black hat® EUROPE 2017

DECEMBER 4-7, 2017

EXCEL / LONDON, UK

#BHEU / @BLACK HAT EVENTS

By Joshua Crumbaugh

Social Engineer & Red Teamer

Chief Hacker @ PeopleSec

How to rob a bank over the phone

#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.

Timeline

Because of time limitations we are going to start on the second call.

- This call begins approximately 8 minutes into the conversation
- Pretext: I’m a quality assurance analyst for their ISP and I’ve identified a problem with their email.
  - During the OSI assessment we found recent post where this VP was compaining about the email at their ISP.
- Goal: Get him to give us remote access to the network.

Penetration Testing is the GREATEST ☺

Call 2

08:00–08:32

Background Story

Recon is EVERYTHING!

Recon for Red Teams

Never underestimate human blindness when it comes to personal desire. Good recon can blind targets to security risks.

Recon For Blue Teams

- Know what OSI is available for yourself, your employees, and vendors.
- Conduct an OSI Assessment

The Pretext

- New department at ISP/email hosting provider.
- Calling about problems we identified on their account
- Preemtively fixing issues
- Testing new server before migrating
- I need his sign off to migrate

Red Teams

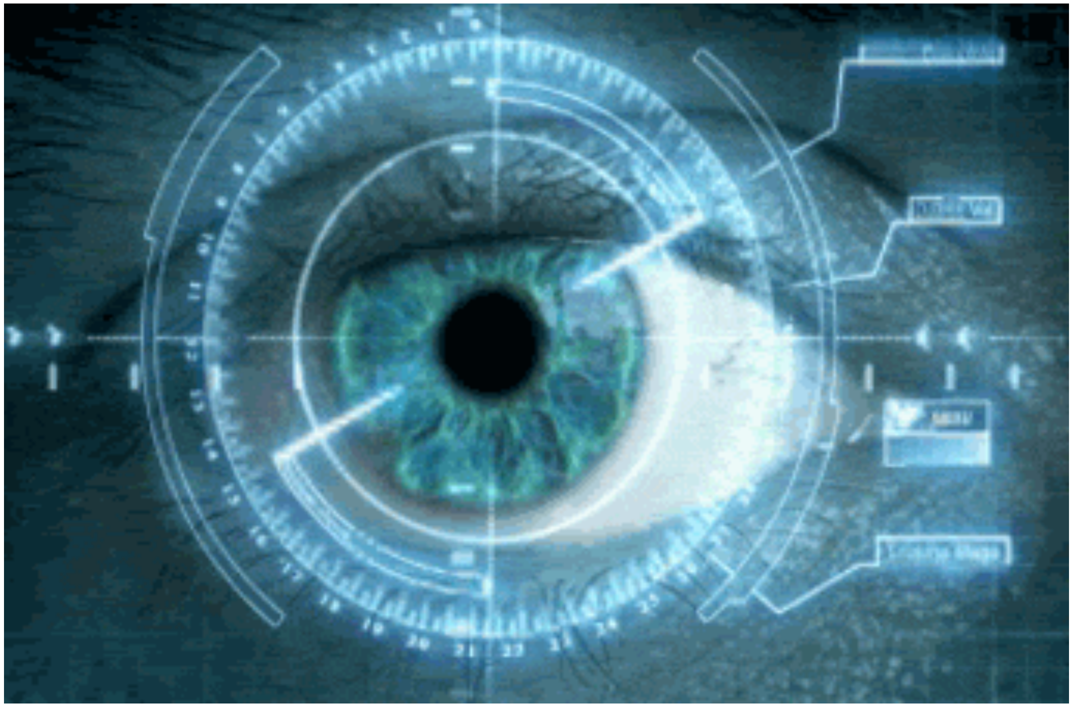
Build rapport by cultivating an “us against the world” scenario

Building comradery…

- Make mistakes on purpose
- Create a sense of comradery
- Work together to solve problems

Call 2

08:32–09:38



Blue Teams

Provide staff with a secure way to verify vendor identities

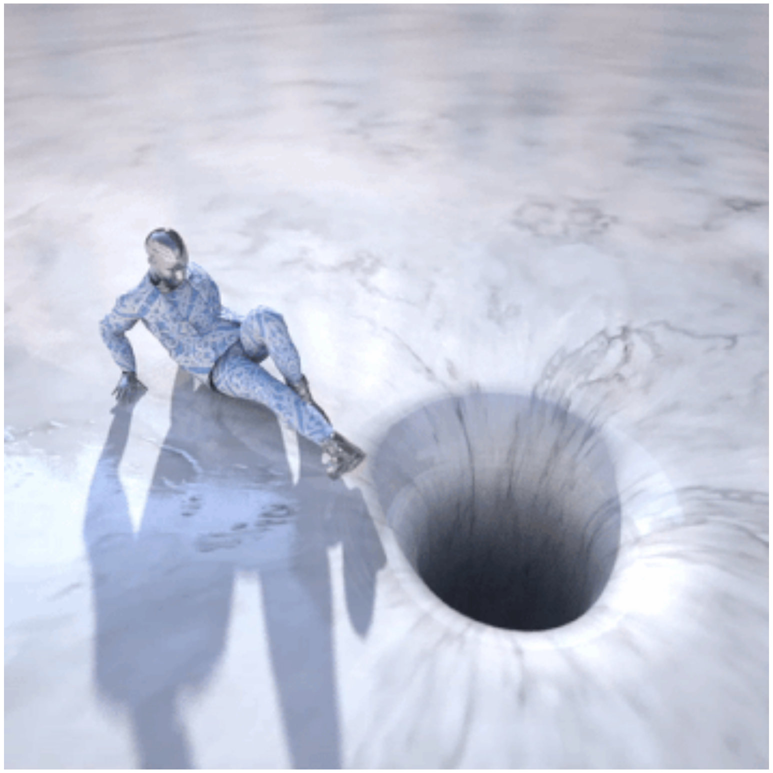
What next?

Call 2

09:34–10:25

Red Team

- You never know when things might go bad
- Plan out all common problems
- Prepare for them



Even with good planning, it can be challenging!

Call 2

10:22–11:16

Never break character!

Don’t be afraid to take time to regroup!

- Multiple calls can help build rapport
- Bigger goals require more pretexting

Call 2

10:22–11:16

Red Team

- Telephone based social engineering does not have to be completed in one call
  - Most sophistacated social engineering attacks require multiple calls

Don’t be afraid to take time to regroup

Red Team

- Always Have a Scapegoat

The “My Boss” Rule

Call 3

11:57–12:09

"My Boss"

Call 3

00:00–00:00

Red Team

- Ask the target permission for their time

“No time better than the present!”

Call 3

12:09–12:31

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

Call 3

12:32–12:36

Red Team

- Be bold in your responses
  - You’re better off answering a question wrong than to answer without confidence
- Most people do not understand technology and this is a potentially exploitable vulnerability

“Save to what drive?”

Call 3

12:36–13:34

Read Between The Lines

- Listen for admissions of misunderstanding of tech

Type email-setup.ps1 and it should run…

Call 3

13:34–15:22

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

Call 3

15:22–18:46

Red Team

- Mention personal faults as excuses to get what you want
- Be persistent

“it would be easier if I could just take control…”

Call 3

18:46-21:40

Red Team

- Do almost everything on behalf of someone

“my boss is big into it though”

Call 3

21:48-22:15

“I’m actually available on Monday”

Call 4

25:02-26:33

Red Team

- Laugh frequently
- Laugh when they laugh

The exciting conclusion

Call 4

33:22-34:01

Red Team

- Laugh frequently
- Laugh when they laugh

Blue Team

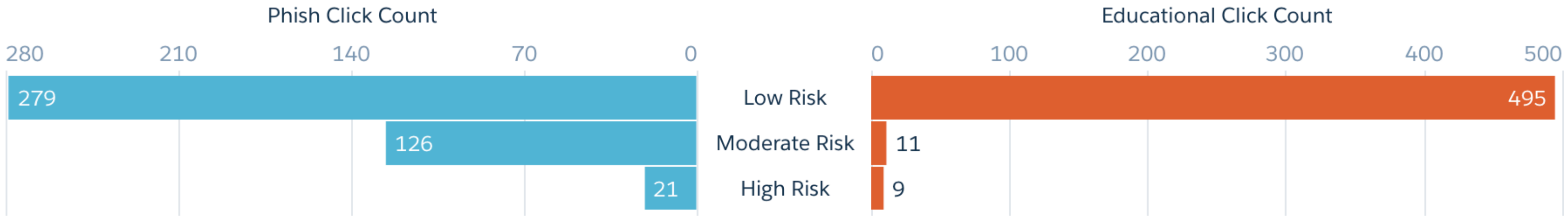
- Social engineering is the largest risk facing your organization

Blue Team

- Social Engineering can bypass your security controls
  - Sometimes the social engineer enlists the help of your staff for bypasses

Blue Team

- A small portion of your staff presents the largest portion of risk



Blue Team

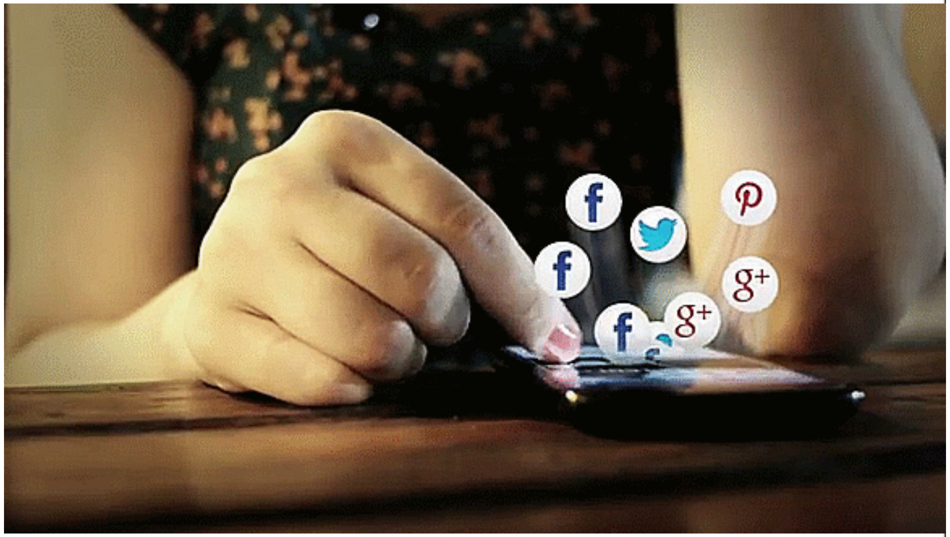
- Your sales staff are 400% more susceptible to phishing on average
- Developers take a close second

Blue Team

- People have an extremely short attention span

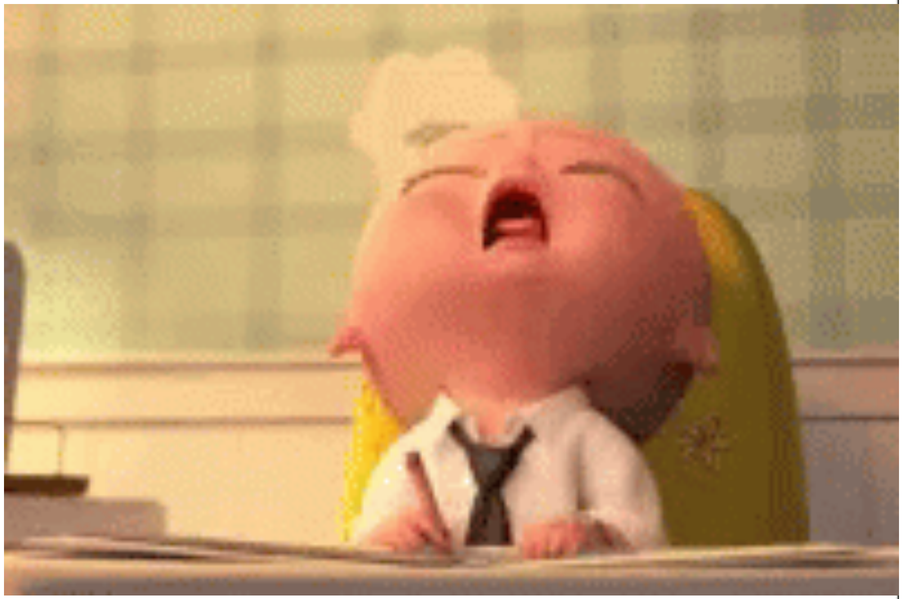
Blue Team

- Education needs to abide by social media rules



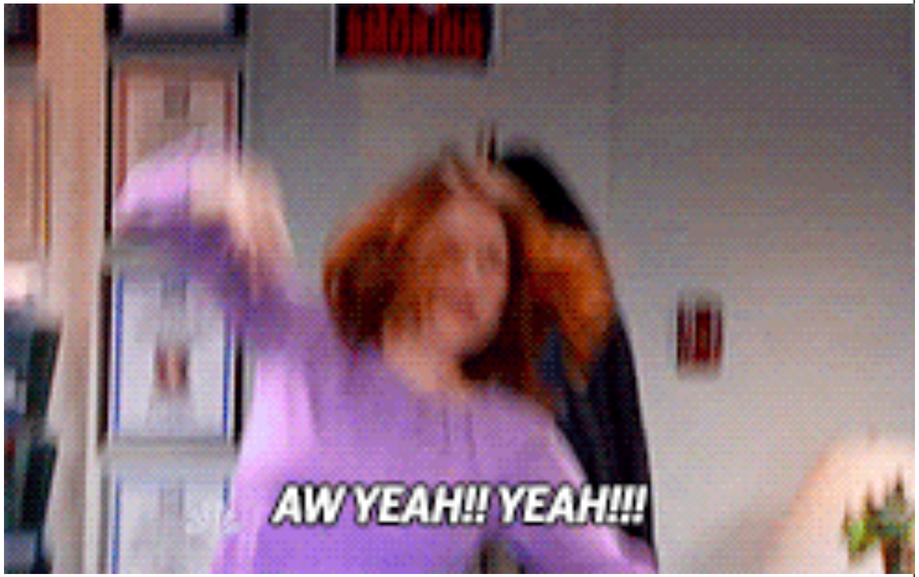
Blue Team

- Education should be fun
  - Avoid boring content



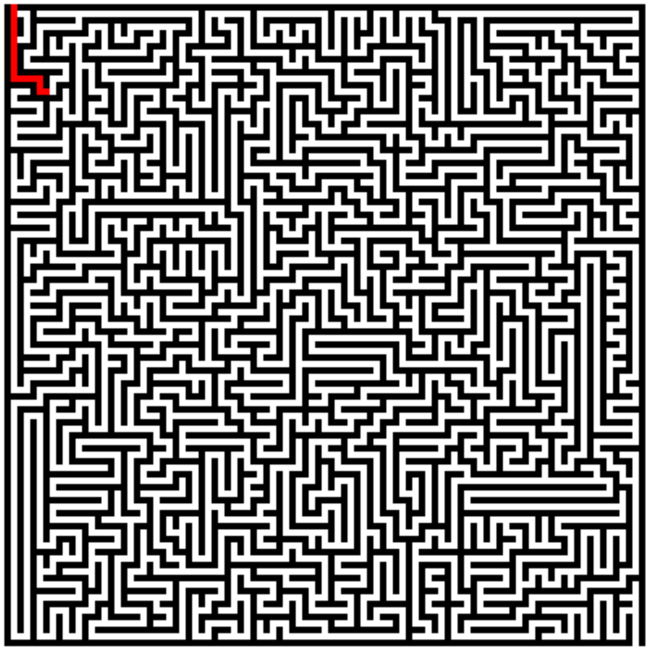
Blue Team

- High frequency education



Blue Team

- Train according to need



Blue Team

- Mass customization

Blue Team

- Integrate everywhere

black hat®

EUROPE 2017

DECEMBER 4-7, 2017

EXCEL / LONDON, UK

#BHEU / @BLACK HAT EVENTS