THE DIFFERENCE BETWEEN A KILLER DEAL AND A DEAL KILLER

MARKUS JAKOBSSON
PAYPAL
THAT DIFFERENCE IS OFTEN SMALL
PART 1/3:
DEALING WITH WEB SPOOFING

JOINT WORK WITH HOSSEIN SIADATI
Theory of When Spoofing Works

An attacker is successful if

1. The victim is tricked, and as a result
2. The victim acts, benefitting the attacker
Theory of When Spoofing Works

An attacker is successful if

1. The **victim** is **tricked**, and as a result
2. The **victim** acts, benefitting the attacker

Traditional countermeasures address **this** part (locks, colors, warnings – a user communication problem)
Theory of When Spoofing Works

An attacker is **successful** if

1. The **victim** is tricked, and as a result
2. The **victim acts**, benefitting the attacker

Can we address this instead?
Imagine a World Where...

GOOD SITE

Account login
Email address
PayPal password

Go to
My account
Log in

Problem with login?
New to PayPal? Sign up.

+ NAÏVE USER

NAÏVE USER (SAME ACTION)

= SUCCESS

SPOOF SITE

Account login
Email address
PayPal password

Go to
My account
Log in

Problem with login?
New to PayPal? Sign up.

+ NAÏVE USER (SAME ACTION)

= ABORT
Here is How to Do It!

On whitelist?

LOG IN NOW

Enter Password:

Y

N

ABORT
Feedback – but no instructions
Performance

![Graph showing performance over time for different student groups. The graph plots the percent of correct action against the day number. The A Students, B Students, and C Students are represented by different line styles. The A Students have a higher performance rate at 75%, followed by B Students at 15%, and C Students at 10%. The graph shows an initial steep increase in performance for A Students, followed by a plateau and slight decline. B Students show a more gradual increase, while C Students have the least consistent performance.]
PART 2/3: DISCOURAGING LYING
HOW LIES “SOLIDIFY”…
AND HOW TO AVOID IT!
EXPERIMENT DESIGN

- MOTIVE
- CRIME
- VARIOUS
- REACTION
- ABLE
EXPERIMENT DESIGN

MOTIVE

CRIME

VARIABLE

REACTION

Affiliate sends you a broken item.
Affiliate sends you a broken item.

You decide to order “and never receive”.

EXPERIMENT DESIGN
EXPERIMENT DESIGN

MOTIVE

CRIME

VARIABLE

ABLE

REACTION

Affiliate sends you a broken item.

You decide to order “and never receive”.

You select item, see photo/name of delivery.

You select item.
What would you do in this situation?

- I did not receive this item, and would like a replacement.
- I did not receive this item, and would like a refund.
- I did receive this item, but have changed my mind and would like to return it.
AN EXPERIMENT – RESULTS

Test: 304
- Liar: 24%
- Honest: 76%

Control: 318
- Liar: 64%
- Honest: 36%

TEST TREATMENT REDUCES LIES BY ~60%
HOW TO AVOID LIES

• Confront the user *before* he has committed to his lie
• Provide him with an “easy out” at the *tipping point*
EXPERIMENT NUMBER 2

MOTIVE

CRIME

VARIABLE

ABLE

REACTION

Affiliate sends you a broken item.

You decide to order “and never receive”.

You select item, told “was your computer”.

You select item.
EXPERIMENT NUMBER 2

Affiliate sends you a broken item.

You decide to order “and never receive”.

You select item, told “was your computer”.

You select item.

TEST TREATMENT REDUCES LIES BY ~30%
HOW TO AVOID LIES

• Order matters: evidence first, decision second
• Always build an emergency exit
• Concrete evidence is more helpful
• Some confrontation hurts the honest – other does not
PART 3/3:

DERIVED PINS

JOINT WORK WITH DEBIN LIU
SOME BAD PINS

1234
2580
Your spouse’s birthday PINs you forget
“Friction”
WHAT WILL USERS SEE

Account Login

Email Address
bobr@aol.com

PayPal PIN

Your PIN is the first four characters of your password

1 2 3
4 5 6
7 8 9
0 + * #
EXAMPLE USER MAPPING

“Blu2thRules” → “2582”
Access; Truncate; Map; Store
Dual Universes
MORE DETAILS

www.spoofkiller.com
www.derivedPIN.com

... or email me at majakobsson@paypal.com ...