



SECURING CODE THROUGH SOCIAL ENGINEERING

CHRISTINA CAMILLERI
@0XKITTY



WHO AM I?



WHO AM I?

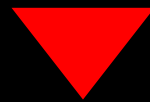


WHO AM I?





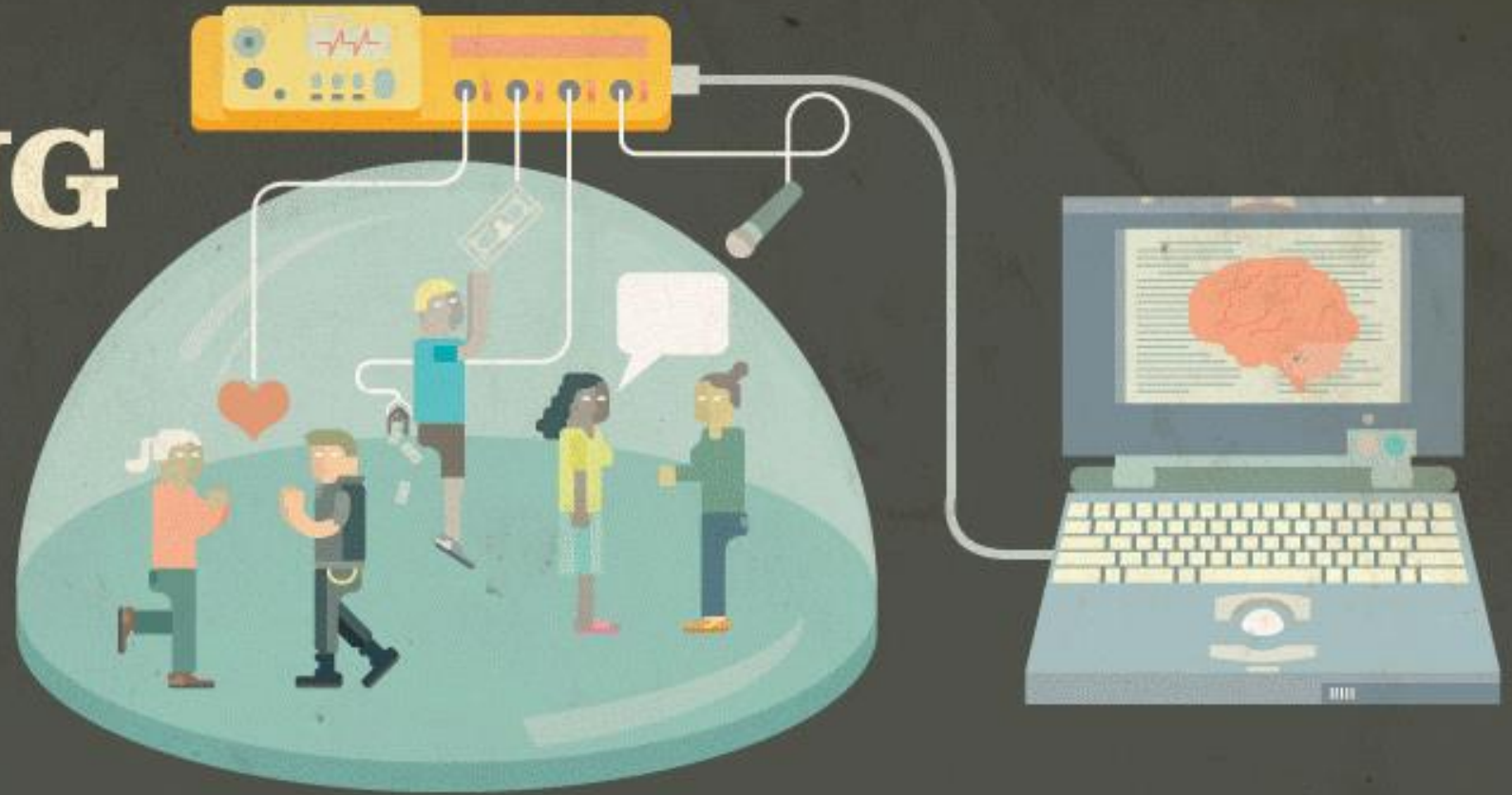
LET'S GET OUR HANDS DIRTY



WHAT IS SOCIAL ENGINEERING?

HACKING THE MIND

A look inside how and why
social engineering works.



**WHAT EXACTLY
IS SOCIAL
ENGINEERING?**

THE ART OF MANIPULATING PEOPLE INTO PERFORMING ACTIONS OR DIVULGING CONFIDENTIAL INFORMATION. WHY BOTHER DEVELOPING AND PLANNING A SOPHISTICATED TECHNICAL HACK WHEN YOU COULD JUST TRICK SOMEONE INTO GIVING YOU ACCESS TO ANYTHING YOU WANT?

AN EXPLOITATION OF **TRUST**

SOMEONE WHO CAN **LEVERAGE THE TRUST** OF THEIR VICTIM TO GAIN ACCESS TO SENSITIVE INFORMATION OR RESOURCES OR TO ELICIT INFORMATION ABOUT THOSE RESOURCES



WE ARE PROFESSIONAL LIARS.

* NOT ACTUALLY A BAD PERSON

WE ARE PROFESSIONAL LIARS.

PEOPLE ARE **VULNERABLE**

AND WE **ARE LAZY.**

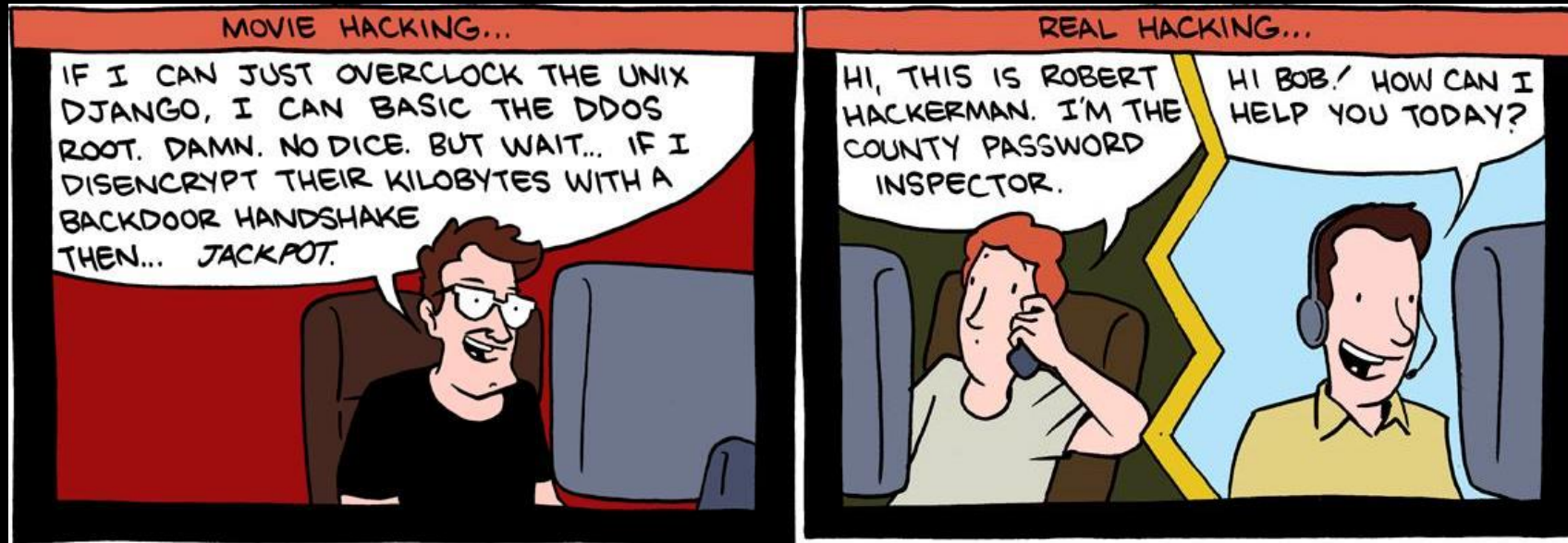
AND WE **WANT TO BE HELPFUL.**

AND WE **WANT TO BE NOTICED.**



LET ME TELL YOU A **STORY.**





AND SOCIAL ENGINEERING IS
THE PATH OF LEAST RESISTANCE.



THE **BIGGEST** ISSUE WE FACE IN INFOSEC.



PATCHING BUGS ! = PATCHING HUMANS



WE ARE THE ROOT OF ALL EVIL, AND THE
REASON FOR ALL SECURITY ISSUES.



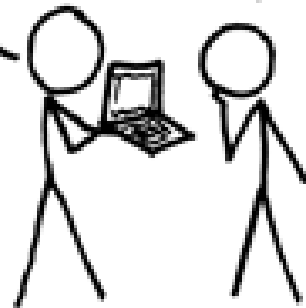
THERE IS NO PATCH FOR HUMAN STUPIDITY.

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

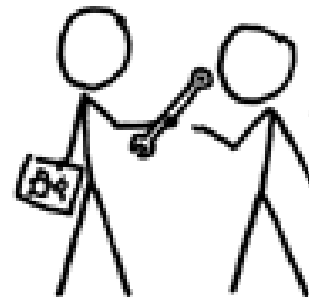
NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



TECHNICAL SYSTEMS ARE:

REVIEWED

SCANNED

PENETRATION TESTED



BUT...



HOW DO WE
MEASURE
VULNERABILITY
IN PEOPLE?



WE DON'T.

WE SHAME AND BLAME.

WE MAKE THEM FEEL BAD FOR THEIR BEHAVIOR.

WE ARE **IGNORANT.**

*AND WE'RE NOT DOING ANYTHING TO EFFECTIVELY CHANGE THIS.

WE AVOID TESTING BECAUSE IT MAKES US
FEEL **VULNERABLE.**



AND WE DON'T LIKE TO FEEL **VULNERABLE.**



PSYCHOLOGY + TECHNOLOGY = 



WE FALL VICTIM TO BASIC PSYCHOLOGICAL
AND PHYSICAL NEEDS:



CIALDINI 6



Pip-Boy

STAT INV DATA MAP RADIO RT
STATUS SPECIAL PERKS

AUTHORITY



HP 90/90

LEVEL 1



AP 70/70

STAT
INV
DATA
MAP
RADIO

RADS



TUNE



Y PERK CHART

POWER



Pip-Boy

STAT INV DATA MAP RADIO [RT]
STATUS SPECIAL PERKS

AUTHORITY



LIKING

HP 90/90

LEVEL 1

AP 70/70

STAT
INV
DATA
MAP
RADIO

RADS



TUNE



[Y] PERK CHART

POWER



Pip-Boy

STAT INV DATA MAP RADIO [RT]
STATUS SPECIAL PERKS

AUTHORITY



LIKING

SOCIAL PROOF

HP 90/90

LEVEL 1

AP 70/70

[Y] PERK CHART

STAT
INV
DATA
MAP
RADIO

RADS



TUNE



POWER



Pip-Boy

STAT INV DATA MAP RADIO [RT]
STATUS SPECIAL PERKS

AUTHORITY



LIKING

SOCIAL PROOF

COMMITMENT AND CONSISTENCY

HP 90/90

LEVEL 1 A horizontal green progress bar representing the current level and progress.

AP 70/70

STAT
INV
DATA
MAP
RADIO

RADS



TUNE



[Y] PERK CHART

POWER



Pip-Boy

STAT INV DATA MAP RADIO [RT]
STATUS SPECIAL PERKS

AUTHORITY



LIKING

RECIPROCITY

SOCIAL PROOF

COMMITMENT AND CONSISTENCY

HP 90/90

LEVEL 1

AP 70/70

STAT
INV
DATA
MAP
RADIO

RADS



TUNE



[Y] PERK CHART

POWER



Pip-Boy

STAT INV DATA MAP RADIO [RT]
STATUS SPECIAL PERKS

AUTHORITY

SCARCITY

LIKING

RECIPROCITY

SOCIAL PROOF

COMMITMENT AND CONSISTENCY



HP 90/90

LEVEL 1

AP 70/70

STAT
INV
DATA
MAP
RADIO

RADS



TUNE



[Y] PERK CHART

POWER



LET ME TELL YOU ANOTHER STORY.



\$Password1



LET ME SHOW YOU **HOW.**



INFORMATION GATHERING



DEVELOPING A RELATIONSHIP



EXPLOITATION

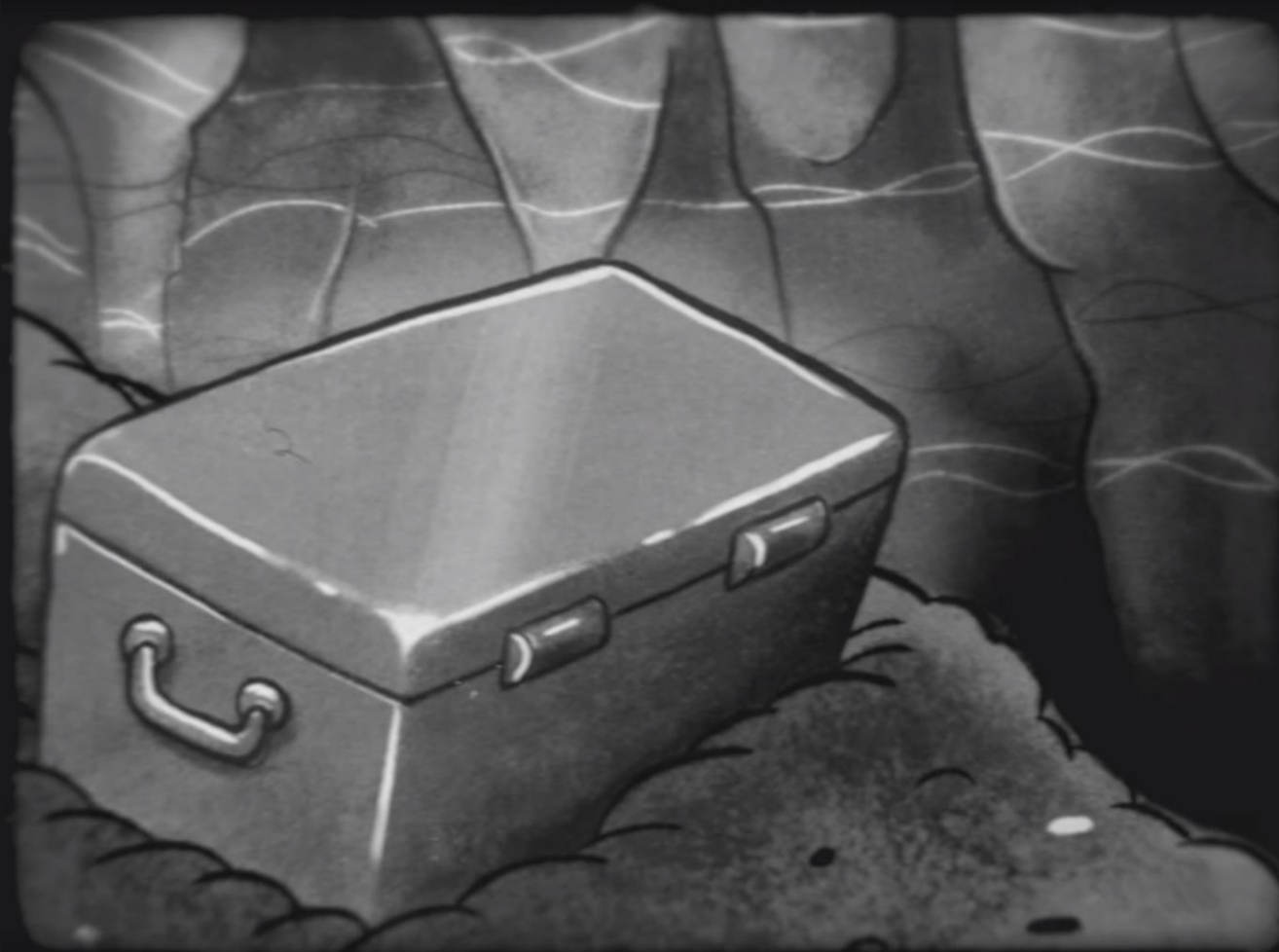


EXECUTION



LET'S FOCUS ON YOU.





DEVELOPERS = GOOD




HACKERS/SOCIAL ENGINEERS = **BAD**?

OPPORTUNITY

M77



A man in a red polo shirt and blue jeans is looking down at a white rope he is holding. He is standing on a grassy field. To his right, a man in a tan shirt and a wide-brimmed hat is looking towards him. In the background, there are other people and trees.

I have a permit.

Citytv

WHAT ARE WE OVERLOOKING?



WE NEED TO **STOP** BEING **GOOD**.



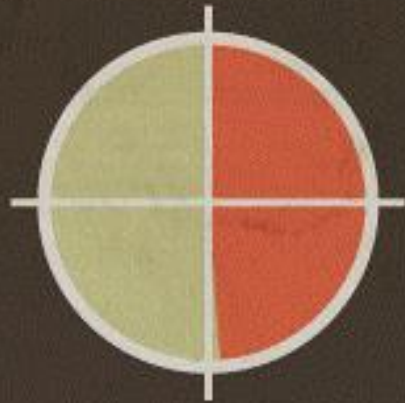
WHAT ARE WE DOING **WRONG**?



WHO IS TARGETED?



EVERYONE



48% of enterprises have been victims of social engineering attacks.



86% of IT and security professionals are aware of the risks of social engineering.



75% success rate with social engineering phone calls to businesses.

ALMOST EVERYTHING.



WE WATCH VIDEOS



WE WATCH VIDEOS

WE DO E-LEARNING MODULES



WE WATCH VIDEOS

WE DO E-LEARNING MODULES

WE TICK BOXES



WE WATCH VIDEOS

WE DO E-LEARNING MODULES

WE TICK BOXES

WE MAKE POSTERS



WE WATCH VIDEOS

WE DO E-LEARNING MODULES

WE TICK BOXES

WE MAKE POSTERS

WE BECOME PCI DSS COMPLAINT





NO.



SOPHISTICATED ATTACKS

VS

SOCIAL ENGINEERING



THE **FIX**?



THE **FIX**?
IN 5 EASY STEPS!





BE OBJECTIVE



BE DESTRUCTIVE



BE PARANOID



DON'T SHAME AND BLAME



AND...HAVE FUN

VIDEO!



TL;DR: RENEW YOUR PROCESSES





QUESTIONS?

SPECIAL THANKS: @LADY_NERD, @LITTLEJOETABLES

CHRISTINA CAMILLERI

@0XKITTY



