NEVER SURRENDER

REDUCING SOCIAL ENGINEERING RISK

ROB RAGAN
@SWEEPTHATLEG

CHRISTINA CAMILLERI
@0XKITTY

SHOWER FOO

I'm the voice inside your head / You refuse to hear / I'm the face that you have to face / Mirroring your stare

Genius Annotation by FeeeelMe and pizza-n-mandolino

He's your conscience.

WHAT IF I SAY I'M NOT LIKE THE OTHERS

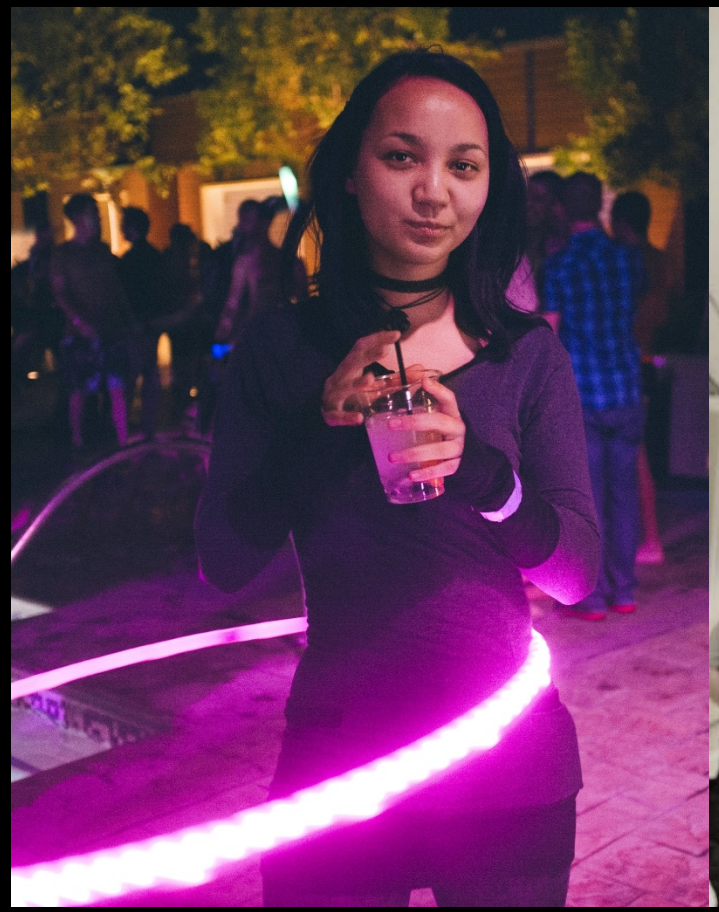
WHAT IF I SAY I'M NOT JUST ANOTHER ONE OF YOUR PLAYS

YOU'RE THE PRETENDER

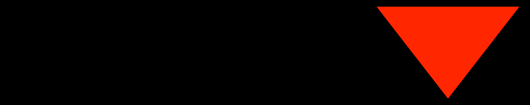
WHAT IF I SAY I WILL

NEVER SURRENDER

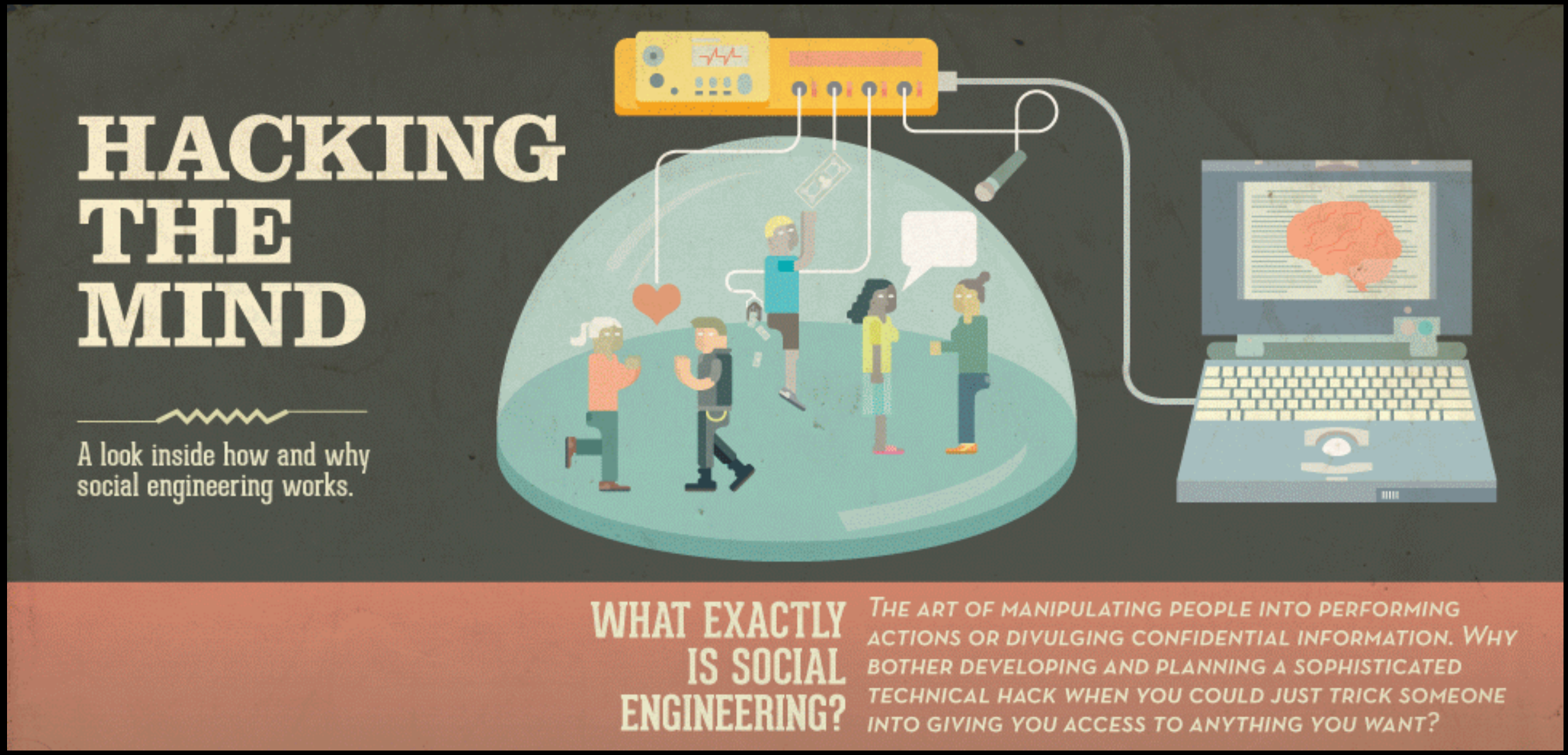
WHO THE...



LET'S GET OUR HANDS DIRTY



WHAT IS SOCIAL ENGINEERING?



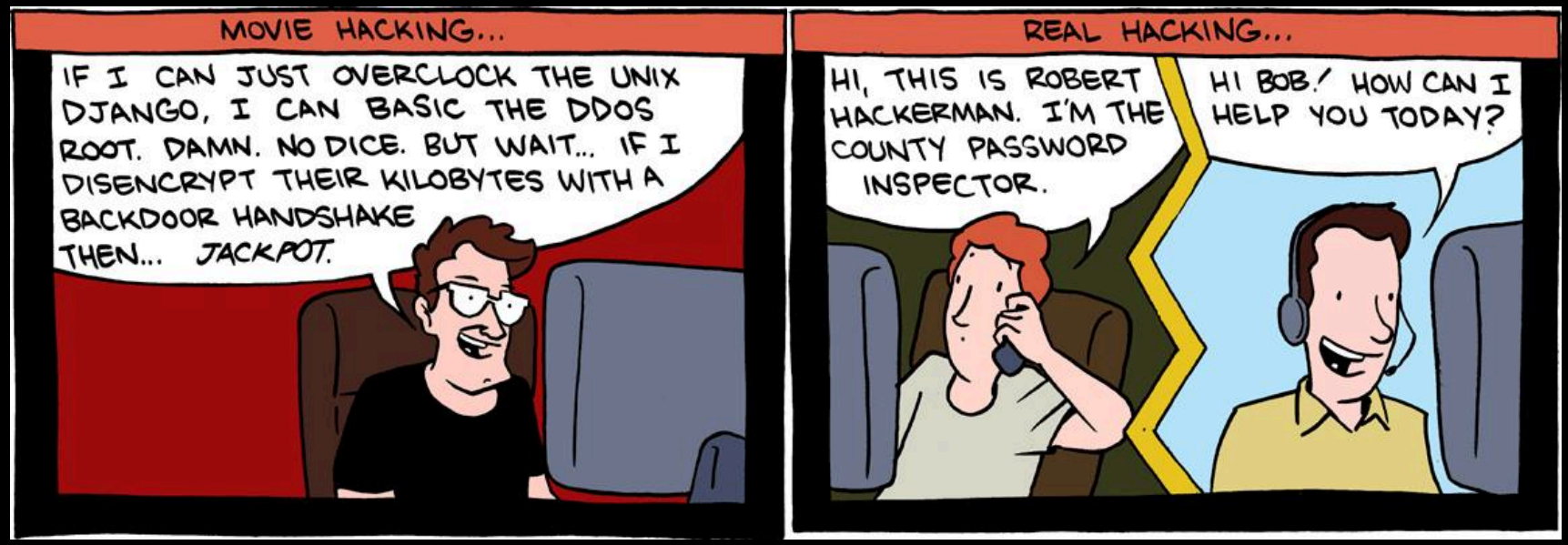
AN EXPLOITATION OF **TRUST**

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.

PEOPLE ARE **VULNERABLE**

AND WE ARE LAZY
AND WE WANT TO BE HELPFUL
AND WE WANT TO BE NOTICED.

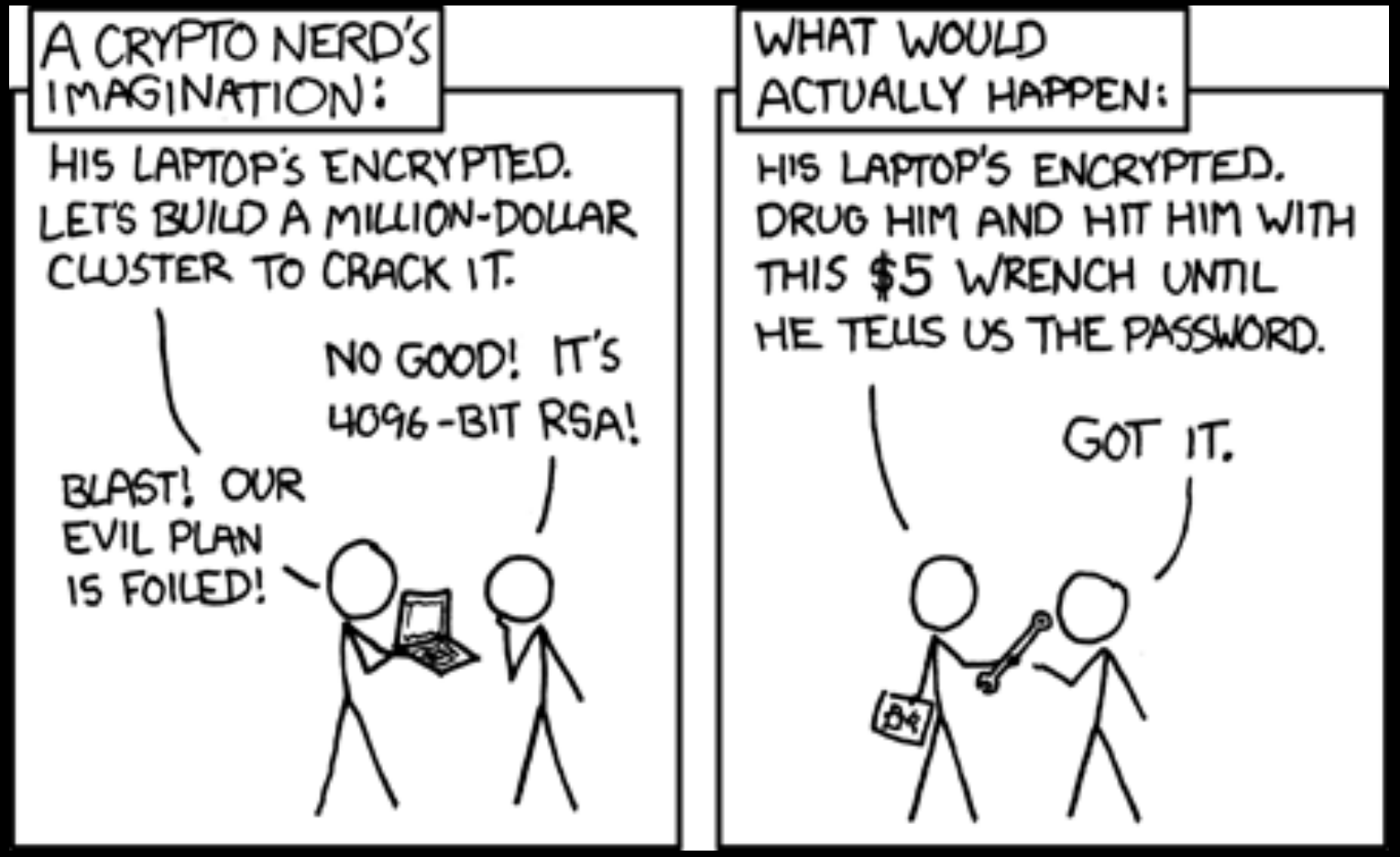


AND SOCIAL ENGINEERING IS THE PATH OF LEAST RESISTANCE.

THE BIGGEST ISSUE WE FACE IN INFOSEC.

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

THERE IS NO PATCH FOR HUMAN STUPIDITY.



PEOPLE – PSYCHOLOGY

COMPUTERS – TECHNOLOGY

WHEN IT COMES TO SECURITY, WE ARE **UNRELIABLE**.

TECHNICAL SYSTEMS ARE:

REVIEWED

SCANNED

PENETRATION TESTED

BUT...

HOW DO WE MEASURE VULNERABILITY IN PEOPLE?

WE DON'T.

WE SHAME AND BLAME.

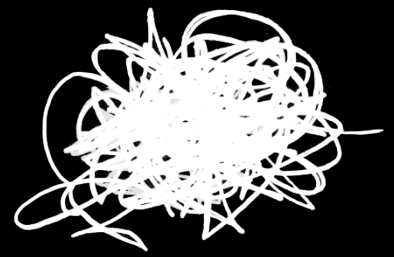
WE MAKE THEM FEEL BAD FOR THEIR BEHAVIOR.

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

AUTHORITY

LIKING

SOCIAL PROOF

SCARCITY

RECIPROCITY

COMMITMENT AND CONSISTENCY

LET ME TELL YOU A STORY.

LET ME SHOW YOU HOW.

INFORMATION GATHERING

▼

DEVELOPING A RELATIONSHIP

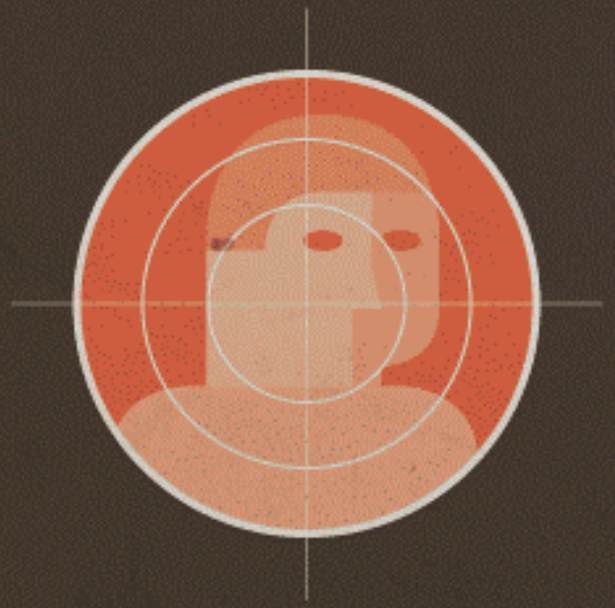
▼

EXPLOITATION

▼

EXECUTION

WHAT ARE WE DOING WRONG?



WHO IS TARGETED?

EVERYONE

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

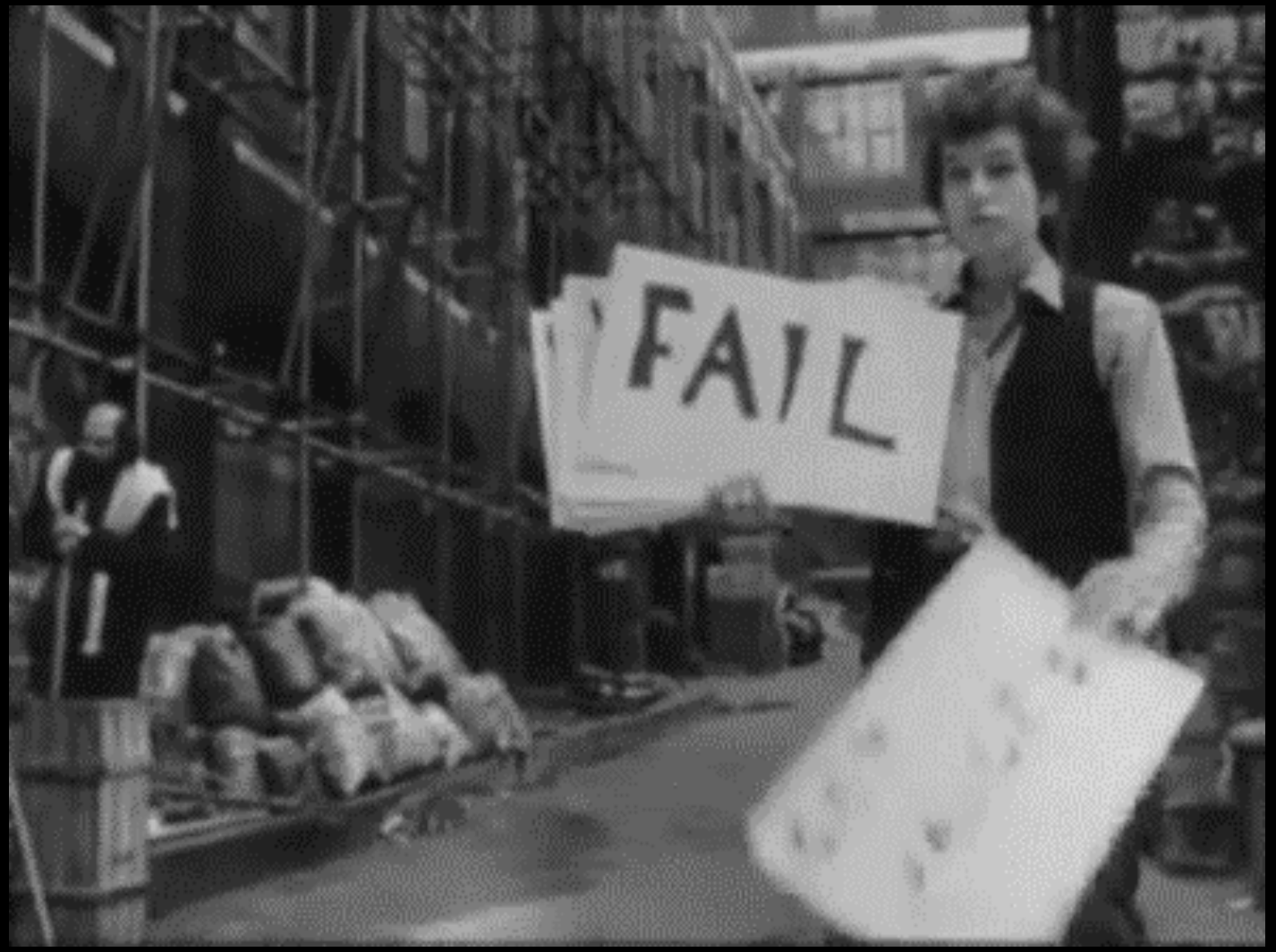
86% of IT and security professionals are aware of the risks of social engineering.

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

ALMOST EVERYTHING.

WE WATCH VIDEOS
WE DO E-LEARNING MODULES
WE TICK BOXES
WE MAKE POSTERS

AND GENERALLY FEEL GOOD ABOUT OURSELVES.



NO. YOU'RE DOING IT WRONG TOO.

TRACKING.
FREQUENCY.
CONDITIONING.

TRACKING.

STOP TRACKING CLICKS

STOP TRACKING BY DEPARTMENT

DON'T TRACK FAILED ATTEMPTS

TRACK SUCCESSES

TRACK SUCCESSFUL REPORTED INCIDENTS.
THE GRAPH SHOULD IDEALLY GO UP
NOT DOWN.

AWARENESS TRAINING SHOULD FEED A STRONG SE SPECIFIC IR PLAN

FREQUENCY.

STOP SHOVING AWARENESS TRAINING DOWN PEOPLE'S THROATS.

CONDITIONING.

STOP USING NEGATIVE REINFORCEMENT.

USE POSITIVE REINFORCEMENT.

LET ME TELL YOU ANOTHER STORY.

HOW DO WE PLAN TO FIX THIS?

A MULTI-PHASED CYCLICAL APPROACH:

SE > PT > IR > PPP > ES >
SE > PT > ...

RINSE, REPEAT

HOW DO WE PLAN TO FIX THIS?

STRATEGIC NEXT STEPS

1. ALIAS FOR REPORTING INCIDENTS
2. IMPLEMENT ANTI-EMAIL SPOOFING (SPF, DKIM, DMARC)
3. DISABLE HTML IN SMTP (PLAINTEXT EMAILS FTW)
4. SANDBOX THE BROWSER AND THE EMAIL CLIENT

STRATEGIC NEXT STEPS

1. ALIAS FOR REPORTING INCIDENTS
2. IMPLEMENT ANTI-EMAIL SPOOFING (SPF, DKIM, DMARC)
3. DISABLE HTML IN SMTP (PLAINTEXT EMAILS FTW)
4. SANDBOX THE BROWSER AND THE EMAIL CLIENT
5. BROWSER PLUGINS
6. ORG WIDE WEB PROXY
7. ALERT ON ORG RELEVANT [PHISHING] DOMAINS
8. CUSTOMIZATION OF AUTHN TO MITIGATE CLONING

STRATEGIC NEXT STEPS

1. ALIAS FOR REPORTING INCIDENTS
2. IMPLEMENT ANTI-EMAIL SPOOFING (SPF, DKIM, DMARC)
3. DISABLE HTML IN SMTP (PLAINTEXT EMAILS FTW)
4. SANDBOX THE BROWSER AND THE EMAIL CLIENT
5. BROWSER PLUGINS
6. ORG WIDE WEB PROXY
7. ALERT ON ORG RELEVANT [PHISHING] DOMAINS
8. CUSTOMIZATION OF AUTHN TO MITIGATE CLONING
9. APPLICATION WHITELISTING
10. ENCRYPT SENSITIVE DATA (IN TRANSIT & AT REST)
11. ENFORCE A VPN WHEN NOT ON INTERNAL NETWORK
12. PERFORM REGULAR SIMULATED SE FOR A MORE PREPARED IR TEAM

QUESTIONS?

SPECIAL THANKS

@LADY_NERD @CANDYSAUR @LUNARCA_ @TASTIC007 @NAPORDIE

ROB RAGAN

@SWEEPTHATLEG

CHRISTINA CAMILLERI

@0XKITTY


gifak.net