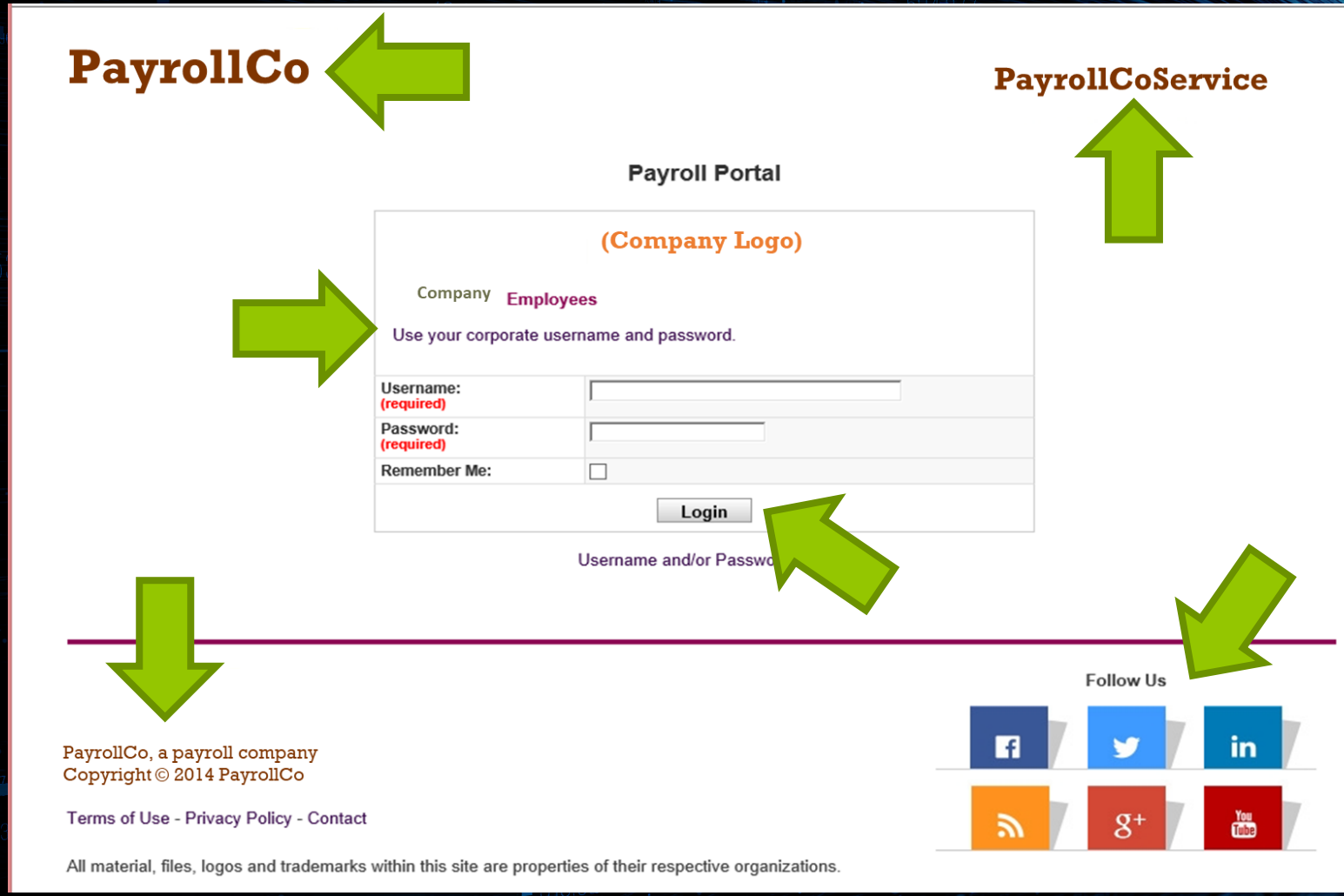
…Does Frank sound convinced?

…Why does he answer my question?

Portals

Collect credentials without directly asking for them

- Payroll
- Charity
- Intranet


PayrollCo
PayrollCoService
Payroll Portal
(Company Logo)
Company
Employees
Use your corporate username and password.
Username:
(required)
Password:
(required)
Remember Me:
Login
Username and/or Passwo
Follow Us
PayrollCo, a payroll company
Copyright © 2014 PayrollCo
Terms of Use - Privacy Policy - Contact
All material, files, logos and trademarks within this site are properties of their respective organizations.

Meanwhile, back at United Hope…

…Does Frank sound suspicious this time?

…Why or why not?

What does resistance sound like?

In conclusion

- Social engineering techniques are becoming increasingly subtle and difficult to detect
- When you do detect that something is amiss, it can still be difficult to resist
- Know who to contact, and how

GROUP EXERCISE!

Research…

- Company site
- Inappropriately exposed docs
- Vendor case studies
- News

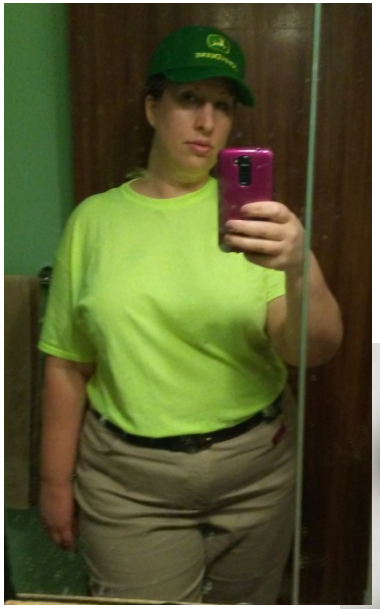
glassdoor

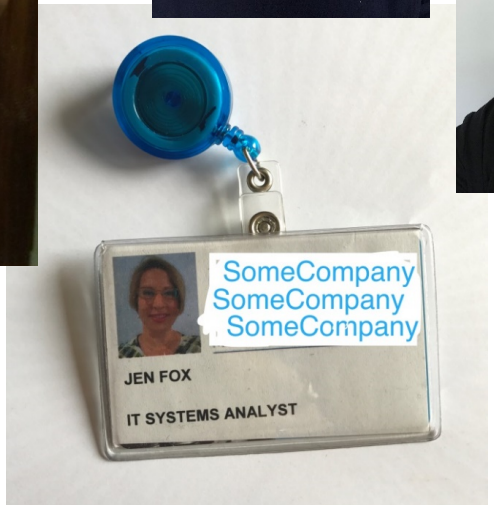
Google

LinkedIn

What's your angle?

- Probability
- Forgettability
- Curiosity





Group Exercise

- Group up!
- Look at the “research” packets
  - What does the information there tell you?
- What would your approach be to:
  - Get login information (ID & Password)
  - Have someone download a “document”
  - Bonus: Get access to someone’s computer


HOW-TO

Why do this?

- Helps people gain a more concrete understanding of how SE attacks work
- Demonstrates the low bar for certain attacks

What to focus on?

- What are the concerns for your org/industry?
- What do you want to accomplish?

Research

- Job postings
- Social media posts
- LinkedIn postings
- Company news / press releases

Variations

- Research focus
- Focus on one vector (in-person, phone, etc.)
- Focus on one pretext (story approach)

Rules of Engagement

If you want to do more than a thought experiment:

- Who/what/where is off-limits?
- Who needs to know in advance?
- How do you handle different outcomes (success or getting ‘caught’)?
- Never do anything illegal, no matter who gives you permission

Security Awareness
Summit & Training

- Jen.fox@dominos.com
- @J_Fox

Q&A

Feedback survey:

sansurl.com/secaware-eval-day1

Ask your questions in Slack:

#workshop-jen-fox