Social Engineering

Omer Usmani

Security Analyst

CCC Technology Center

Social Engineering

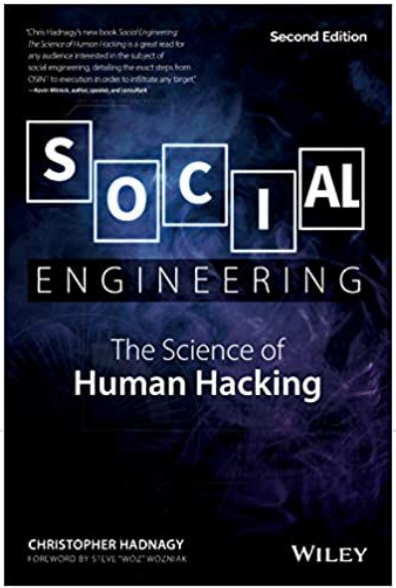
Overview of common methods

Best prevention practices

Famous Social Engineers

Definition

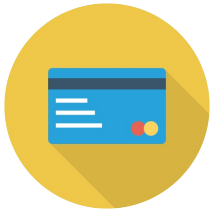
“Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests” - Christopher Hadnagy.



California Community Colleges

Information Stolen

- Credit card
- Bank account
- Social security numbers
- Usernames
- Passwords
- Email Addresses

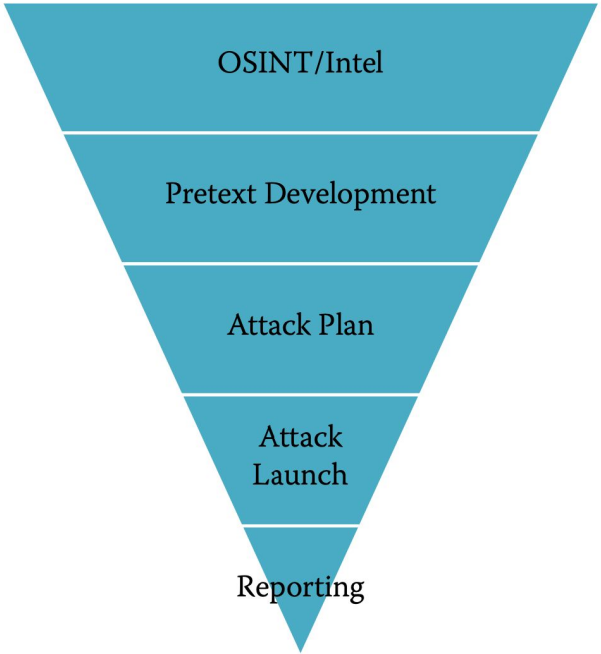


California Community Colleges

Types of Social Engineering

- Phishing
- Vishing
- Smishing
- Physical Impersonation

Workflow



California Community Colleges

Open Source Intelligence

- Framework for gathering intelligence from publicly available information.

Open Source Intelligence

Table 2-1 Sample OSINT questions

Type of Organization	Questions to Ask
Corporation	How does the corporation use the Internet? How does the corporation use social media? Does the corporation have policies in place for what its people can put on the Internet? How many vendors does the corporation have? What vendors does the corporation use? How does the corporation accept payments? How does the corporation issue payments? Does the corporation have call centers? Where are headquarters, call centers, or other branches located? Does the corporation allow BYOD (bring your own device)? Is the corporation in one location or many locations? Is there an org chart available?
Individual	What social media accounts does the person use? What hobbies does the person have? Where does the person vacation? What are the person's favorite restaurants? What is the family history (sicknesses, businesses, and so on) of the person? What is the person's level of education? What did the person study? What is the person's job role, including whether people work from home, for themselves, and who they report to? Are there any other sites that mention the person (maybe they give speeches, post to forums, or are part of a club)? Does the person own a house? If yes, what are the property taxes, liens, and so on? What are the names of the person's family members (as well as any of the previously mentioned info on those people)?

Source: Hadnagy; Social Engineering

OSINT Tools

- Google
- Whois
- Shodan

Whois

```
omers-MBP:~ omer$ whois google.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com
```

Google Dorking

- Using the Google search engine to query for information that may or may not be intended to be available to the public.

Operators

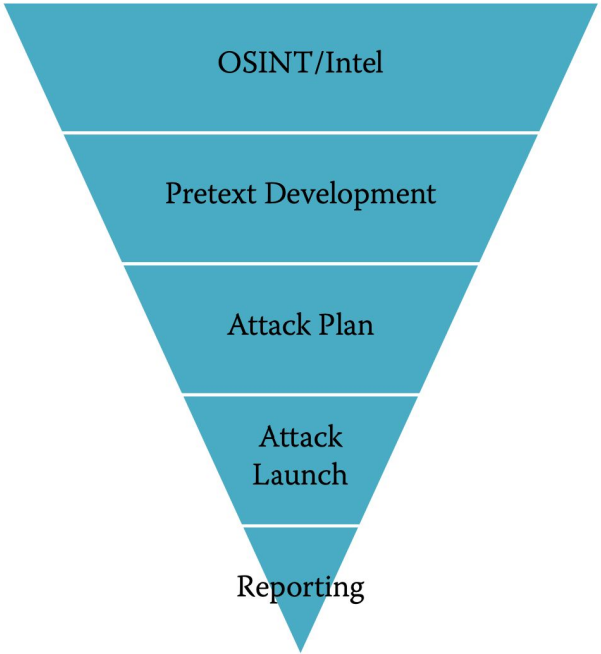
- cache:
- allintext:
- allinurl:
- allintitle:
- link:
- site:
- filetype:
- *
- |
- +
- -

Pretexting

Pretexting

1) Thinking through your goals
2) Understanding reality versus fiction
3) Knowing how far to go
4) Avoiding short-term memory loss
5) Getting support for pretexting
6) Executing the pretext

Workflow



California Community Colleges

Phishing

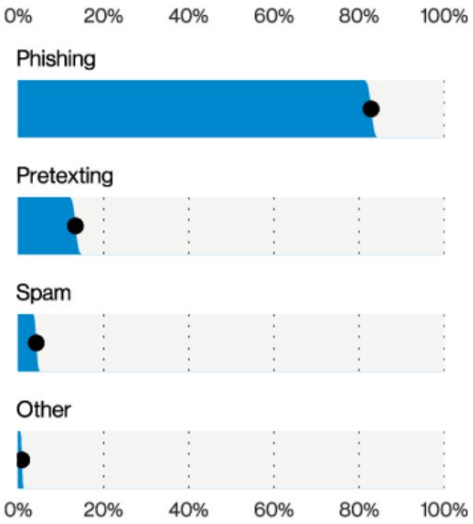


Figure 73. Top Social varieties in Social Engineering incidents (n=3,810)

California Community Colleges

2021 Verizon Data Breach and Investigations Report

Consequences of Being Phished

- Installation of Malicious Software
- Precursor to Ransomware
- Financial Loss
- Customer Information Compromised
- Loss of Consumer Trust

Types of Phishing

1) Deceptive Phishing
2) Spear Phishing
3) Wailing

Deceptive Phishing

1) Legitimate Links
2) Company Logos & Theme
3) Copy of Landing/Login Page
4) Shortened URL & Redirects

Spear Phishing

Whaling

- SImilar to spear phishing
- Aimed at executives of a company
- Goal is to gain access to an administrator account (Windows AD, Linux, AWS, etc.)

Protecting Against Phishing

“Does the directly email relate to a matter that I am involved in?”

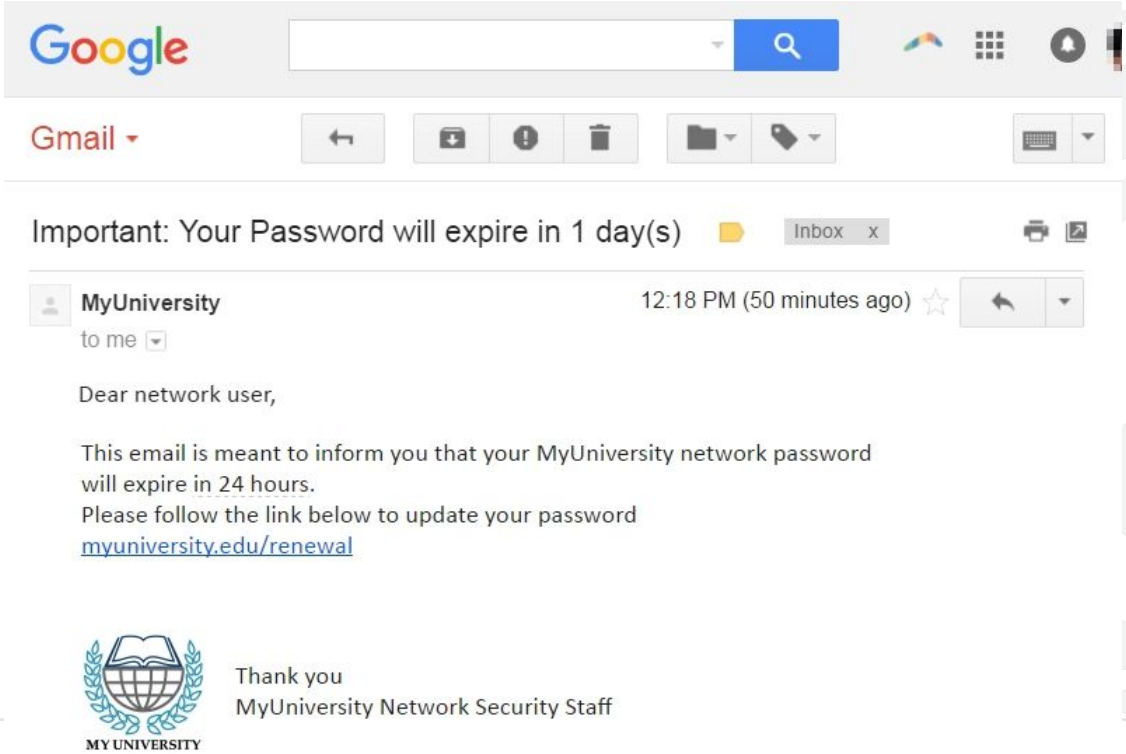
1.“Change password immediately”

2.“Your mailbox is out of space”

3.“There was a problem with your credit card information”

4.”We have migrated to a new ……: **Click Here**”.

Email Example



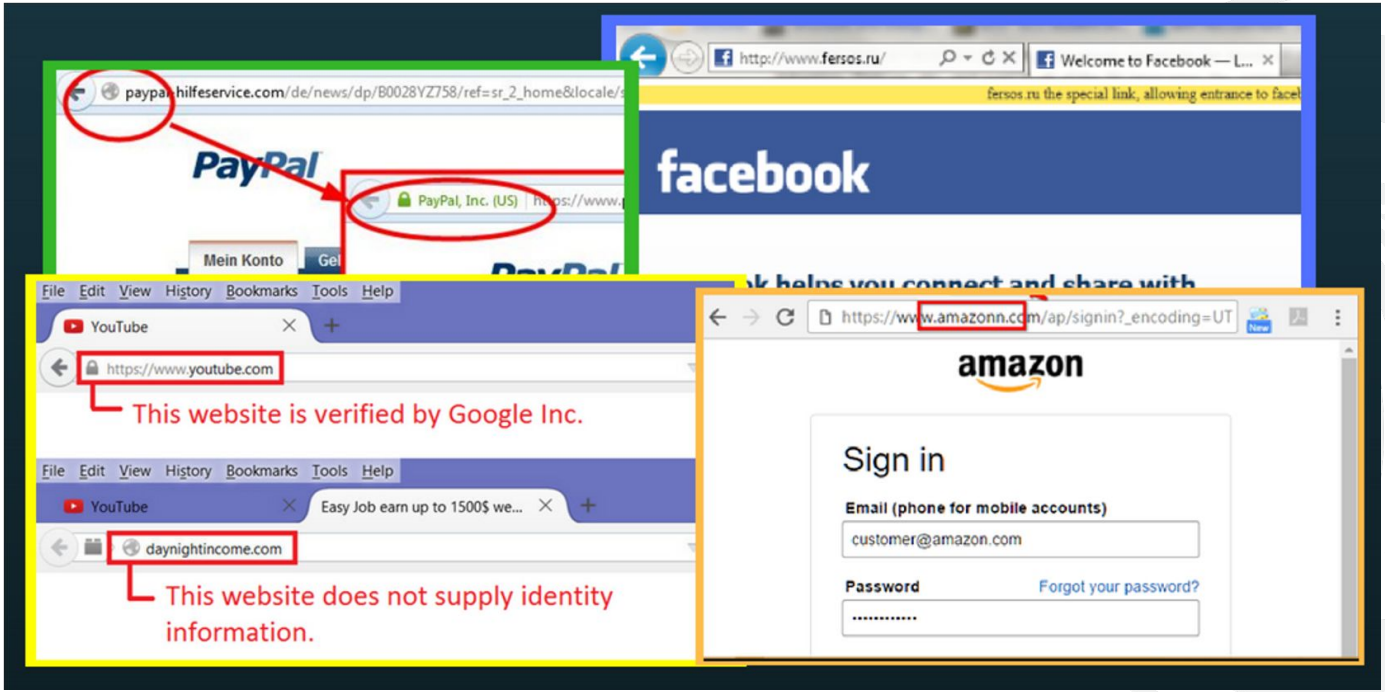
Source: Imperva

California Community Colleges

URL Example

Source: Imperva

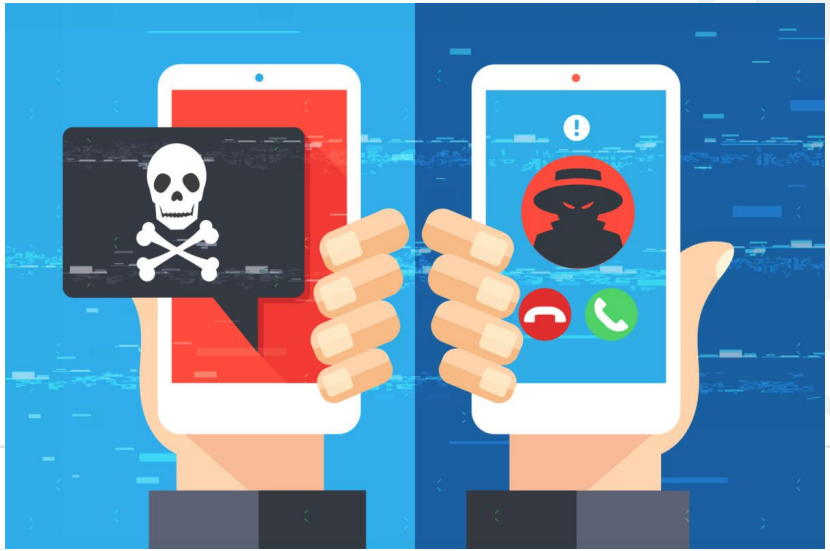
Web Page Checks



California Community Colleges

Vishing

- Similar to Phishing
- Scam phone call to extract personal information



California Community Colleges

Vishing Techniques

1) ID Spoofing

1) Corporate Jargon

1) Mumbling Answers

Vishing Themes

- Compromised bank or credit card accounts
- Call from the IRS
- Investment offers
- Medicare
- Social Security
- Student Loans
- Scholarships

Vishing Video

California Community Colleges

Vishing Prevention

- Never give out personal information over the phone
- Avoid taking calls from unknown phone numbers
- Register your phone number with the National Do Not Call Registry (Not very effective)

Recent Example of Vishing Attack

When a Hacker Calls: How Robinhood Fell Victim to a Vishing Raid

By Annie Massa, William Turton, and Jack Gillum
November 27, 2021, 8:00 AM PST

https://www.bloomberg.com/news/articles/2021-11-27/when-a-hacker-calls-how-robinhood-fell-victim-to-vishing-attack

Smishing

- Use of text (sms) messages to acquire personal information

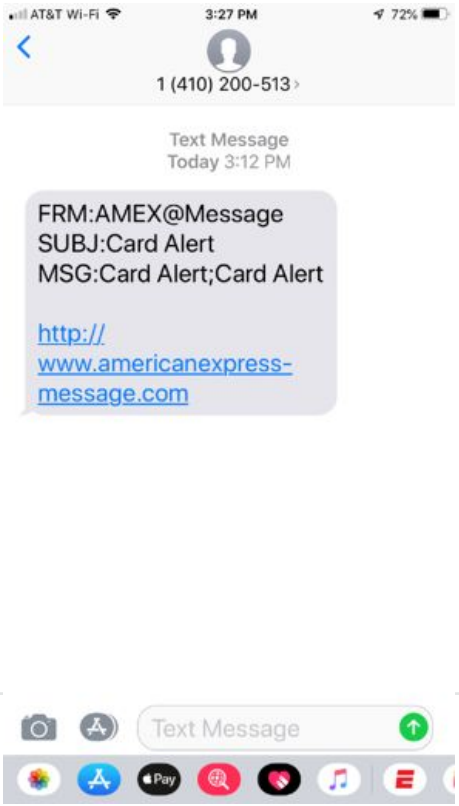
Smishing Techniques

1) Download of a Malicious App

1) Link to Data-Stealing Forms

1) Instruct the User to Contact Tech Support

Example Smshing Message



California Community Colleges

Defending Against Smishing Attacks

1) Check for spelling and grammar mistakes
2) Visit the companies website itself
3) Verify the sender's phone number
4) Do not open links from unknown senders
5) Be wary of keywords such as “act fast”, “sign up now”, or an offer that seems to good to be true

Example of A Recent Smishing Campaign

TangleBot Campaign Underscores SMS Threat

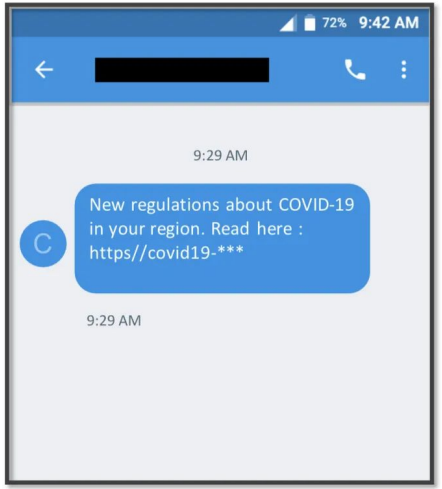
The attack targets Android devices and starts with a malicious SMS message that aims to bring malware onto compromised devices.

Robert Lemos
Contributing Writer

September 24, 2021

https://www.darkreading.com/threat-intelligence/tanglebot-campaign-underscores-sms-threat

Example of A Recent Smishing Campaign



https://www.darkreading.com/threat-intelligence/tanglebot-campaign-underscores-sms-threat

California Community Colleges

Physical Impersonation

- Impersonating an employee
- Take identity of a trusted entity

Physical Access Prevention

- Have identification procedures
- Employees should be aware of members belonging to other venders or contractors

Famous Social Engineers

Kevin Mitnick

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W214460021).

NAME: .....MITNICK, KEVIN DAVID

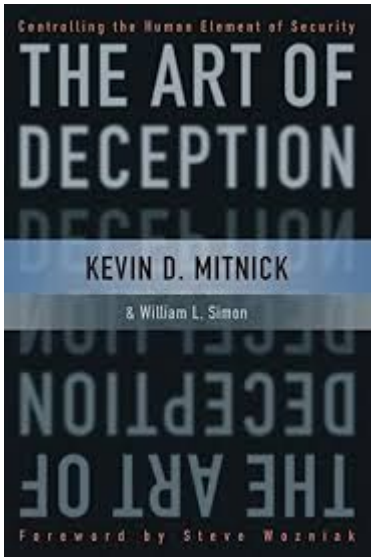
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

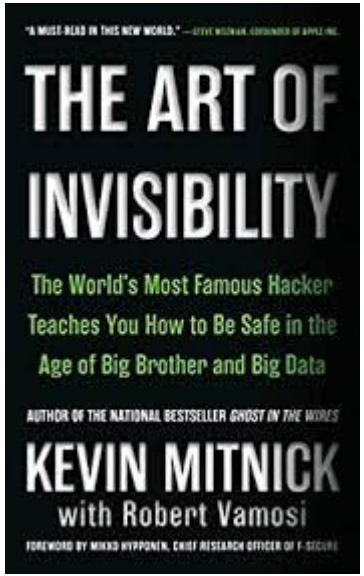
DESCRIPTION:

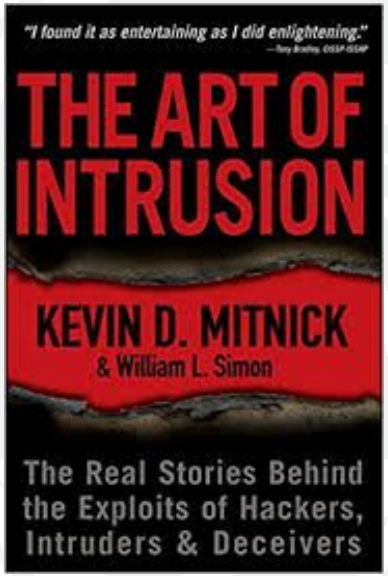
Sex:.....MALE
Race:.....WHITE
Place of Birth:.....VAN NUYS, CALIFORNIA
Date(s) of Birth:.....08/06/63; 10/18/70
Height:.....5'11"
Weight:.....190
Eyes:.....BLUE
Hair:.....BROWN
Skintone:.....LIGHT
Scars, Marks, Tattoos:.....NONE KNOWN
Social Security Number (s):.....550-39-5695
NCIC Fingerprint Classification:...DOPM20PM13DIPM159M09

California Community Colleges

Kevin Mitnick

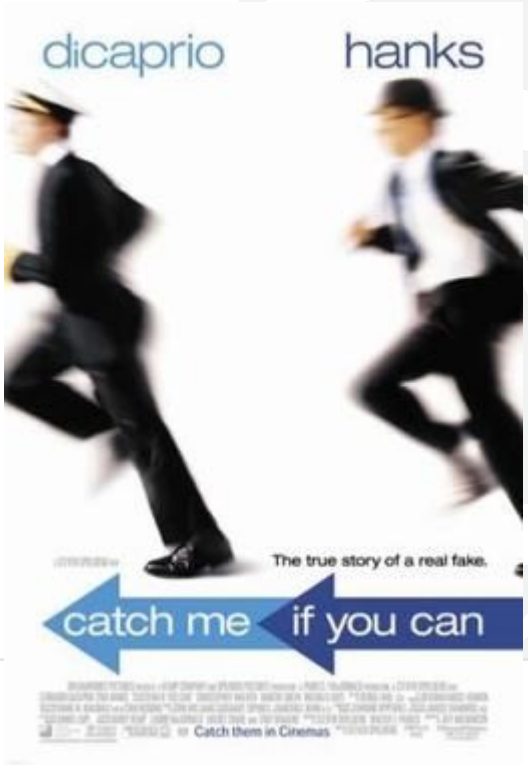






California Community Colleges

Frank William Abagnale



California Community Colleges

Charles Ponzi

Resources

- HaveIBeenPwned
- Intelligence X
- DeHashed
- SpiderFoot
- https://transparencyreport.google.com
- https://phishcheck.me
- https://checkphish.ai
- https://www.virustotal.com

Thank you

And protect yourselves out there!