FISSEA 2009

22nd Annual Conference

Defensive Training for Social Engineering

Stacey Banks, CISSP, CCO, CSM

Background

Oxford Federal, LLC

- Information security solutions and services company providing certification and accreditation, risk management, software development, and training.

BECCA

- Serves to research and exchange information about business espionage controls and countermeasures; to establish and encourage a code of ethics within the profession, and to promote our professional image within the business community through a Certified Confidentiality Officer (CCO) program.

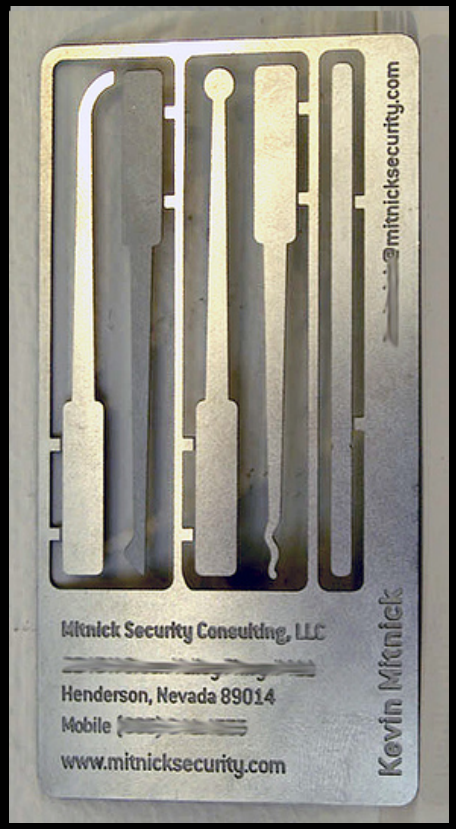
Stacey Banks, CISSP, CCO, CSM

- Specializes in providing security guidance and implementation to Federal agencies.

Agenda

- Definition
- Who is at risk
- How are they at risk
- What can be done

Definition



"Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."

-Kevin Mitnick

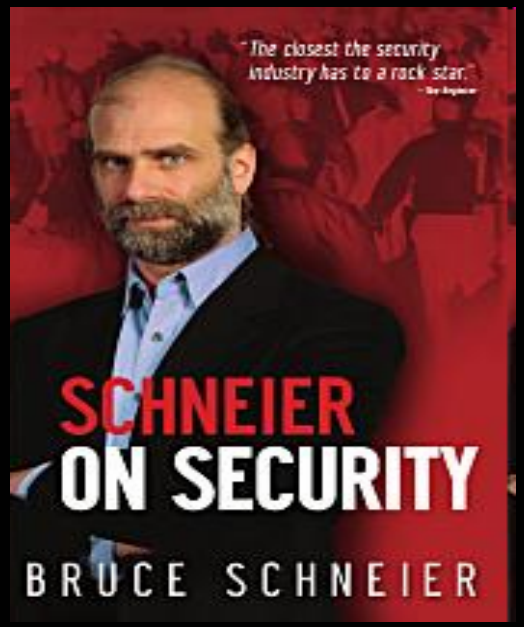
Definition

"Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable."

-Kevin Mitnick, *The Art of Deception*

Definition



"Social engineering will probably always work, because so many people are by nature helpful and so many corporate employees are naturally cheerful and accommodating. Attacks are rare, and most people asking for information or help are legitimate. By appealing to the victim's natural tendencies, the attacker will usually be able to cozen what she wants."

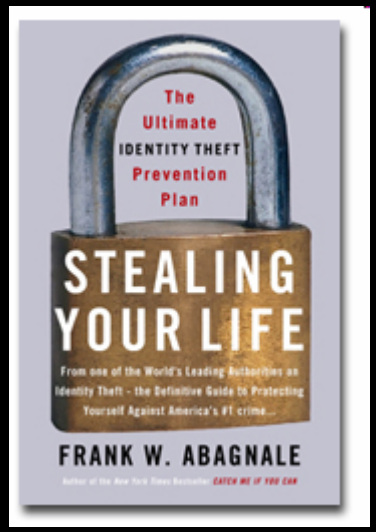
-Bruce Schneier, "*Beyond Fear*"

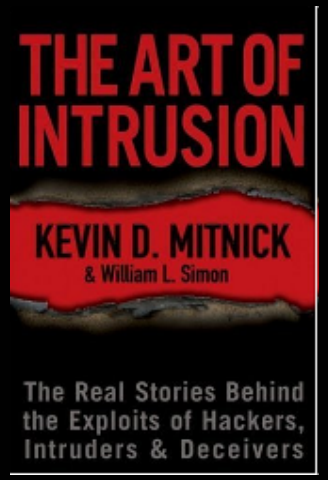
Who Is A Target?

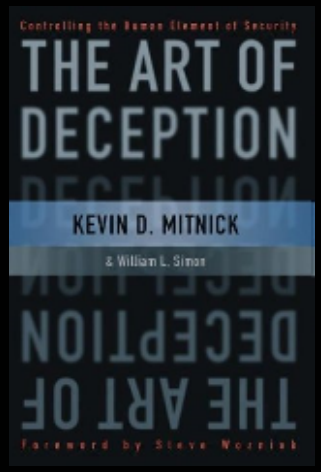
- Receptionist
- Janitor
- New Hires
- President
- Human Resources
- In short, everyone!

You Are the Weakest Link!

Famous for Social Engineering







Social Engineering Attack Types

Phishing

Account Activity locked!
Dear Valued Customer,

Our security department notice several access into your account from a foreign IP address and automatically your account activity was locked for security reason.

However, kindly click here to update and re-activate your account online banking profile.

Your security is important to us. For further inquiries, please contact us immediately at 1.800.432.1000

This alert relates to your Online Banking profile, rather than a particular account. This alert is for verification purposes only.

For security reasons, open this link on internet explorer browser and disable pop-up blocker.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

Chat Attack

<Cthon98> hey, if you type in your pw, it will show as stars
<Cthon98> ********* see!
<AzureDiamond> hunter2
<AzureDiamond> doesnt look like stars to me
<Cthon98> <AzureDiamond> *******
<Cthon98> thats what I see
<AzureDiamond> oh, really?
<Cthon98> Absolutely
<AzureDiamond> you can go hunter2 my hunter2-ing hunter2
<AzureDiamond> haha, does that look funny to you?
<Cthon98> lol, yes. See, when YOU type hunter2, it shows to us as *******
<AzureDiamond> thats neat, I didnt know IRC did that
<Cthon98> yep, no matter how many times you type hunter2, it will show to us as *******
<AzureDiamond> awesome!
<AzureDiamond> wait, how do you know my pw?
<Cthon98> er, I just copy pasted YOUR ******'s and it appears to YOU as hunter2 cause its your pw
<AzureDiamond> oh, ok.

http://www.bash.org/?244321

Voice Mail

"You've reached Bob, Director of R&D. I'll be out of the office until April 1st. If you need immediate assistance please call Tom, Assistant Director, at x123."

"You've reach Susan, I will be on client site today and tomorrow but checking voicemail and email. You can reach me on my cell at 555-1234."

Email Response

I am out of the office and will return on 01/20/2010.

If urgent, Please call:
Paula, Acting Chief at 202-555-5555.

Dumpster Diving

- Once left for pick-up is no longer private property
- Can only be called private property if they have to trespass to get to it (don’t leave it on the sidewalk overnight)
- Single way shredding vs. cross-cut
- “Set it and forget it”

Public Disclosure

- Your cone of silence is broken
- Conferences
- Shoulder surfing the Metro
- Eavesdropping at Starbucks
- Blackberry confessionals

Pretexting

- The practice of getting your personal information under false pretenses.
  - Surveys
  - 2006 HP spying scandal

Technical Vulnerabilities

- Brute force attacks on password files
- Edge devices left with factory defaults
  - Firewall
  - Router
  - PBX
- Autoplay left enabled

Going Defensive

What Can Be Done

- More complete training for employees on ways people will use to get information from them
- Review with employees what they cannot discuss outside of company
- Non-disclosure agreements

Preventative Actions

- Utilize Defense-in-Depth
- Develop policies and procedures to address the issues
- Understand legal requirements and recourses