There's No Patch for Social Engineering

Decoding the Language of "African" Scam Letters

RSA CONFERENCE 2010

SECURITY DECODED

Davi Ottenheimer,
flyingpenguin LLC

Harriet Ottenheimer,
Kansas State University

March 2, 2010

Overview

Data

Three Perspectives

Application

RSA CONFERENCE 2010

SECURITY DECODED

Overview

"African" Scam Letters

Also known as "**419/Advance Fee Fraud**"

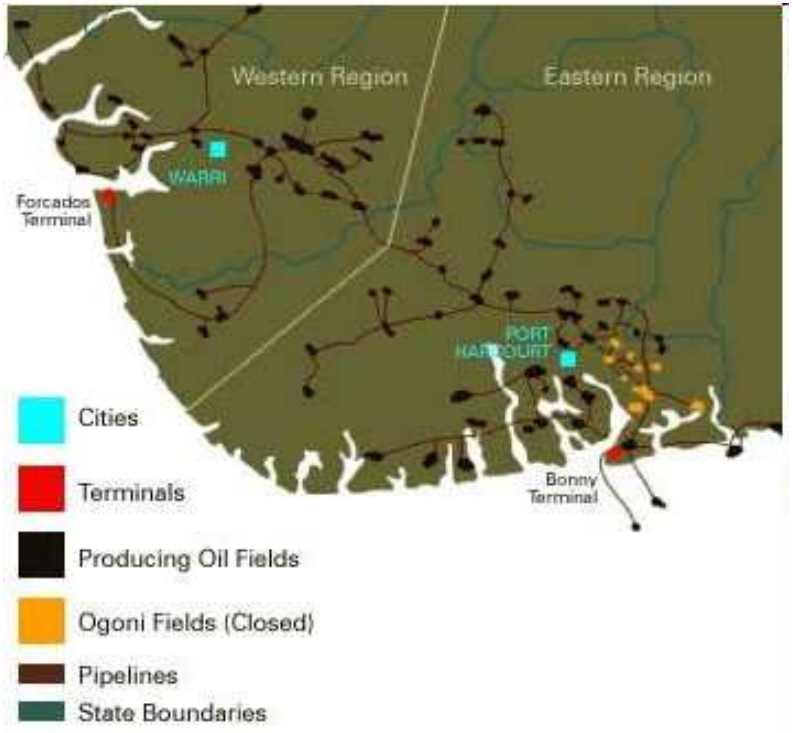
Speed Bump, copyright Dave Coverly

Definitions

- Email offers share in clandestine wealth
- Victims must pay “advance fees” for access
- Advance fees escalate endlessly
- Victims borrow or steal to continue payments

History

- 1980s rise after Nigerian oil crisis
- 1920s "Spanish Prisoner" scam variant
- Spread globally
- Spawned variations
  - African Prisoner
  - Lost/Stolen Wallet
  - Terminal Illness



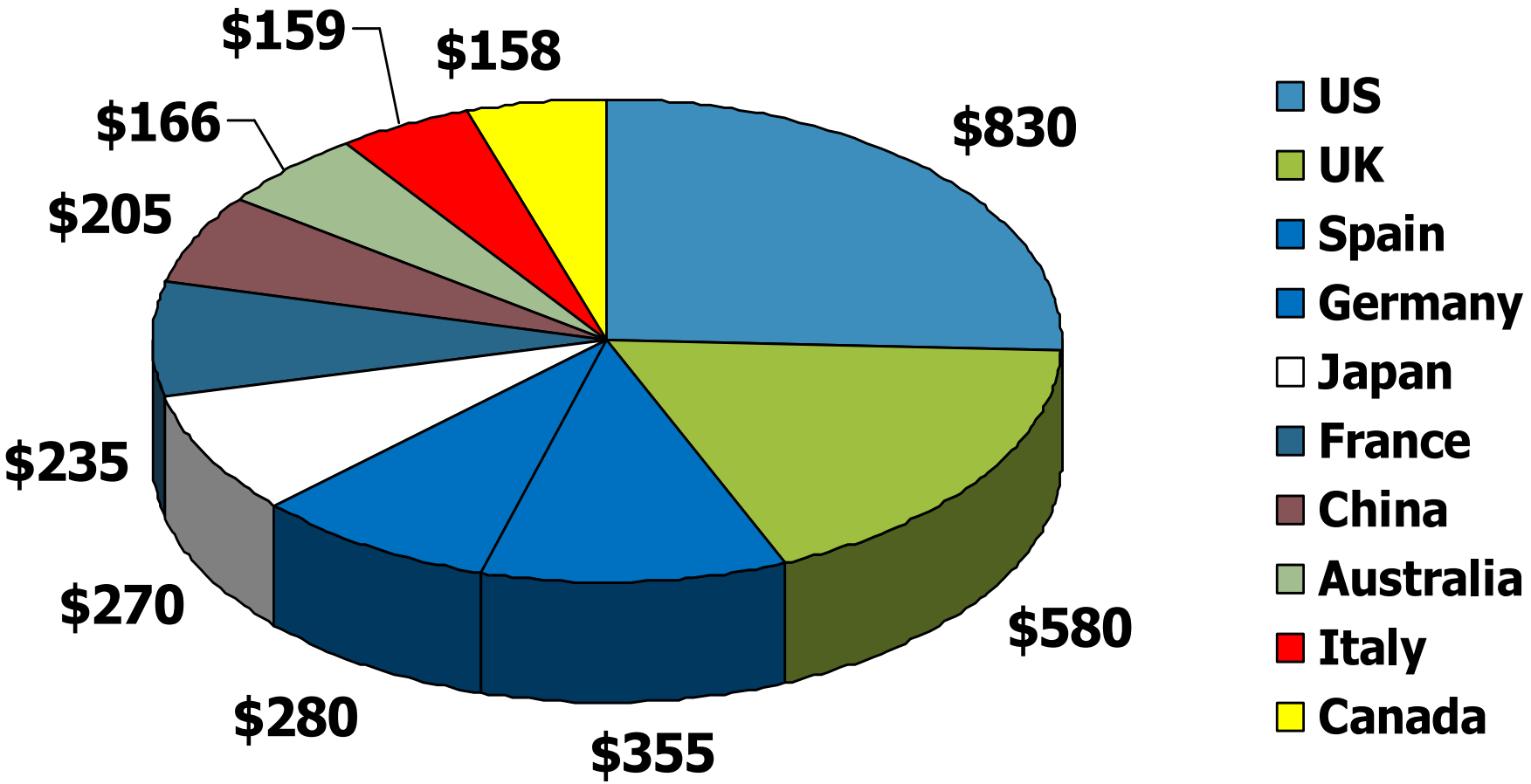
http://www.theoildrum.com/node/2348

Scope

- Since 1994 15 murders tied to 419 scams[1]
- 2005 global loss estimate at US$3 billion, one-half million victims in 37 countries.[2]
- 2007 loss estimate at US$4.3 billion (300 thousand – 12 million per case).[3]
- 2007 300,000 perpetrators estimated in over 69 countries; growth estimate of 3%.[4]

1. http://www.canada.com/nationalpost/news/issuesideas/story.html?ID=8a2dde06-dee9-47b3-b606-53f6b5b7b7d9
2, 3, 4. http://www.ultrascan-agi.com/public_html/html/419_statistics.html

Losses in 2007 (in millions)



http://www.ultrascan-agi.com/public_html/html/419_statistics.html

Brazil

- Resident active scam rings
  - 2006: 3
  - 2007: 4
- Individual members of scam rings
  - 2006: 24
  - 2007: 33
- Company and personal loss
  - 2006: 16 million US$
  - 2007: 22 million US$
- Career, job, or home loss in 2007
  - Careers or jobs: 32
  - Homes: 5

http://www.ultrascan-agi.com/public_html/html/419_statistics.html

Victim Profiles

- Michigan County Treasurer lost US$72,000 own funds then US$1.23 million in county funds in 2007[1]
- Professor of Psychiatry in California lost US$3 million to Nigeria over ten years (1996-2006)[2]
- Czech doctor (former intelligence agent) lost own retirement funds, then neighbors' funds (2003)[3]
- Top official, Banco Noroeste, São Paulo lost US$242 million bank funds over five years (1996-2001)[4]

1. http://mi.gov/ag/0,1607,7-164-34739-170122--,00.html
2. CBS News, March 2, 2006; Washington Post, May 28, 2006
3. http://allafrica.com/ February 21, 2003
4. http://business.timesonline.co.uk/tol/business/article1055200.ece.

RSA CONFERENCE 2010

SECURITY DECODED

Data

Gathering the Data

- 120 messages captured for analysis
  - One mailbox
  - Six-month capture-period
- 109 claimed African origins
- 11 claimed other origins
  - Brunei (1)
  - London, England (2)
  - Mauritius (1)
  - Philippines (2)
  - Taiwan (4)
  - Yugoslavia (1)

Tracing the Sources

- Untraceable (headers not saved): 4
- Blocked (but possible to identify region): 78
  - Africa: 46
  - Europe: 16
  - U.S.: 14
  - Middle East: 2
- Traceable: 38
  - Africa: 17 (***fewer than half!***)
  - U.S.: 12
  - Europe: 7
  - Hong Kong: 1

Examining the Content

- Identities
  - Family members
  - Civil servants
  - Bankers
- Subjects
  - Urgency (26)
  - Opportunity (25)
  - Appeals for assistance (19)
  - Confidentiality (4)

		african	non
bankers	28	22	6
sons	19	19	0
wives	18	16	2
wives' assts	2	2	0
contracts	15	14	1
corporate	10	10	0
govt	9	9	0
aides	8	8	0
daughters	3	2	1
military	1	1	0
investor	1	1	0
w farmer	1	1	0
captured	1	0	1
lottery admin	1	1?	0

RSA CONFERENCE 2010

SECURITY DECODED

Three Perspectives

Social Engineering

Investment Scams

Linguistic Anthropology

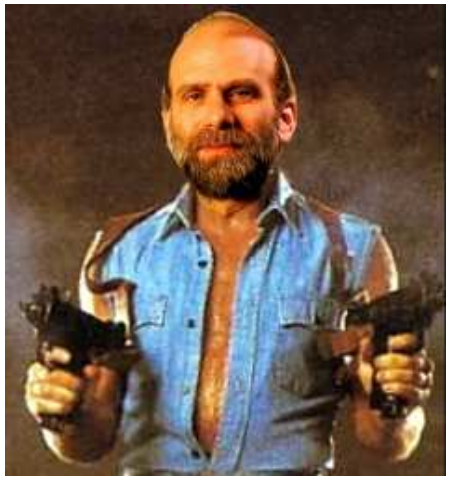
RSA CONFERENCE 2010

SECURITY DECODED

Social Engineering

Social Engineering

"You try to make an emotional connection with the person on the other side…. That is the whole idea: to create a sense of trust and then exploit it."[1]



"Amateurs hack systems, professionals hack people."[2]

1. Kevin Mitnick, *ZDNN*, July 17, 2000
2. Bruce Schneier, *The Economist*, November 01, 2002

Social Engineering Attacks

1. Responsibility
   - Use important sounding names
   - Invoke authority or official body
2. Opportunity
   - Offer of unique/competitive advantage
   - Chance for reward, profit, sex etc.
3. Relationship
   - Gaining incremental trust over time
   - Trying to fit-in, seem “regular”

Social Engineering Attacks

4. Morality
   - Invoking sense of duty or honor
   - Harm may come if no action taken
5. Guilt
   - Evoking empathy or sympathy
   - Appealing to moral values
   - Victim feels guilt if requests not granted
6. Samaritan
   - Abuse of helpfulness and generosity
   - Prey on moment (“hold the door, please”)

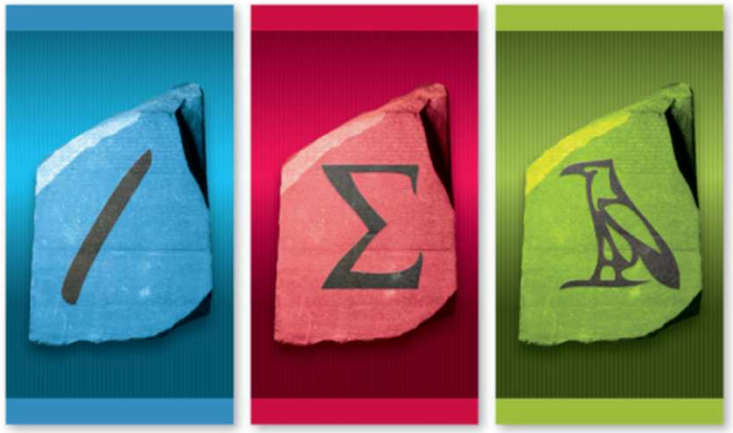
Social Engineering Attack Patterns

7. Reverse Samaritan
   - Offering to help victim
   - Providing “support” or reassurance
   - Being “reasonable” and patient
8. Validation
   - Pretending to have secret or classified information
   - Demonstrating inside knowledge
   - Official-looking uniform, letterhead, etc.
9. Urgency
   - Trying to force action without thought
   - Making an emotional appeal
   - Used in conjunction with others to increase chances of success

"African" Scam Letters

Combined social engineering attacks

1. Responsibility: dropping names
2. Opportunity: offering money
3. Relationship: establishing trust
4. Moral: invoking sense of honor
5. Guilt: evoking sympathy
6. Validation: implying access to secret information
7. Samaritan: appealing to sense of helpfulness
8. Reverse Samaritan: offering to share in wealth
9. Urgency: implying loss of opportunity



RSA CONFERENCE 2010

SECURITY DECODED

Investment Scams

Investment Scams

"Investors who have been victimized scored 10 percent higher on a financial literacy test."[1]

"Investment fraud victims appear to pay more attention to sales pitches, and to rely more on their own experience and knowledge in making their investment decisions."[2]

1. NASD 2006: 6-9
2. NASD 2006: 7

Investment Scam Attacks

1. Phantom Fixation
   - Dangling the prospect of wealth and riches
2. Source Scarcity
   - Making the product offered seem rare to increase its value
3. Source Credibility
   - Claiming to be from a known legitimate business
4. Comparison
   - Juxtaposing a more expensive price with the offered price
5. Friendship
   - Appearing to be the victim's friend

Investment Scam Attacks

6. Commitment
   - Victim commits early, con uses this against victim
7. Social Consensus
   - Con makes it seem like everyone else wants in
8. Reciprocity
   - Con does a small favor for the victim
9. Landscaping
   - Structuring interaction so all roads lead where con wants
10. Profiling
    - Identifying victim hot buttons through interaction, questioning

Investment Scam Attacks

11. Fear
    - Using intimidation to persuade the victim
12. Authority
    - Con plays the role of an authority figure in order to put the victim in a role as agent of that authority
13. Dependency
    - Con plays the role of a young, helpless dependent in order to put the victim in the role of a parent who will help, by buying whatever he or she is selling

"African" Scam Letters

Some investment scam attacks:

1. Phantom Fixation: huge sums of money available

3. Source Credibility: establishing "African" identity

6. Commitment: once started victim can't stop

8. Reciprocity: victim and con are "assisting" one another
9. Landscaping: each step/fee leads to another
10. Profiling: appealing to victim's sense of importance
11. Fear: of discovery; urgent need for secrecy
12. Authority: oil officials, bankers, military figures, royalty
13. Dependency: needing help from a smart foreigner

RSA CONFERENCE 2010

SECURITY DECODED

Linguistic Anthropology

Linguistic Anthropology

- Linguistic ideologies access vulnerabilities
- Ideas about languages and their speakers invoke ("index") stereotypes of those speakers
- Scammers use linguistic ideologies to convince victims of "authenticity"

"I therefore personally appeal to you seriously and religiously for your urgent assistance"

Indexes ideas about Africans

Linguistic Attack: Phonology

Punctuation and spacing errors

- "I am elder son of . Maj.General Gwazo former Military chief Security officer"
- "send me a letter ofInvitation, in other for me to get my Visa to join you up"

Capitalization errors

- "Dear sir, Before i start, i must first apologize"
- "I was opportune and pleasured to have come across your Contact though this satellite media"

Linguistic Attack: Morphology

Fancy words carefully spelled

- "my family has been subjected to all sorts of harassment and intimidation"
- "This money is now floating in the NPA domiciliary account"
- "Modalities have been worked out at the highest level"

De-contractions

- "Our status as refugees does not permit us to run an account here"
- "We do not know whom exactly to blame"
- "we can not leave the country"
- "my need to get some one to assist me"

Linguistic Attack: Syntax

Insertion of infinitives

- "that made me ***to*** contact you"

Unusual word order

- "money ***of which*** I am in possession"
- "***Since after*** the death of the Head of State"
- "we shall be ***coming over*** to your country"

Incorrect agreement

- "things get**s** better"
- "until my father is release"
- "The Federal Government ***have*** seized all our properties"

Florid style

"I am glad to say that with the introduction of Internet and website, I was opportune and pleasured to have come across your Contact though this satellite media"

"I therefore personally, appeal to you seriously and religiously for your urgent assistance to move this money into your country where I believe it will be safe since we can not leave the country due to the restriction of movement imposed on my father and the members of our family by the Nigerian Government."

"African" Scam Letters

Linguistic ideology invokes African stereotypes

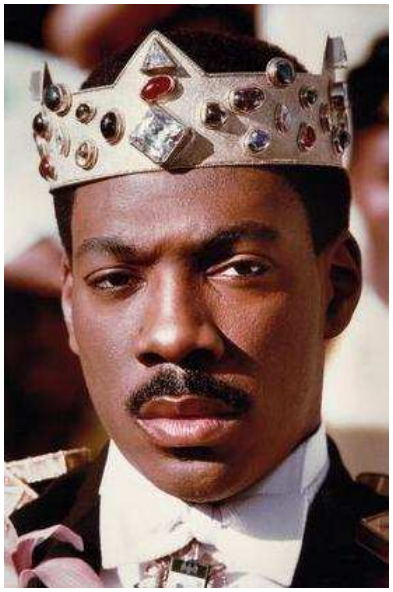
- Despotic dictators
- Political instability
- Widespread corruption
- Elite accumulation of wealth

"**His Excellency President for Life Field Marshal Al Hadji Dr. Idi Amin, VC, DSO, MC, Lord of All the Beasts of the Earth and Fishes of the Sea and Conqueror of the British Empire in Africa in General and Uganda in Particular**."

Is this the way Africans Talk?

"Coming to America" Movie Dialog

- Lisa: "Does everyone in Africa talk like you?"
- Akeem: "Why, do you not like it?"
- Lisa: "No, I love it. It's nice to be with a man who knows how to express himself"



Reinforced Stereotypes

"Sire, Akeem and I have exhausted our funds. Kindly send three hundred thousand American dollars immediately as we are in dire straits."

- Telegram from Semmi to King Joffer

“Real” African

Phonology (frequent misspellings)

“appreciated” (for “appreciate it”)

Morphology (many contractions)

“I’m so happy to hear about you.”

Syntax (generally correct, occasional odd ordering)

“2 watches for some one that doesn’t see very well”

Discourse (not very florid)

“I am very happy that I have known you.”

“Real” vs “Mock” African

African	Real	Mock
Misspellings	Frequent	Few
Contractions	Frequent	Few
Syntax	Correct	Incorrect
Florid Discourse	Some	Very

"Mock" African v. "Mock" Spanish

Mock	Spanish[1]	African
Awareness	Unconscious	Deliberate
Motive	Humor	Profit
Group	Dominant	Subordinate

Both index stereotypes

1. "Mock Spanish: A Site for the Unconscious Reproduction of Racism in American English" Jane Hill, 1995, Reprinted in H. Ottenheimer, 2006, The Anthropology of Language (Workbook/Reader.

Deliberateness of Mock African

"I was told to write like a classic novelist . . . very old world, very thick sentences. . . "

– **Alleged scammer**

"before I begin, let me caution you that this is an affair demanding the greatest secrecy, and that I should most probably lose the position I now hold, were it known that I confided it to any one. . . . I have received personal information, from a very high quarter, that a certain document of the last importance, has been purloined from the royal apartments."

– **Classic work of literature**

“Real” v. “Mock” African

Can you tell which are real?

1. “I did not forget you because you are the source of my success”
2. “Sorry to bother you too much but one day things will get better for me.”
3. “Since the death of my father the present government has been tormenting members of the Abachas family including family friends.”
4. “Even though I’m a very sad about loosing my favorite cousin i have [to] be strong, thank God for what happened, and pray for him”

RSA CONFERENCE 2010

SECURITY DECODED

Application

Guard Against Attacks

At individual level

- Identify attack signs
  - Recognize discourse ideologies and stereotypes
  - Check requests/offers carefully
- Take responsibility, take action
  - Follow “safe” computing practices
  - Record and report attack details to authorities

Guard Against Attacks

At organizational level

- Investigate and educate
- Apply controls with reasonable monitoring
- Cooperate with law enforcement

Know the enemy

Pride goes before a fall

There's No Patch for Social Engineering

Decoding the Language of "African" Scam Letters

RSA CONFERENCE 2010

SECURITY DECODED

Davi Ottenheimer,
flyingpenguin LLC

Harriet Ottenheimer,
Kansas State University

March 2, 2010