

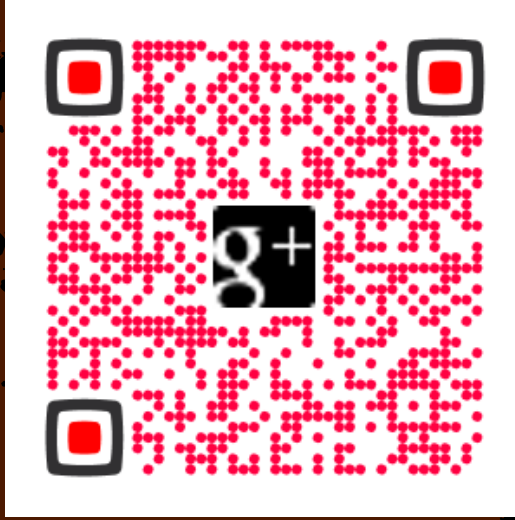
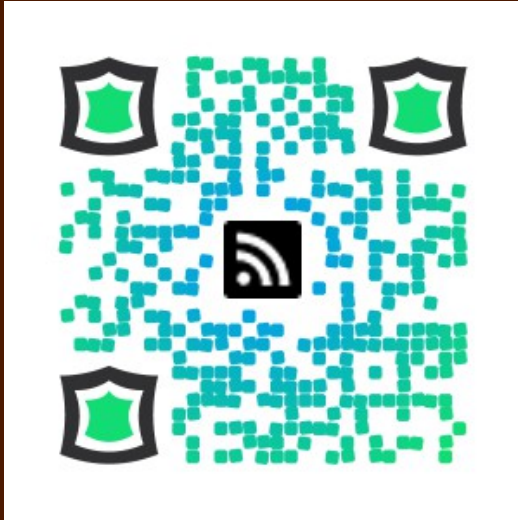
# HACKING PEOPLE

No Mask Required



# Tom Webster

"SamuraiLink3"



 SamuraiLink3.com

 SamuraiLink3@gmail.com

 plus.google.com/+TomWebster

 @SamuraiLink3



# Old Gods and Boogymen

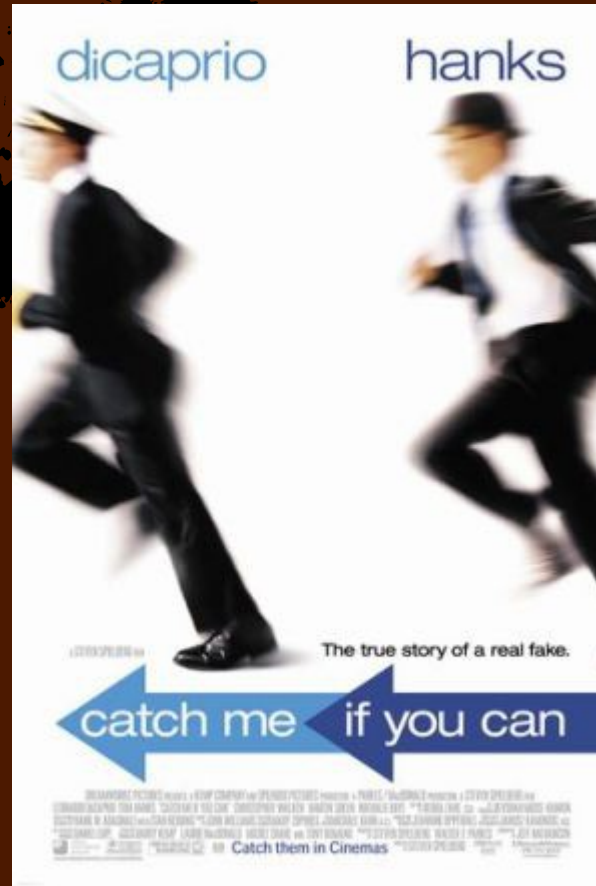
Kevin Mitnick



- Fugitive Hacker
- Popularized the use of Social Engineering
- Became a security consultant and wrote some books.

# Old Gods and Boogeymen

Frank Abagnale



# Old Gods and Boogymen

Frank Abagnale



- His life portrayed in "Catch Me if You Can"
- Impersonated an airline pilot, doctor, lawyer, teaching assistant, security guard, etc...
- Expert in forgery and manipulation.

# Magic, Curse, Hex, Incantation

It goes by many names, But we know it as:

It goes by many names, But we know it as:

# Magic, Curse, Hex, Incantation

It goes by many names, But we know it as:

# SOCIAL ENGINEERING

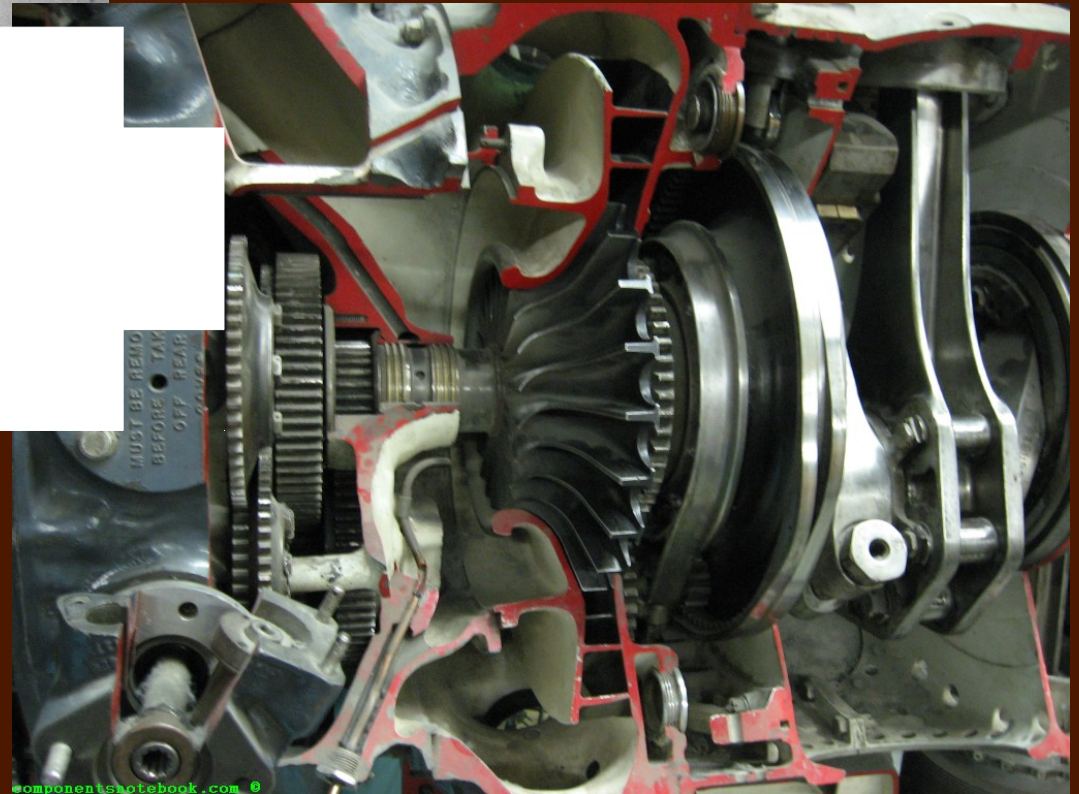
# Social Engineering

What does that even mean?



## Communicating

## With an End Goal



# Social Engineering

What does that even mean?

Bluff

Deceive

Use

Con

Dupe

Lie

Fraud

Manipulate

Cheat

**The old gods' tricks are alive and well**

**And we still haven't learned their lessons**

# The old gods' tricks are alive and well

Mat Honan



- Lost most of his digital life thanks to social engineering leveraged against Apple and Amazon.
- Apple issued a temporary password based on **Last 4 of Credit Card** and **Billing Address**.
- Using Two-Factor Authentication could have saved him.

# The old gods' tricks are alive and well

Mat Honan



## Information Found

- Twitter
  - Personal Website
- Personal Website WHOIS:
  - Name
  - Gmail Address
  - Billing Address
- Google
  - Apple Email Address
- Amazon
  - Last 4 of all known credit cards
- Apple
  - iCloud Access

# The old gods' tricks are alive and well

Naoki Hiroshima



- Lost prized Twitter Account (@N) through extortion, enabled by social engineering.
- PayPal gave out personal information and **last 4 of credit card** due to social engineering attack.
- Personal information and social engineering used to take over GoDaddy account and hold web services for ransom.
- GoDaddy uses **last 6 of credit card**, representative had attacker keep guessing starting numbers between 00-09, since he had the last 4.
- Naoki was extorted into releasing his Twitter password.

# The old gods' tricks are alive and well

Naoki Hiroshima



## Information Found

- PayPal
  - Personal Information
  - Last 4 of Credit Card
- GoDaddy representative
  - Other 2 digits of credit card
  - Complete domain control
    - Including MX records

**WHAT CAN WE DO?**

# **1. LEARN HARD LESSONS**

**2. ACCOUNT LINKING  
IS DANGEROUS**

**3. COMPANIES HOLD  
THE KEYS TO OUR  
DIGITAL LIVES**

**3.1 "SOME OF THE BIGGEST  
COMPANIES IN THE WORLD  
HAVE SECURITY THAT IS ONLY  
AS GOOD AS A MINIMUM-WAGE  
PHONE SUPPORT WORKER  
WHO HAS THE POWER TO  
RESET YOUR ACCOUNT. AND  
THEY HAVE VALID BUSINESS  
REASONS FOR GIVING THEM  
THIS POWER." - JOSH BRYANT**

**4. WE'RE BAD AT THIS**

**5. STOP USING CREDIT  
CARDS FOR  
AUTHENTICATION**

**DISTRUST BY DEFAULT**

**THANKS!**