Social Engineering

Omer Usmani

Security Analyst

CCC Technology Center

Social Engineering

Overview of common methods

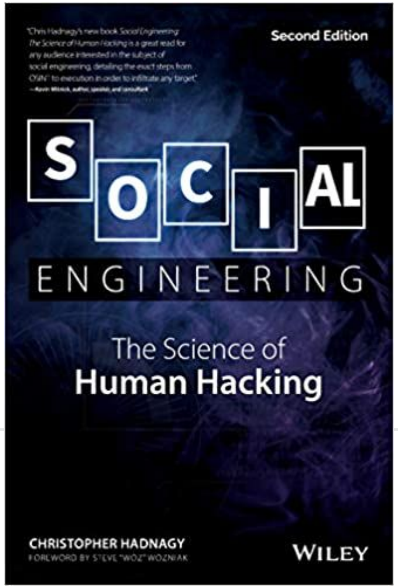
Best prevention practices

OSINT

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.


"Chris Hadnagy's new book Social Engineering: The Science of Human Hacking is a great read for any audience interested in the subject of social engineering, detailing the exact steps from OSINT to execution in order to infiltrate any target."
—Kevin Mitnick, author, speaker, and consultant
Second Edition
SOCIAL
ENGINEERING
The Science of
Human Hacking
CHRISTOPHER HADNAGY
FOREWORD BY STEVE "WOZ" WOZNIAK
WILEY

Information Stolen

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

Types of Social Engineering

- Phishing
- Vishing
- Smishing
- Physical Impersonation

Phishing

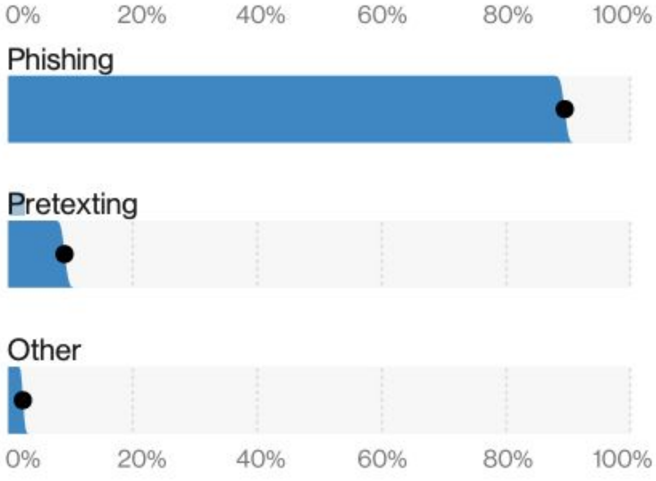


Figure 28. Top Social varieties in incidents (n = 3,594)

2020 Verizon Data Breach and Investigations Report

Consequences of Being Phished

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

Types of Phishing

1) Deceptive Phishing
2) Spear Phishing
3) Wailing

Deceptive Phishing

1) Legitimate Links
2) Modifying Company Logos
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

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

Be wary of emails that imply urgency regarding passwords or account information:

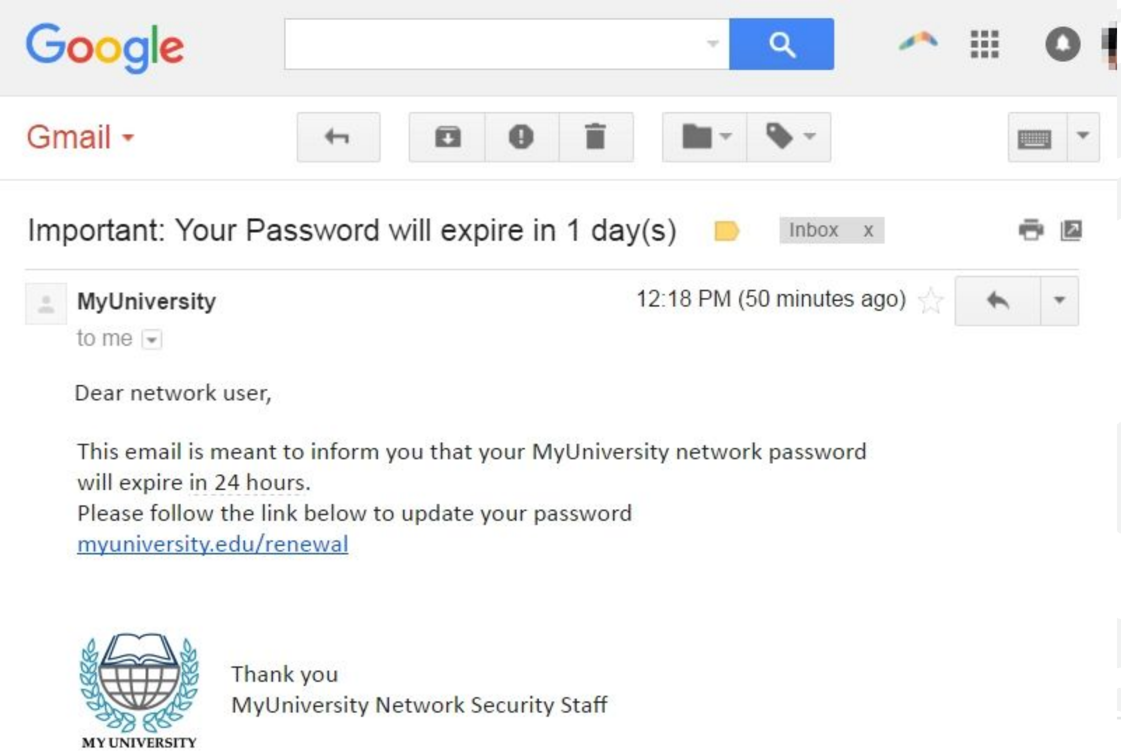
1.“Change password immediately”

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



Important: Your Password will expire in 1 day(s)

MyUniversity
to me

12:18 PM (50 minutes ago)

Dear network user,

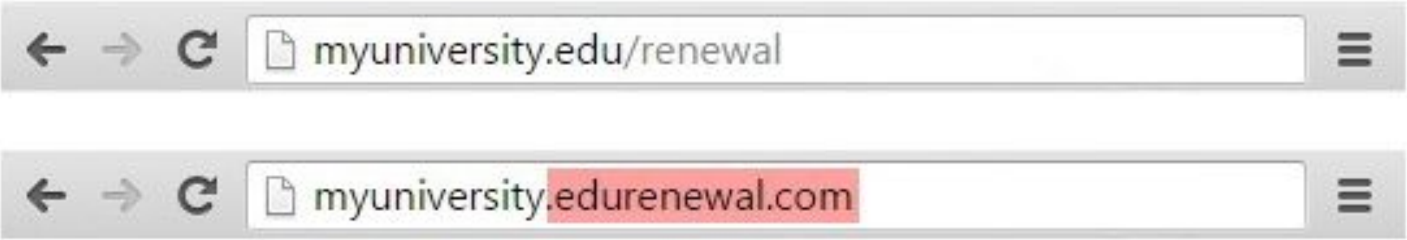
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

Source: Imperva

California Community Colleges

URL Example

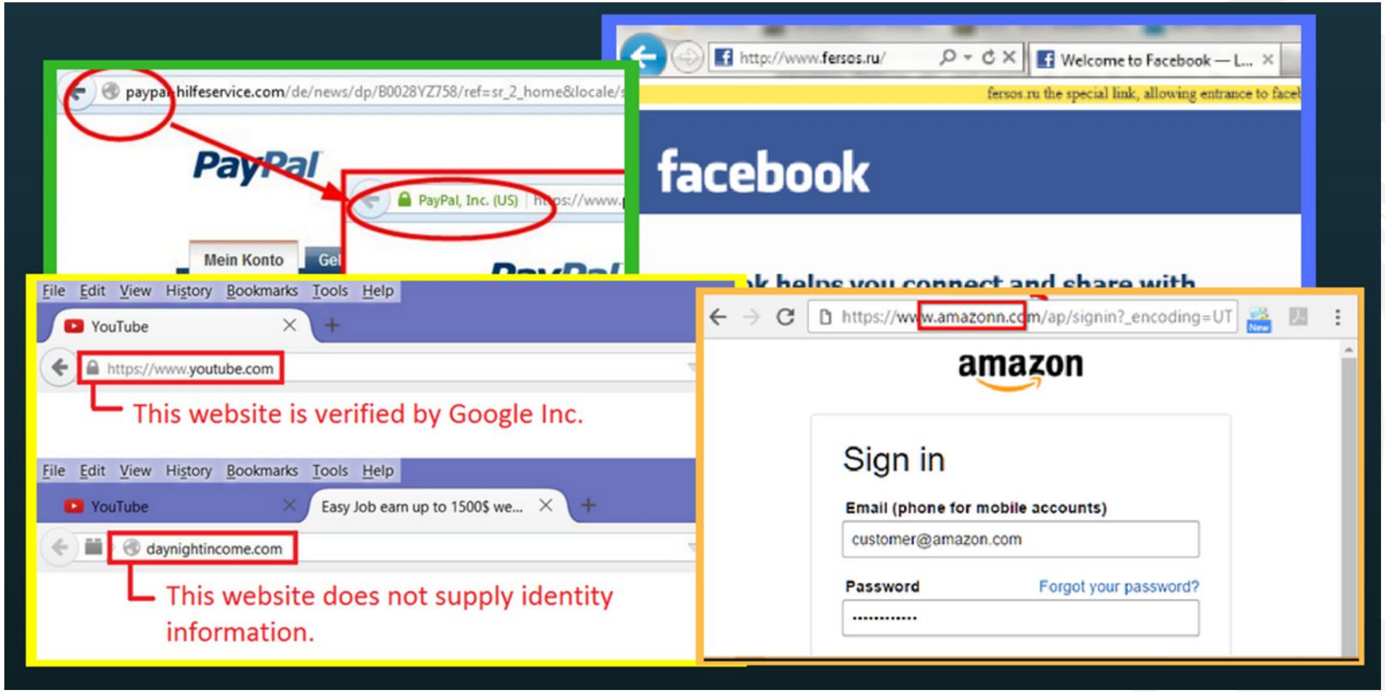


myuniversity.edu/renewal

myuniversity.edurenewal.com

Source: Imperva

Web Page Checks



paypal-hilfeservice.com/de/news/dp/B0028YZ758/ref=sr_2_home&locale/

PayPal, Inc. (US) https://www.

http://www.fersos.ru/

Welcome to Facebook — L...

fersos.ru the special link, allowing entrance to faceb

https://www.youtube.com

This website is verified by Google Inc.

Easy Job earn up to 1500$ we...

daynightincome.com

This website does not supply identity information.

https://www.amazonn.com/ap/signin?_encoding=UT

Sign in

Email (phone for mobile accounts)

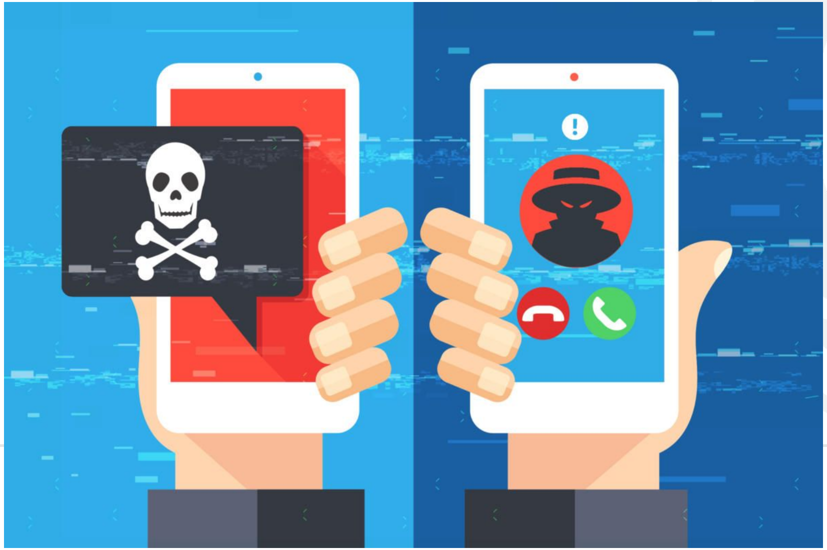
customer@amazon.com

Password

Forgot your password?

Vishing

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



Vishing Techniques

1) ID Spoofing

2) Corporate Jargon

3) Mumbling Answers

Vishing Themes

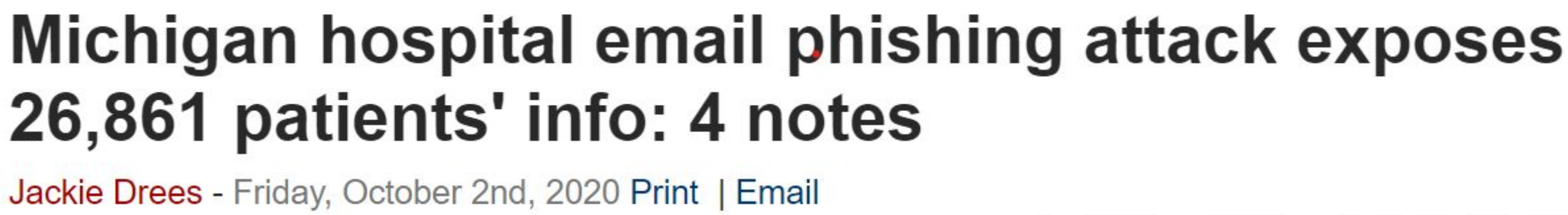
- Compromised bank or credit card accounts
- Call from the IRS
- Investment offers
- Medicare
- Social Security
- Student Loans
- Scholarships

Vishing Video

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

Recent Example of Vishing Attack



Michigan hospital email phishing attack exposes 26,861 patients' info: 4 notes

Jackie Drees - Friday, October 2nd, 2020 Print | Email

Smishing

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

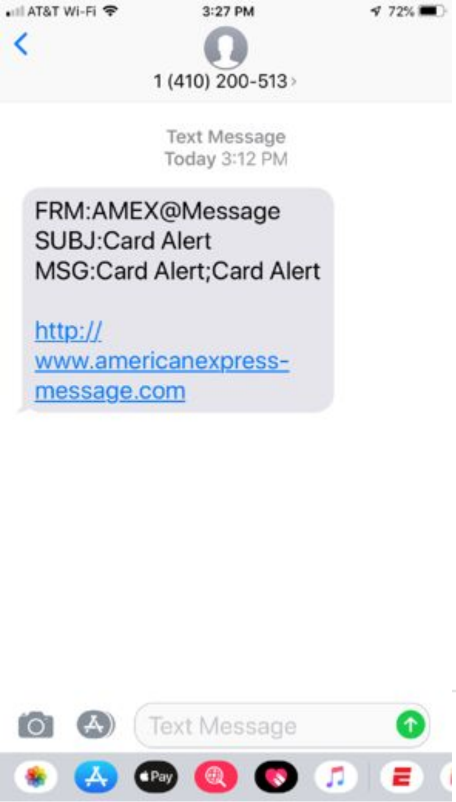
Smishing Techniques

1) Download of a Malicious App

2) Link to Data-Stealing Forms

3) Instruct the User to Contact Tech Support

Example Smishing Message



FRM:AMEX@Message
SUBJ:Card Alert
MSG:Card Alert;Card Alert

http://www.americanexpress-message.com

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 Attack

SMishing Attacks Masquerading as USPS and FedEx

by Lisa O'Reilly on September 24, 2020

Physical Impersonation

- Impersonating an employee
- Take identity of a trusted entity

[“We have a 100% success ratio in physical breaches” - social-engineer.org]

Physical Access Prevention

- Have identification procedures

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

Information Gathering

A successful social engineering attack requires gathering relevant information on a target. How do they do this effectively?

OSINT

- Framework for gathering intelligence

- Information often found on social media or organization’s online directory.

Reconnaissance

OSINT Tools

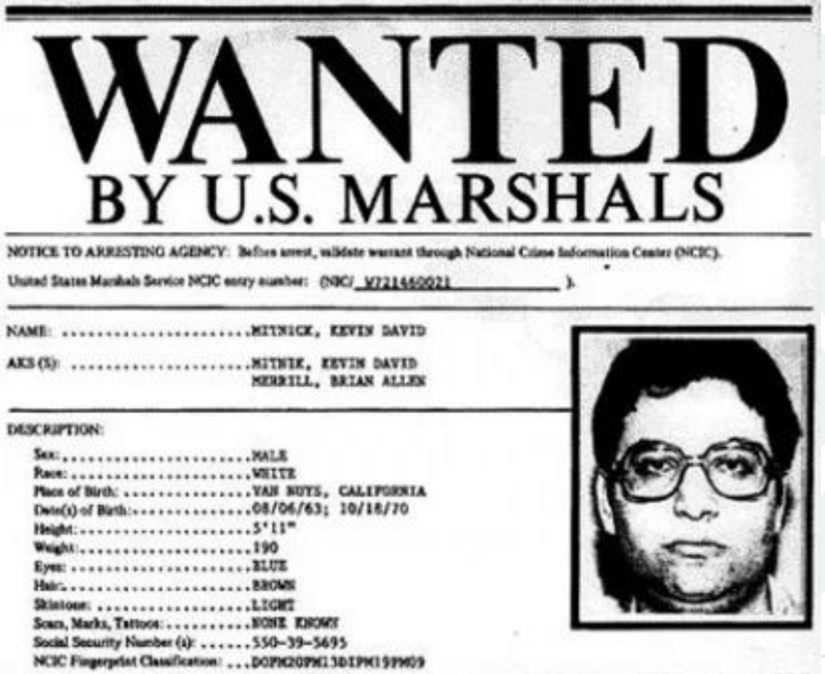
- Google
- Whois
- Shodan

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
```

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/ W721460021).

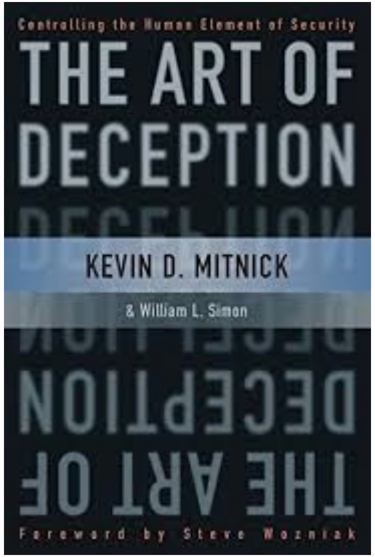
NAME: ....MITNICK, KEVIN DAVID

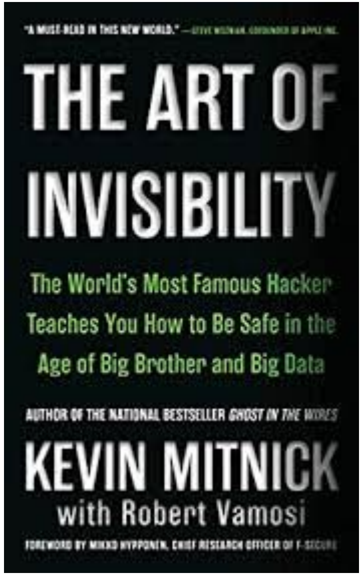
AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

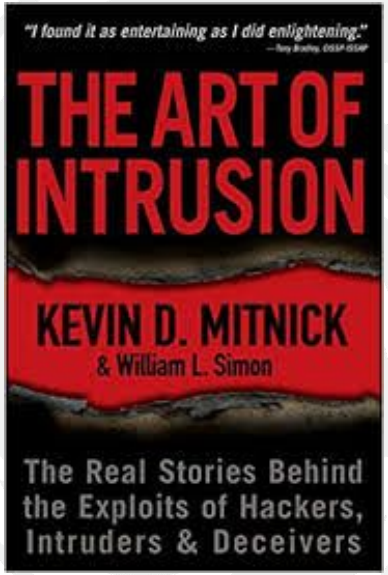
DESCRIPTION:

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: ...DOPM20PM13DIPM19PM09

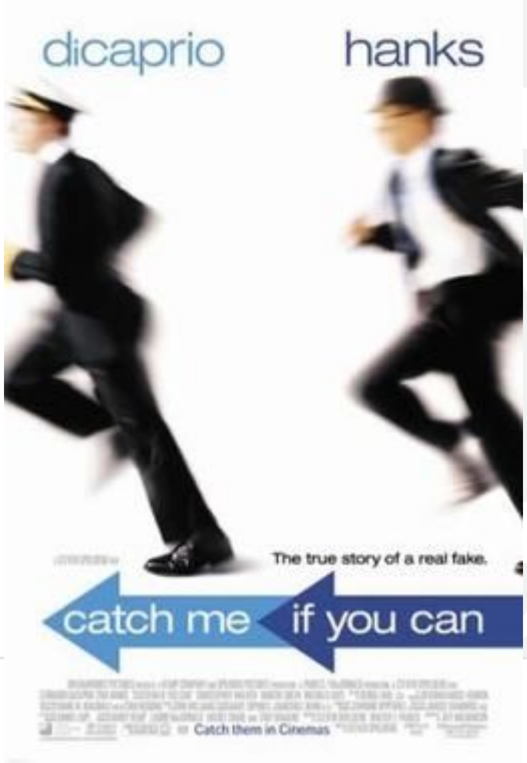
Kevin Mitnick


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak


"A MUST-READ IN THIS NEW WORLD." —STEVE WOZNIAK, COFOUNDER OF APPLE INC.
THE ART OF INVISIBILITY
The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data
AUTHOR OF THE NATIONAL BESTSELLER GHOST IN THE WIRES
KEVIN MITNICK
with Robert Vamosi
FOREWORD BY MIKKO HYPPONEN, CHIEF RESEARCH OFFICER OF F-SECURE


"I found it as entertaining as I did enlightening."
—Tony Bradley, CISSP-ISSAP
THE ART OF INTRUSION
KEVIN D. MITNICK
& William L. Simon
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Frank William Abagnale



Charles Ponzi

Thank you

And protect yourselves out there!