

Robbing A Bank Over The Phone

Joshua Crumbaugh,
CEO
PhishFirewall

Phishing Urgency



Joshua Crumbaugh

CEO
PhishFirewall

CYBERSECURITY
AWARENESS MONTH
2024



Joshua Crumbaugh is an internationally esteemed cybersecurity expert, ethical hacker, social engineer, published author, innovator, and keynote speaker. Joshua engages audiences with intriguing stories of his social engineering accomplishments, such as talking his way into bank vaults, fortune 500 data centers, casinos, and more. Joshua's engaging, entertaining, and highly informative keynotes are a crowd favorite at every event.



#SocialEngineering

How to rob a bank over the phone

By Joshua Crumbaugh



Social Engineering is the GREATEST 😊

STORY TIME

TALKING MY WAY INTO A FORTUNE 500 DATACENTER



WHAT YOU'LL LEARN

BETTER DEFEND THROUGH A STRONGER UNDERSTANDING OF OFFENSIVE TACTICS

SOCIAL ENGINEERING IS BASIC PSYCHOLOGY AND CAN BE USED ENHANCE PERSONAL RELATIONSHIPS, BUSINESS OBJECTIVES, SALES AND MORE.

RED TEAMS CAN USE THESE TACTICS TO IMPROVE THEIR ENGAGEMENTS, GAIN CONFIDENCE AND INCREASE ENGAGEMENT SUCCESS RATES

#SocialEngineering / @PhishDoctor



WHY I'M SHARING THIS

IN CYBERSECURITY WE REGULARLY SHARE INTELLIGENCE WITHIN THE INDUSTRY TO HELP ENHANCE DEFENSIVE CAPABILITIES UNTIL IT COMES TO SOCIAL ENGINEERING.

I BELIEVE THAT WE CAN ONLY GET BETTER THROUGH KNOWLEDGE SHARING!

THIS IS A REAL LIFE SCENARIO TO SHOW JUST HOW QUICKLY THINGS CAN GET OUT OF CONTROL!

#SocialEngineering / @PhishDoctor



PRIVACY NOTICE

TO PROTECT THE IDENTITY OF THE BANK VP ALL RECORDING IS RESTRICTED ON SLIDES CONTAINING THE FOLLOWING ICON:

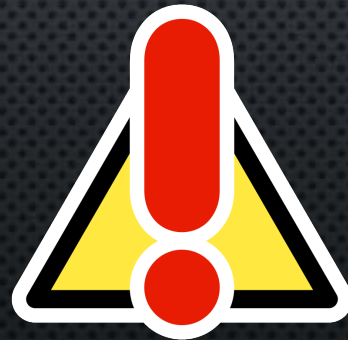
THE VOICE OF THE VP HAS BEEN MODIFIED FOR IDENTITY PROTECTION CONCERNS.



FAULT NOTICE

MOST OF THE TIME THE FAULT IS ON MANAGEMENT AND NOT THE EMPLOYEE.

IT'S OUR RESPONSIBILITY TO EDUCATION AND TEST THE USER TO ENSURE THEY'RE PREPARED FOR SOCIAL ENGINEERING ATTACKS.



#SocialEngineering / @PhishDoctor



Cybersecurity Education for Awareness and Compliance



Ismini Vasileiou and Steven Furnell



WHOAMI

- FOUNDER/CEO – PHISHFIREWALL, INC.
- WORLD'S FOREMOST EXPERT ON SECURITY AWARENESS & PHISHING
- CO-AUTHORED COLLEGE CURRICULUM
- WORLD FAMOUS ETHICAL HACKER & SOCIAL ENGINEER

THE PRETEXT

- NEW DEPARTMENT AT ISP/EMAIL HOSTING PROVIDER.
- CALLING ABOUT PROBLEMS WE IDENTIFIED ON THEIR ACCOUNT
- PREEMPTIVELY FIXING ISSUES
- TESTING NEW SERVER BEFORE MIGRATING
- I NEED HIS SIGN OFF TO MIGRATE
- GOAL – GET HIM TO RUN MY MALWARE
 - SET OBTAINABLE GOALS
 - BE OPPORTUNISTIC AND TAKE ADVANTAGE WHEN YOU CAN GET MORE





DID WE JUST BECOME BEST FRIENDS?

HOW IT STARTS

BUILD RAPPORT BY CULTIVATING AN “US AGAINST THE WORLD” SCENARIO

BUILDING COMRADERY...

- Mistakes as a weapon
- Creating collaboration
- Working together to solve problems



Recon is EVERYTHING!



*That's what I do. I drink
and I know things.*

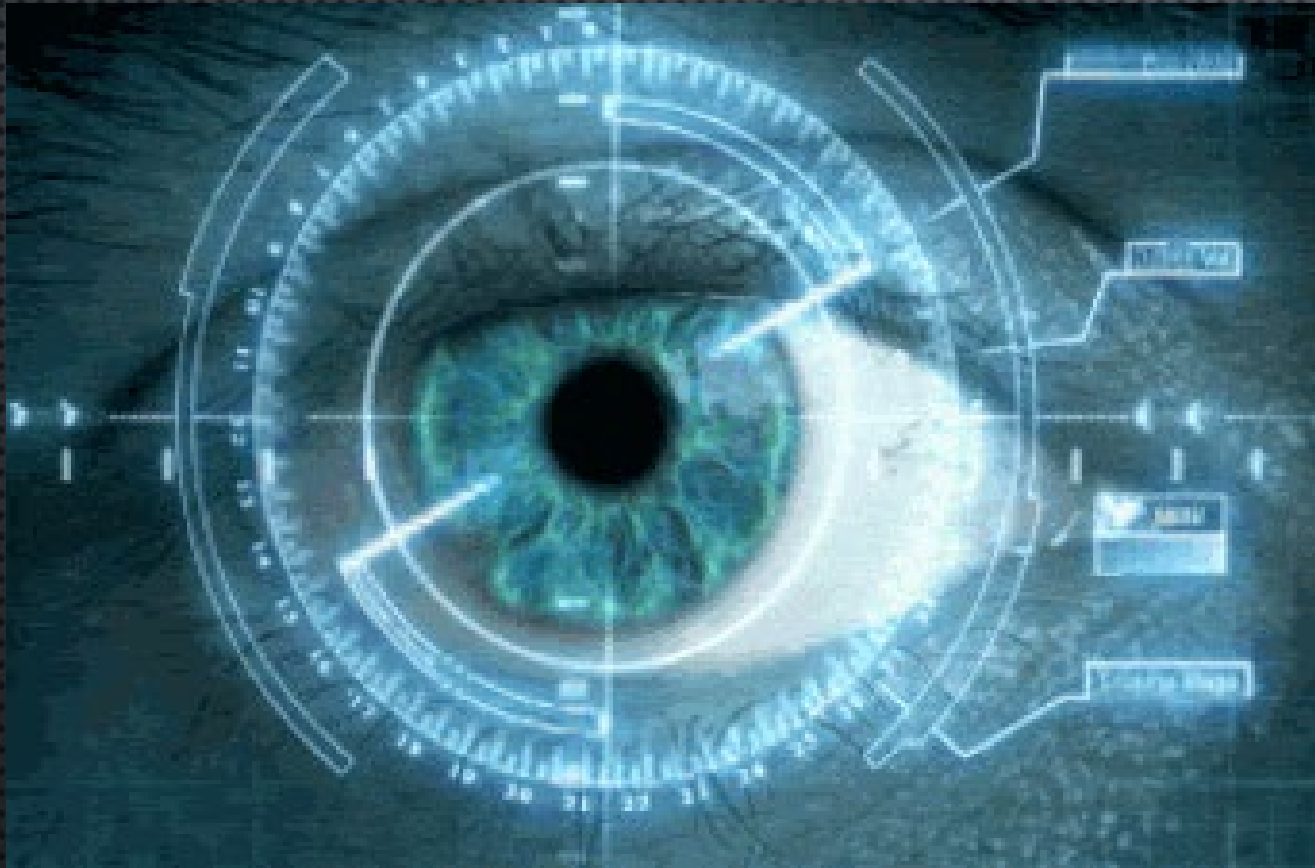
#SocialEngineering / @PhishDoctor



Recon for Red Teams

NEVER UNDERESTIMATE HUMAN BLINDNESS WHEN IT COMES TO PERSONAL DESIRE. GOOD RECON CAN BLIND TARGETS TO SECURITY RISKS.





BLUE TEAMS

PROVIDE STAFF WITH A SECURE
WAY TO VERIFY VENDOR
IDENTITIES

OOPS...



RED TEAM TACTICS

- YOU NEVER KNOW WHEN THINGS MIGHT GO BAD
- PLAN OUT ALL COMMON PROBLEMS
- PREPARE FOR THEM



EVEN WITH GOOD PLANNING, IT CAN BE CHALLENGING!





**NEVER
BREAK
CHARACTER!**

DENIAL OF THINKING ATTACK

SOCIAL ENGINEERING ATTACKS SOMETIMES TAKE MONTHS

- It's not uncommon for attackers to call you multiple times



BOSSSES BE LIKE...



YOU'RE STILL COMING TO WORK RIGHT?

THE "MY BOSS" RULE
ALWAYS HAVE A SCAPEGOAT

THE “MY BOSS” RULE – IN ACTION



RED TEAM

- SOUND EFFECTS HELP SUBLIMINALLY SELL YOUR STORY TO THE TARGET

SUBLIMINAL – USE SOUND EFFECTS

- THE FIRST 4 SECONDS OF THIS CLIP HAVE BEEN AMPLIFIED TO EMPHASIZE THE POINT



RED TEAM

- PROVIDE FREQUENT FEEDBACK TO THE TARGET IF YOU'RE NOT TALKING TO THEM
- BE DECENTLY APPOLOGETIC AND THANKFUL FOR THEIR TIME

“WE WERE SUPPOSED TO TEST ALL THIS AND...”

- Provide constant feedback
- Apologize for taking the target’s time
- Talk to yourself on purpose
- Use volume to emphasize your point
- Remind the target of goals



“IT WOULD BE EASIER IF I COULD JUST TAKE CONTROL...”



THE EXCITING CONCLUSION

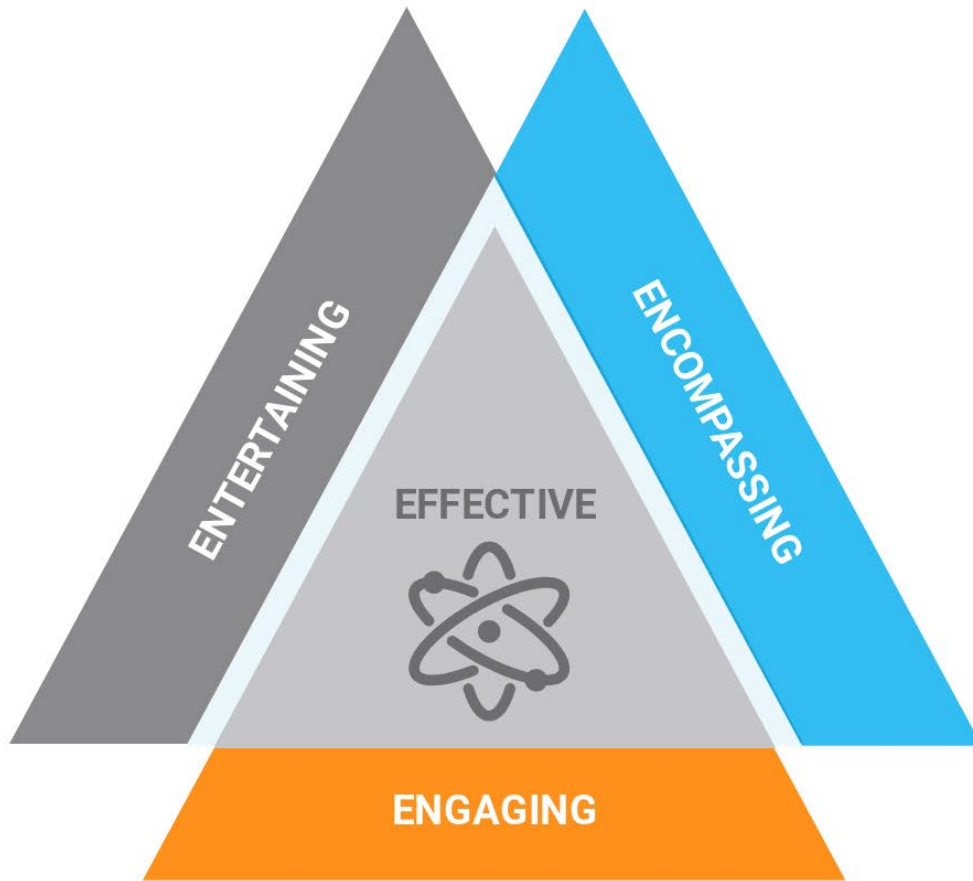


HOW DO WE FIX THIS?



PEOPLE ARE SIMILAR TO COMPUTERS
HARD TO TRAIN, BUT EASY TO PROGRAM

The **FOUR E's** of security awareness



ENTERTAINING

We must entertain our users to make them want to learn

ENCOMPASSING

Does the program address all human security weaknesses?

ENGAGING

Users must be engaged in security monitoring and protection

EFFECTIVE

Programs need to be measured by results no compliance.

TOP FIVE (5) SECURITY AWARENESS TIPS

- BE KIND TO YOUR USERS
- SIMPLIFY MESSAGING
- ANCHOR IN EMOTION
- TRAIN ACCORDING TO NEED
- PHISH FREQUENTLY TO EMBED HUMAN VIRUS DEFINITIONS



DID YOU KNOW?

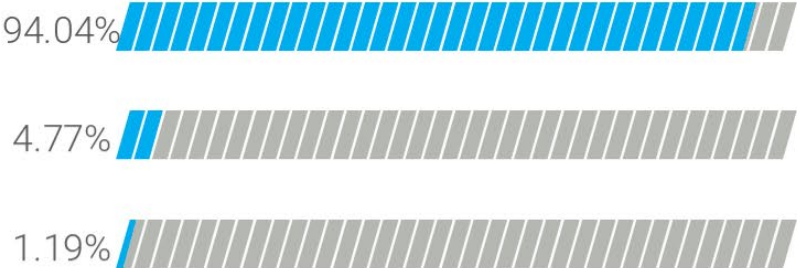
- A SMALL PORTION OF YOUR STAFF PRESENTS THE LARGEST PORTION PHISHING OF RISK

Why Small Percentages Matter

1.19% of Users Represent **89.82%** of Total Phish Risk

% of Employee Population

Percentage of employees in each group



VS

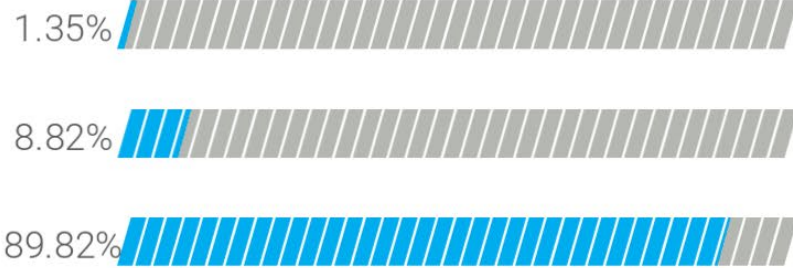
Low Risk

Moderate Risk

High Risk

Risk Distribution

Total phish risk each group poses



FOR MORE BLUE TEAM TIPS WATCH MY RECENT GRRCON TALK

[HTTP://WWW.IRONGEEK.COM/I.PHP?PAGE=VIDEOS/GRRCON2018/GRRCON-2018-ADA15-
GUARANTEED-FAILURE-AWARENESS-THE-GREATEST-CYBER-INSANITY-JOSHUA-NAGA-CRUMBAUGH](http://www.irongeek.com/i.php?page=videos/grrcon2018/grrcon-2018-ada15-guaranteed-failure-awareness-the-greatest-cyber-insanity-joshua-naga-crumbaugh)

OR

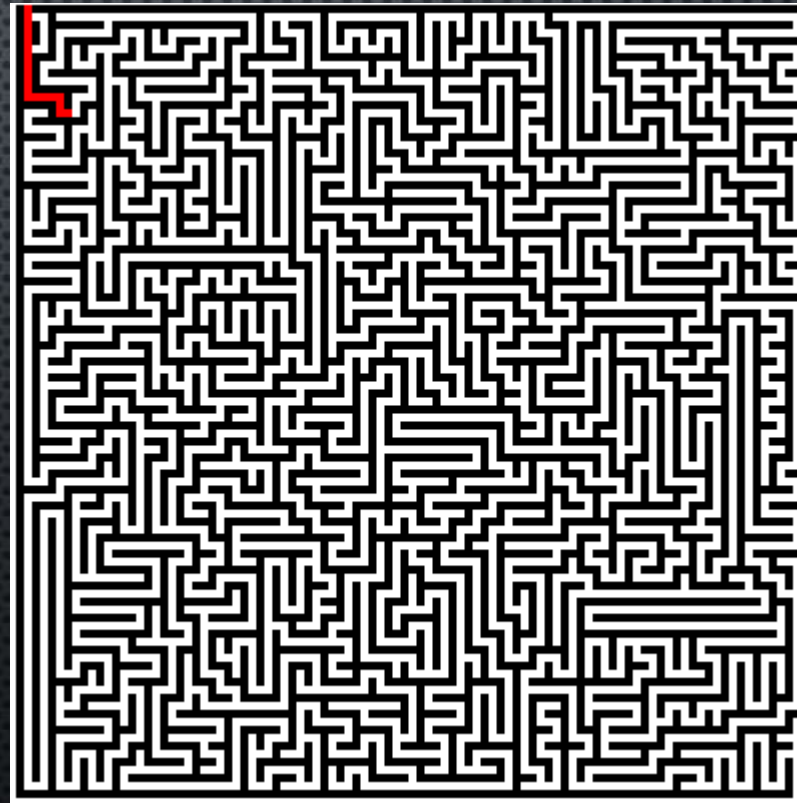
[HTTPS://GOO.GL/9PRU3A](https://goo.gl/9PRU3A)

BLUE TEAM

- SOCIAL ENGINEERING CAN BYPASS YOUR SECURITY CONTROLS
 - SOMETIMES THE SOCIAL ENGINEER ENLISTS THE HELP OF YOUR STAFF FOR BYPASSES

BLUE TEAM

- TRAIN ACCORDING TO NEED
- PHISH ACCORDING TO SUSCEPTIBILITY



BLUE TEAM

- ANCHOR LESSONS IN EMOTION
- JUST-IN-TIME IS KEY

BLUE TEAM

- INTEGRATE EVERYWHERE
 - PAY STUB
 - ELEVATOR
 - DESKTOP BACKGROUNDS
 - EVERYWHERE YOU CAN THINK OF

THE REST OF THE STORY



Joshua Crumbaugh – CEO
PhishFirewall
Joshua@PhishFirewall.com

SIGN UP FOR FREE TRAINING @ WWW.PHISHFIREWALL.COM

