INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

Set Theory for Hackers

uid=1027(pruby) gid=0(insomnia)

Apology: Clickbait

16/11/2018

$\forall$ D $\in$ My Dumplings:

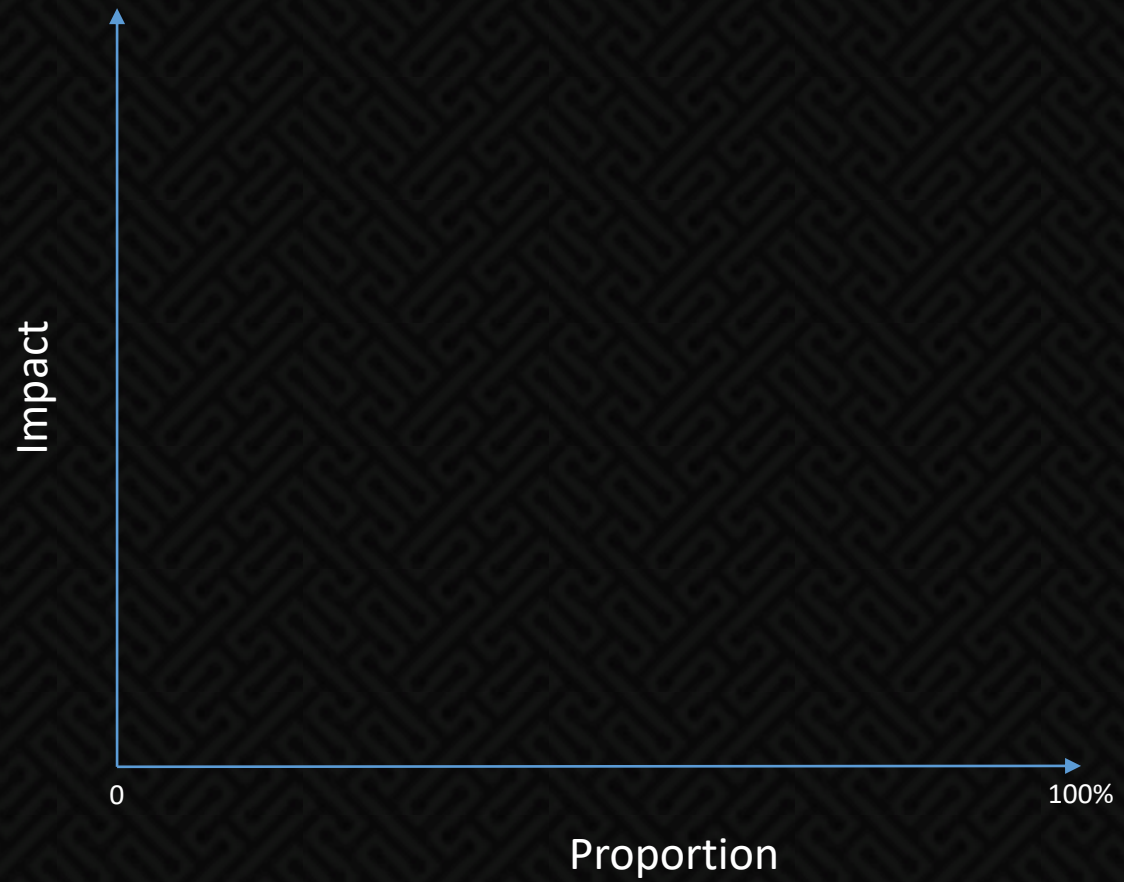
D contains

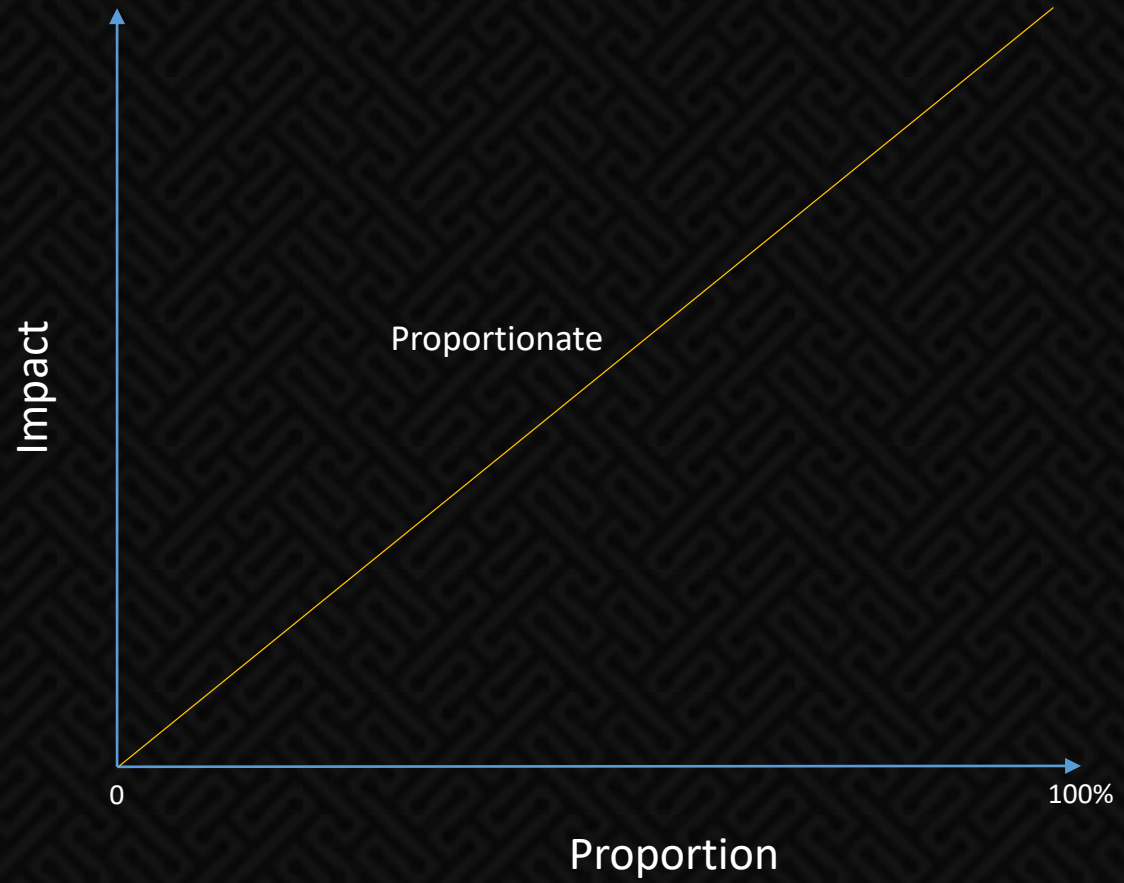
⇒ om nom nom

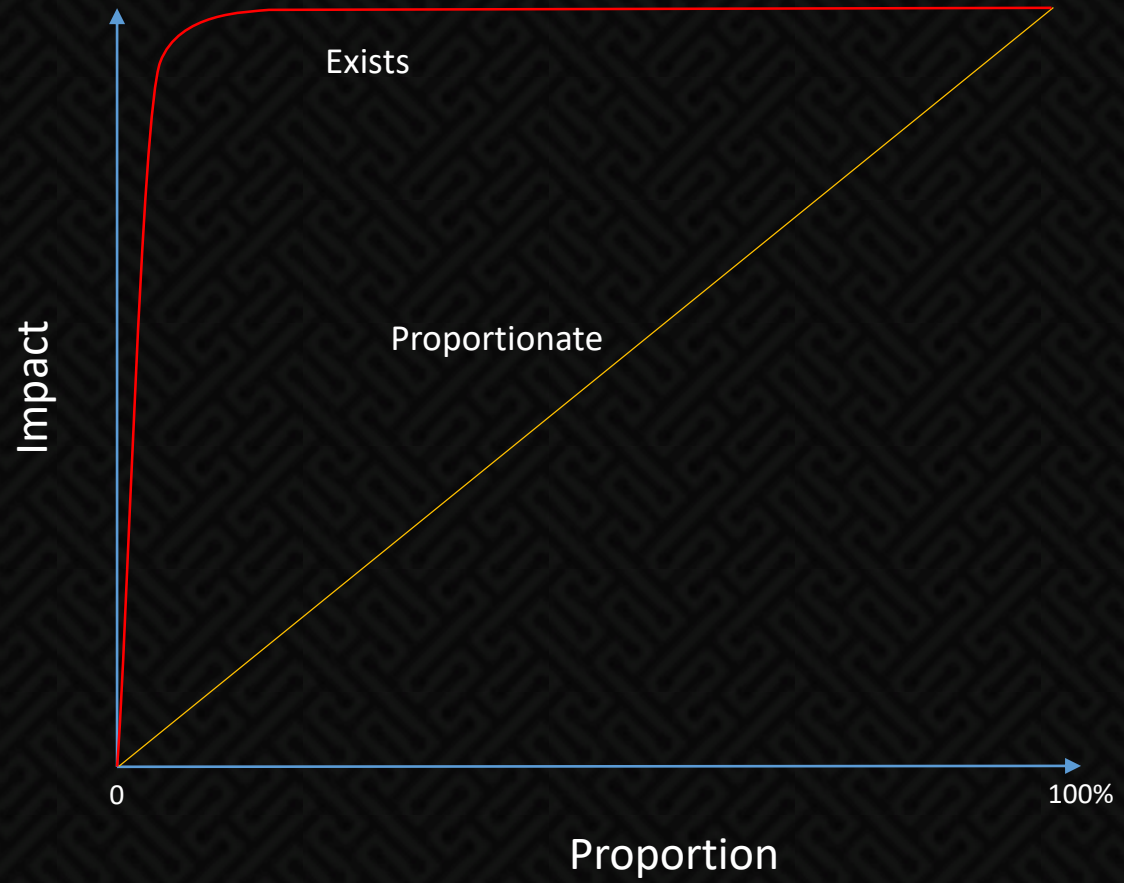
∃ D ∈ My Dumplings:

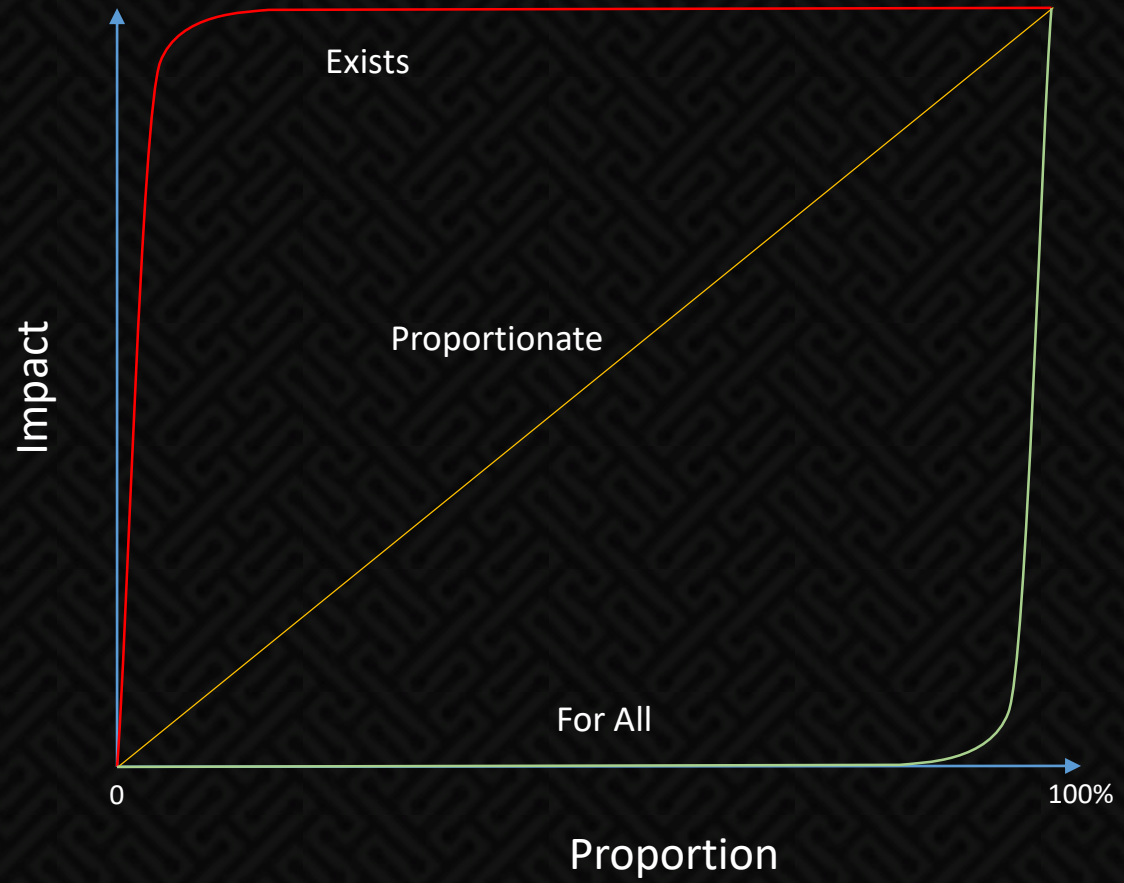
D contains

⇒ bluuurgh


Impact
0
100%
Proportion


Impact
Proportionate
0
100%
Proportion


Exists
Proportionate
Impact
0
100%
Proportion


Exists
Proportionate
For All
Impact
0
100%
Proportion

Example:
Phishing

200 Staff

Trusted Corporate Network

Act on email ⇒ Attacker on Network

$\exists$ S $\in$ My Staff:

S Follows Email Instructions

⇒ Breach

∀ S ∈ My Staff:

S Ignores Bad Email

⇒ Attack Failed

Direct Response:

“Don’t Click”

Initially lots of clicks…

Months of Work…

Only 1% Click! Celebrate!

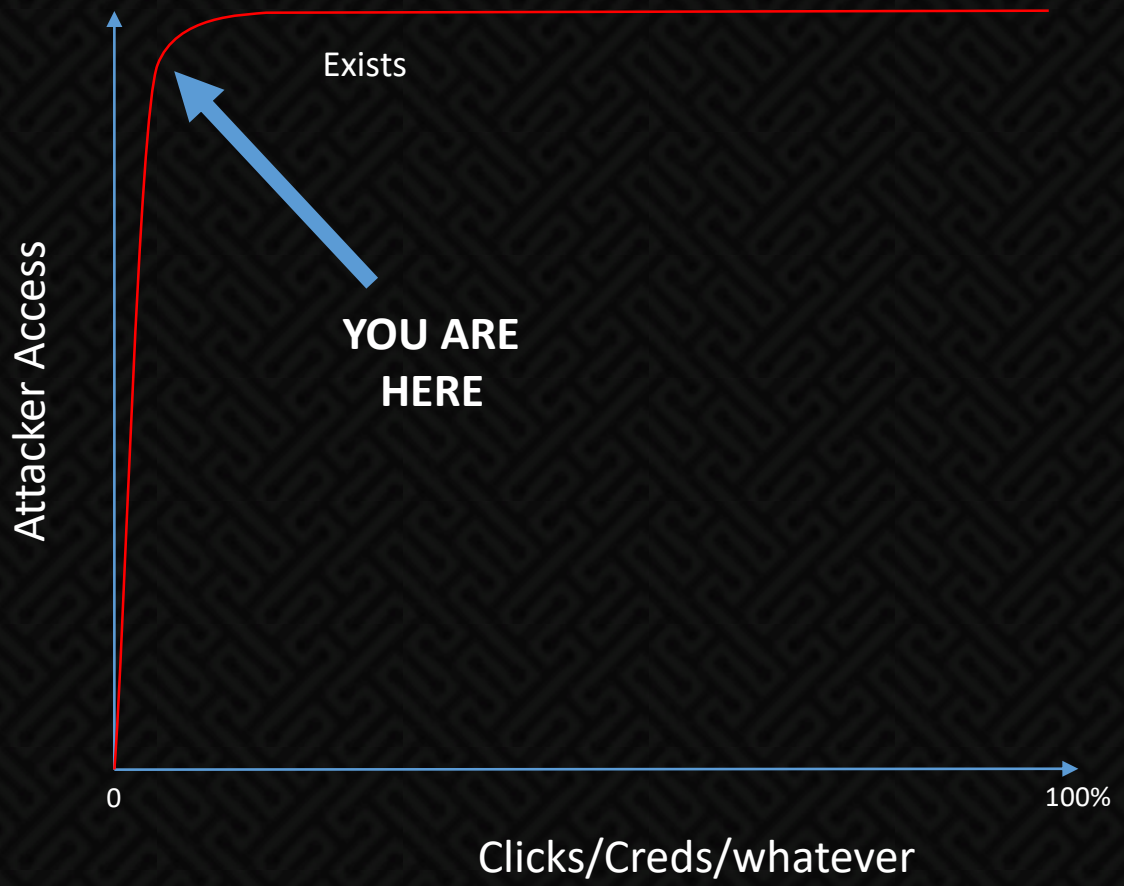
What impact?

… model it out

$$(0.99)^{200} = 0.134$$

86.6% Attacker Wins

What went wrong?

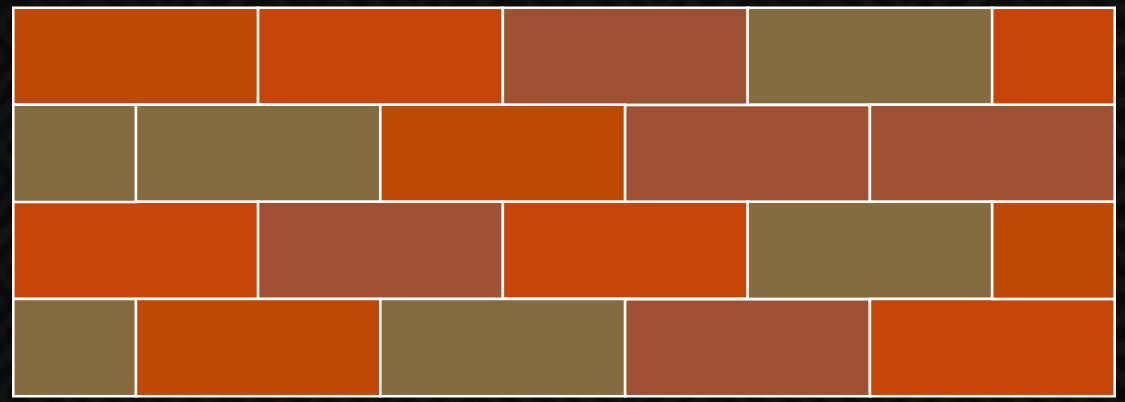

Exists
YOU ARE HERE
Attacker Access
0
100%
Clicks/Creds/whatever

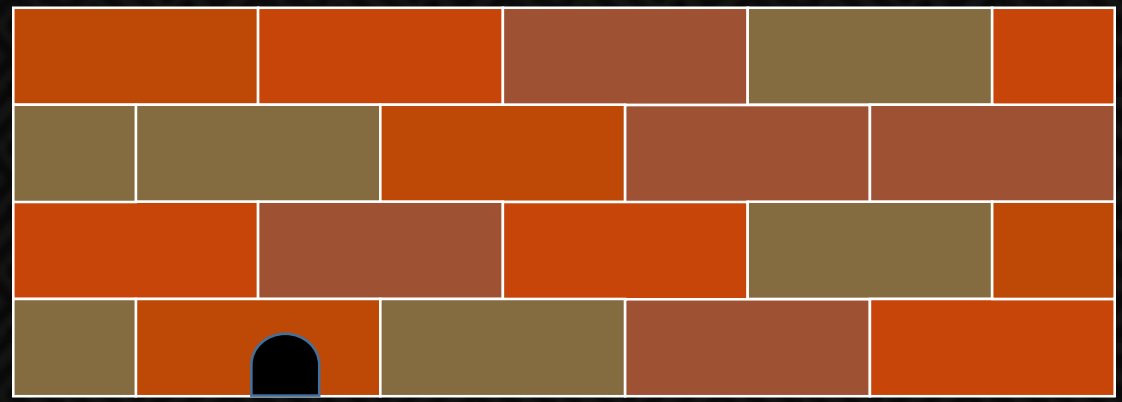
In general we can:

Target Individual Odds

(Diminishing Returns @ Extremes)

16/11/2018





?

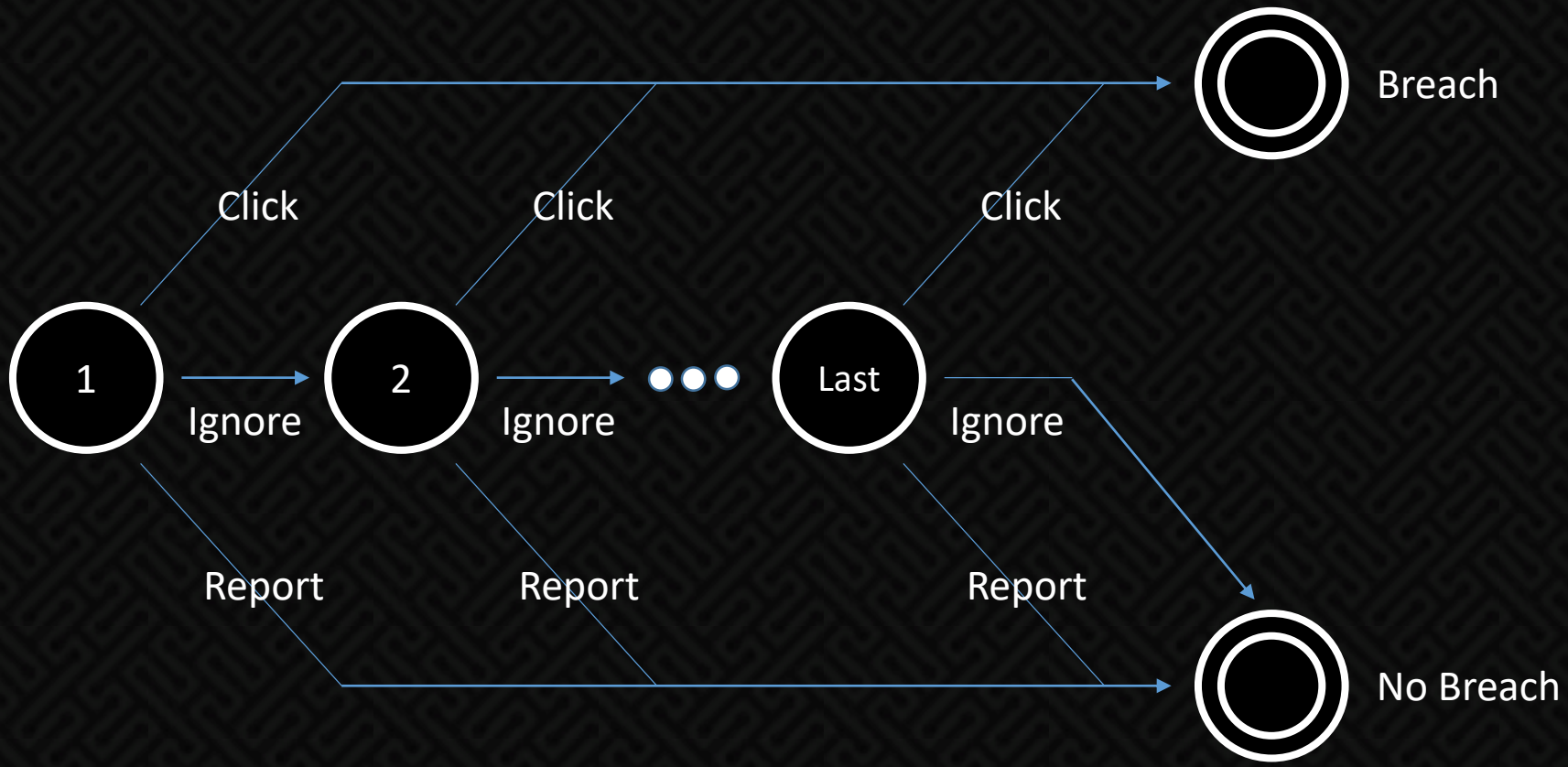
$\exists$ S $\in$ My Staff:

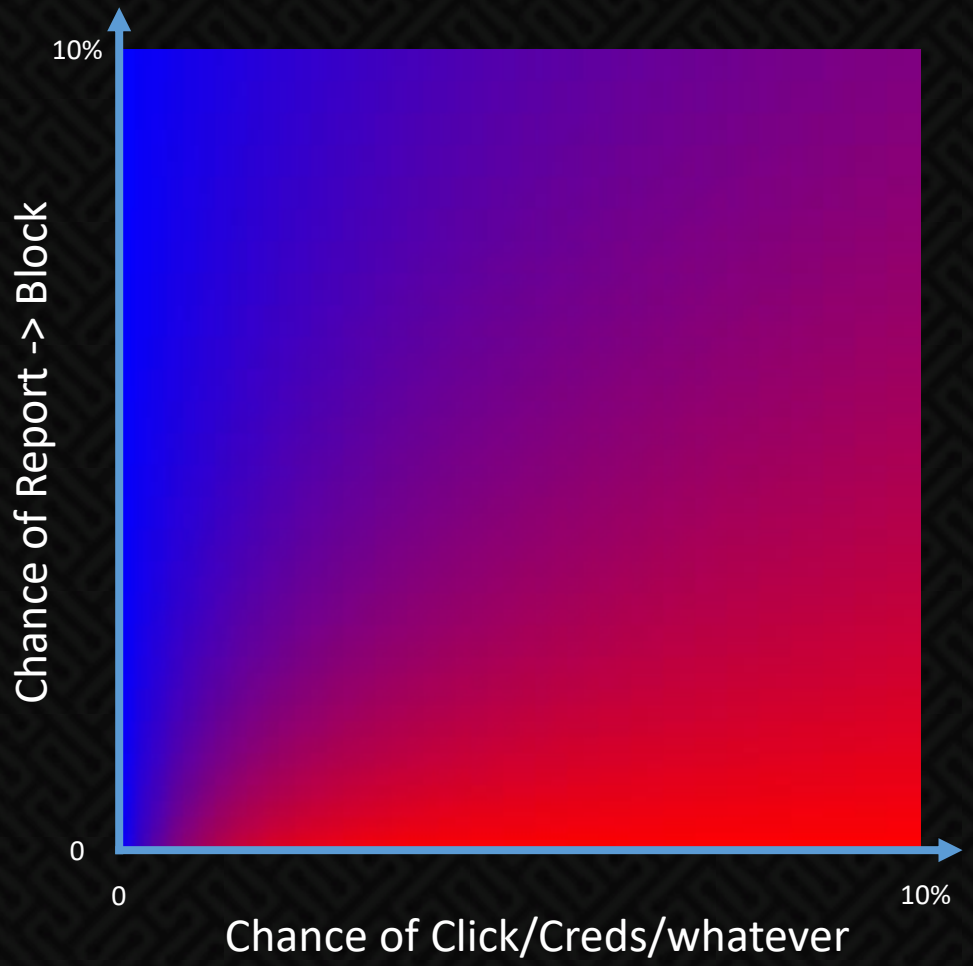
S Reports Attack

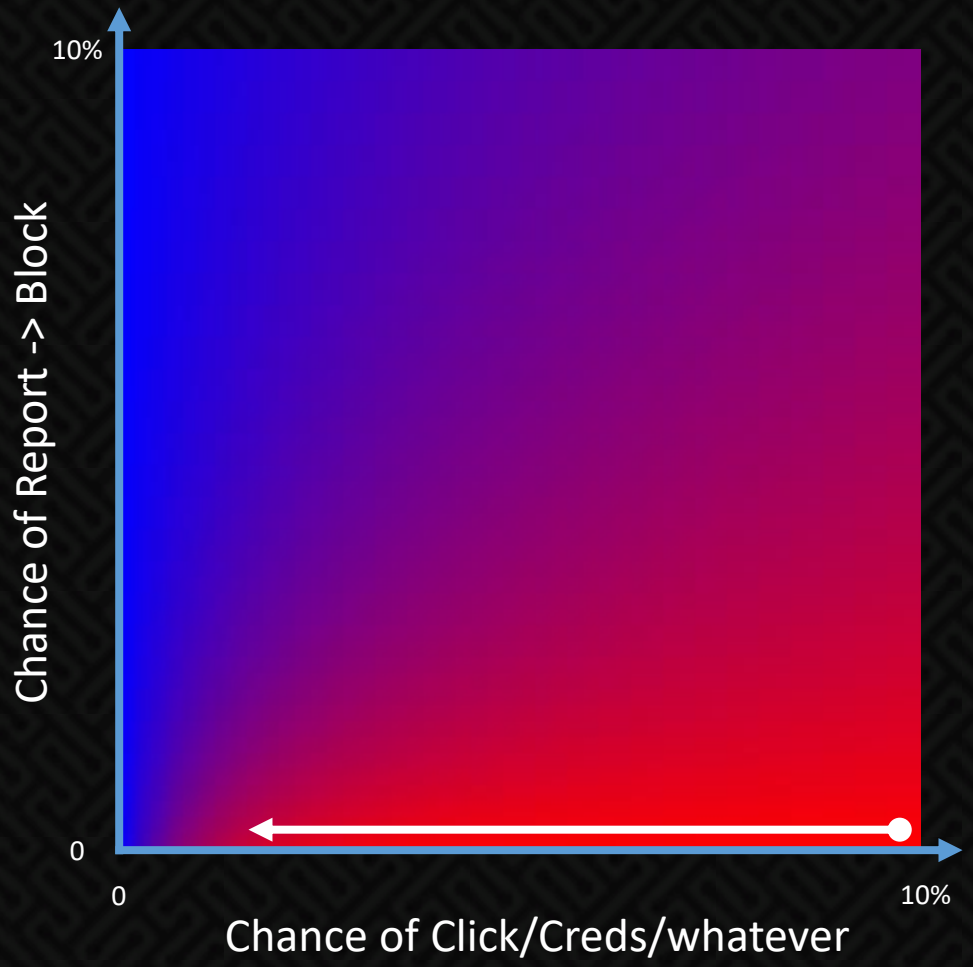
and we can block it

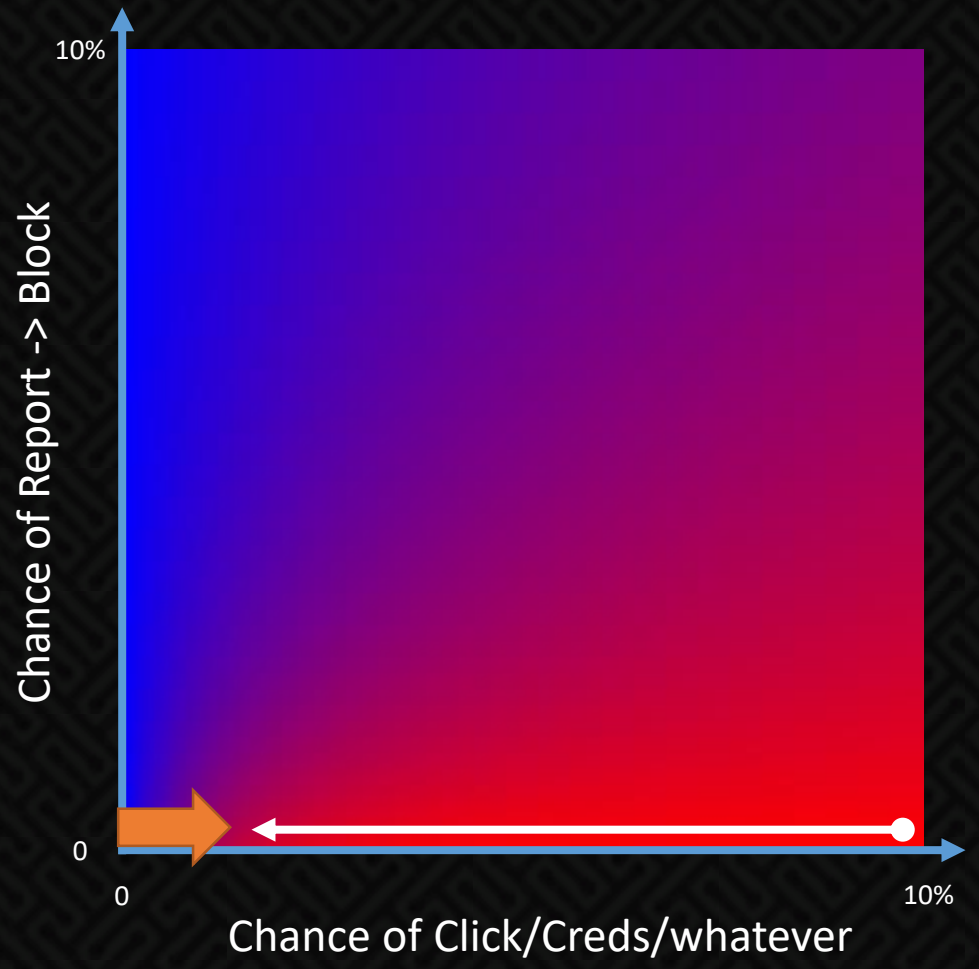
⇒ This Attack Fails

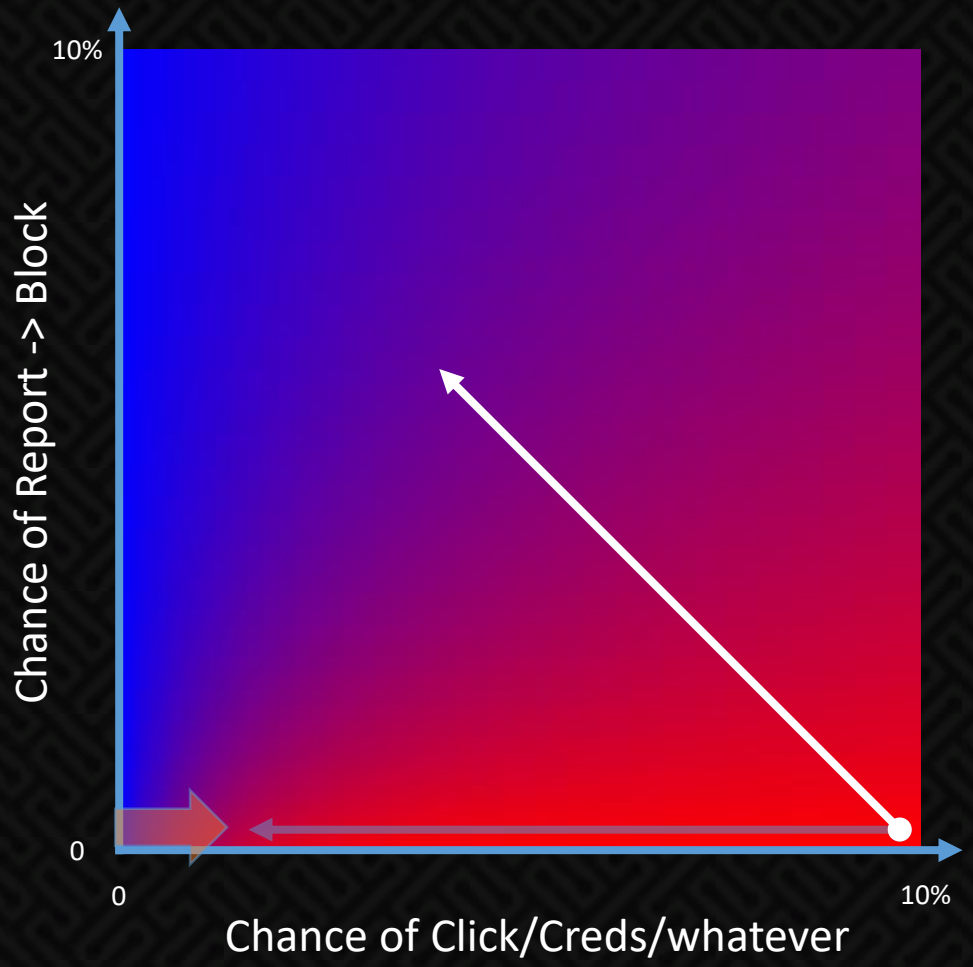
Against all later openers


Breach
Click
Click
Click
1
Ignore
2
Ignore
Last
Ignore
Report
Report
Report
No Breach


10%
Chance of Report -> Block
0
0
10%
Chance of Click/Creds/whatever


10%
Chance of Report -> Block
0
0
10%
Chance of Click/Creds/whatever


10%
Chance of Report -> Block
0
0
10%
Chance of Click/Creds/whatever


10%
Chance of Report -> Block
0
0
10%
Chance of Click/Creds/whatever

General Concept

∀ vs. ∃
Fight!

K.O.
∃ wins

Are You on the Right Side?

Models can help…

16/11/2018