THE DARK ARTS OF SOCIAL ENGINEERING

Jen Fox
jfox@allcovered.com
@j_fox
Who am I?

• Sr. Cyber Security Consultant
• DEF CON 23 black badge, Social Engineering CTF
How we fear our users will respond
Social engineering is an organized process

1. Goals & Requirements
2. Research & Recon
3. Analysis
4. Attack!
5. Fail / Succeed
6. Pivot
We do our homework.

What I look for:

- Timeliness
- Credibility
- Language
Being social engineered is stressful

• Unusual / unexpected situation
• Forced to make a decision/take action on the spot
  ▪ Difficult for many to think on their feet and come up with a good response
• Would have to violate social norms to resist or say no
  ▪ This alone can be very stressful
In this moment of stress and pressure, this person will make a security decision for your organization.
What happened next

New call

Got creds

Logged into Intranet

Company Directory

Found “new” name

Dept names, UID, Extensions

Internal newsletter

Monthly birthdays

Portal spoof & phish
Portals

• Collect credentials without directly asking for them
  • Payroll
  • Charity
  • Intranet
All information is valuable to someone

No level of access is too low

• Even low levels of access can be a source of more info that allows a social engineer to ‘level up’
• Someone who really wants in will take the time
Process protects us

Rules don’t help people respond well under pressure

Process reduces:

• Uncertainty

• Snap decision making for important transactions
  – Example: wire fraud or password reset
Encourage reporting

• Formal
• “Local”
  
  – This makes shenanigans more visible to a team or department that is being targeted
Permission to say “no”

Knowing it is OK to say “no” and escalate to someone else if needed

• No repercussions
• No exceptions for entitled VIPs
“I’m sorry, I’m unable to disclose that information. How else may I help you today?”

• A simple way to shut down off-topic information requests
• Repeat for repeated requests
• Shows there is a line you will not let them cross
Outlets for human inclination

- We love to share things we’re excited about
  - Understand how misuse happens
- Give appropriate alternatives
So.

- Being social engineered is weird and stressful
- Give people what they need to resist effectively and confidently
- Create formal procedures to support critical processes
  - Consider the power of ceremony
- Encourage communication about odd things or asking questions

@j_fox
Email: jfox@allcovered.com
Things to do

• Key processes or functions that need:
  – A script for saying “no”
  – Process or ceremony

• Find similar domain names

• Check the “low bar”

• Ceremony: A Profound New Method for Achieving Successful and Sustainable Change by Tom Meloche

Email: jfox@allcovered.com