

High and Low-Tech Cyber Attacks: From Malware to Social Engineering

Daryl Pfeif

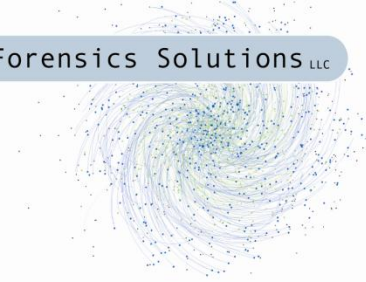
daryl@digdeeply.com

Joe Sylve

joe@digdeeply.com

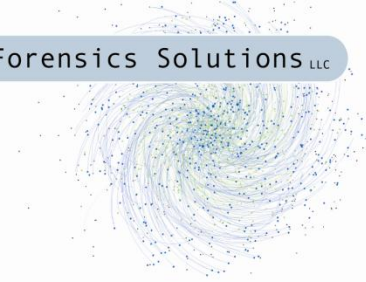
Digital Forensics Solutions, LLC

www.DigitalForensicsSolutions.com



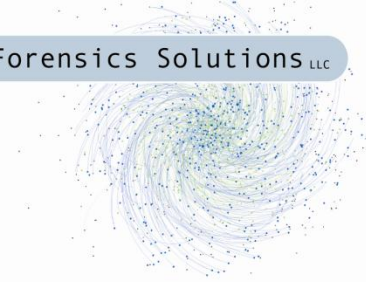
Who Are These People?

- Daryl Pfeif
 - Co-Founder & CEO of Digital Forensics Solutions, LLC
 - Board of Directors - Digital Forensics Research Workshop (DFRWS)
 - Member Gulf Coast Government Contractors Association
 - Member Louisiana Technology Council
- Joe Sylve
 - Senior Forensics and Security Analyst
 - GIAC-Certified Digital Forensics Investigator
 - M.S. Computer Science, University of New Orleans



Malware

- Malware == malicious software
- Malware can:
 - Modify your data
 - Delete your data
 - Transmit your data to remote sites
 - Send emails
 - Attack other computer systems
 - Download child pornography or other contraband and cause you serious trouble!

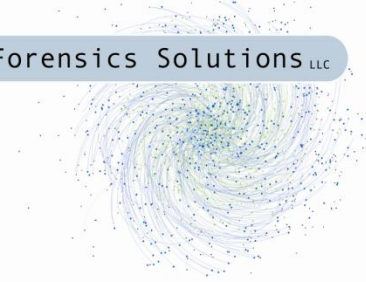


Malware (2)

- Typically spread via:
 - Malicious email attachments
 - Internet downloads
 - Peer to peer networks
 - Bittorrent downloads
 - Illegal copies of software
 - Friends: “Hey! Try this new thing I just downloaded”
 - Exploits of software vulnerabilities
 - Directed attacks at networked computer systems
 - Browser vulnerabilities
 - USB vulnerabilities
 - etc.
- Malware is “high tech” in that it needs to spread automatically and be stealthy

Broad Categories of Malware

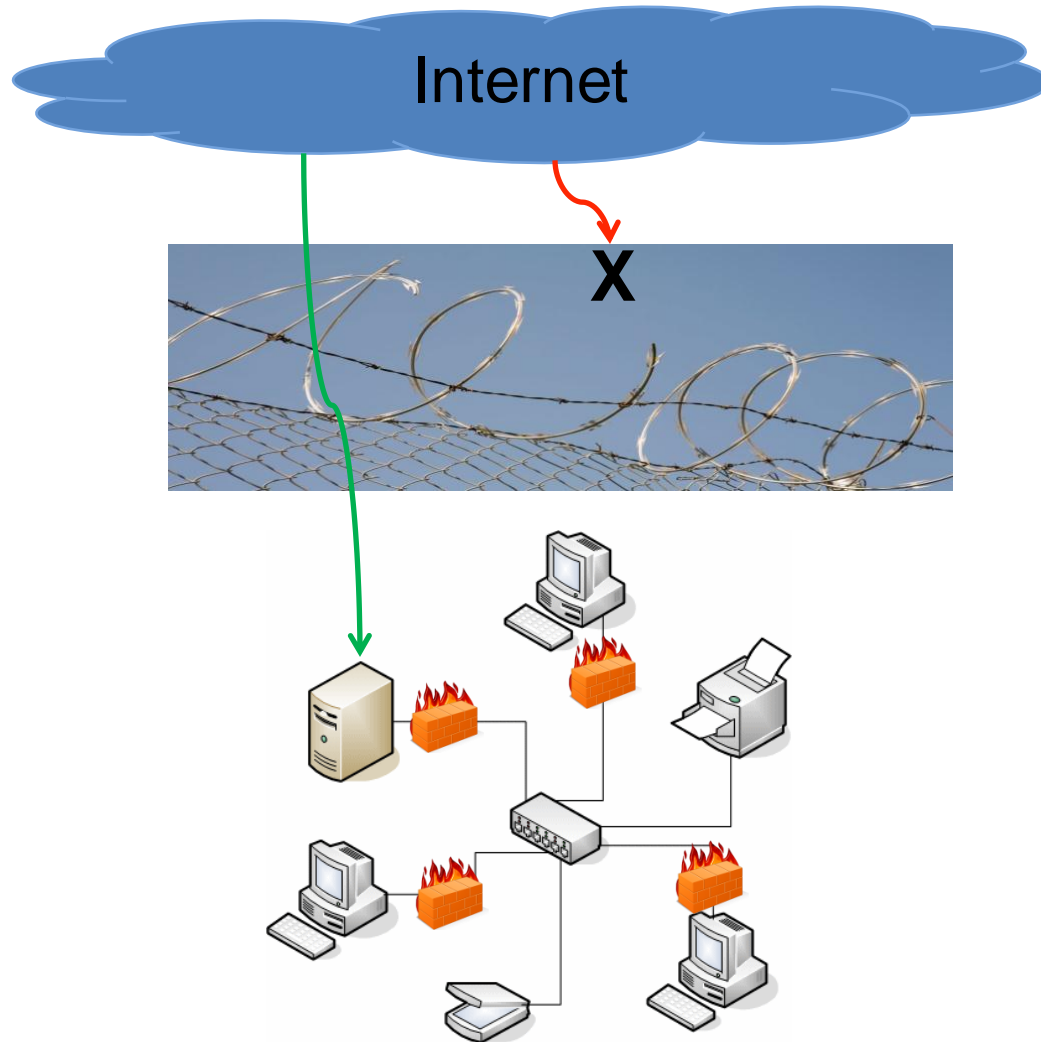
- Backdoor
 - A “back way” into a system
 - Commonly via hidden code introduced by a programmer
 - “Job security”
- Trojan horse
 - Program that performs an undesirable or unexpected function, often posing as a different sort of program
- Virus
 - Self-propagating computer code that infects other applications
 - Generally propagates when infected application is executed
- Worm
 - Self-propagating code that actively seeks to infect other systems
 - Connects to other systems over a network to install copies of itself...which then do the same...
- Spyware
 - Secretly reports on/redirects user web-browsing, steals passwords, etc.
- Rootkit
 - Modifies operating system to maintain presence



Why Do I Care?

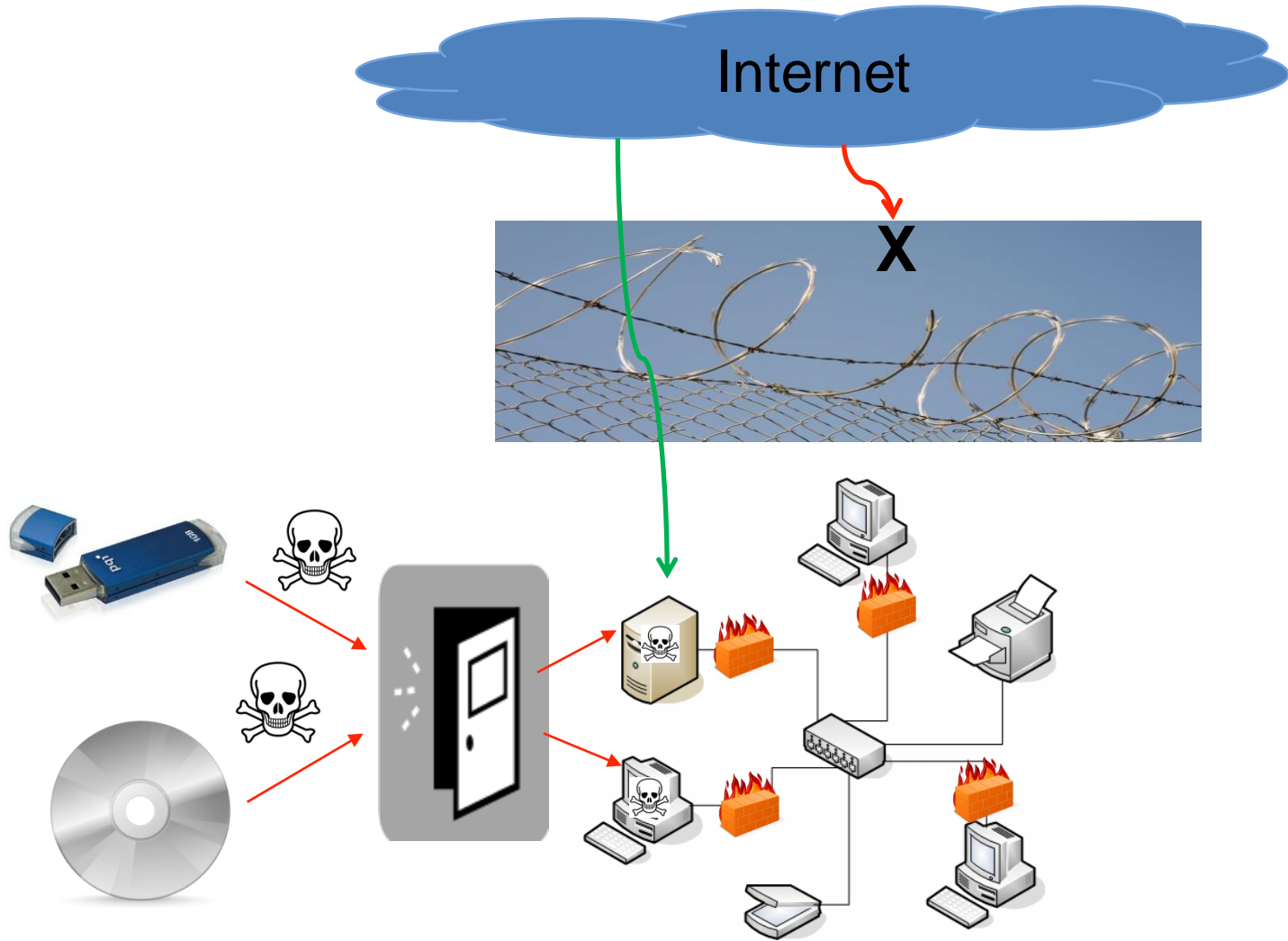
- Malware has a number of potential effects
- Few of them are good
- Some malware is written only to investigate infection strategies
- But malware's payload (effect) is arbitrary!
- Can (to nail this point home):
 - Modify your data
 - Delete your data
 - Transmit your data to remote sites
 - Send email
 - Attack other computer systems
 - **Download child pornography or other contraband and cause you serious trouble!**

External Defenses Aren't Enough





Not Enough (2)



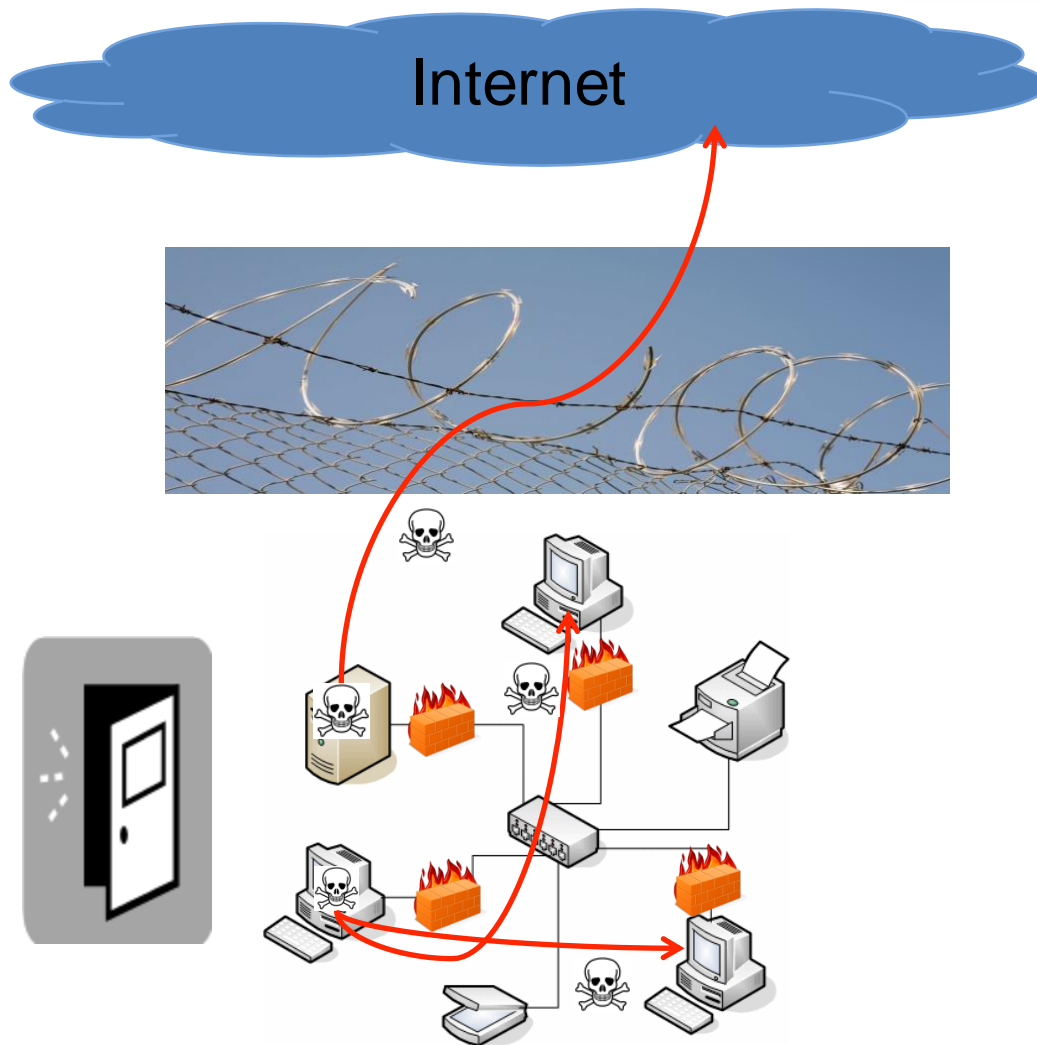
Seek And You Won't Find



<https://makersmarket.com/products/68-micronickel-hollow-spy-coin>



Once the Malware is Inside Your Defenses...



“But I Run Antivirus”



- For modern malware, **antivirus is so yesterday**
- Antivirus misses a large percentage of malware, particularly new stuff!
- Antivirus relies on a number of things that modern malware can easily defeat, including:
 - Signatures
 - Emulation
- Antivirus will never have seen custom or “zero day” malware before—thus, no signatures—no detection
- Modern malware may directly attack and disable antivirus
- It may also disable your ability to visit websites that offer antivirus solutions or patches!
- Real defense is education and best practices!

Modern: Example: Metamorphic Malware

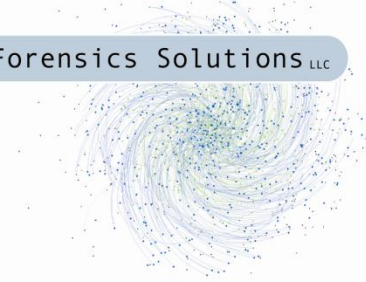
- Metamorphism (“metamorphic malware”)
 - Malware’s code is rewritten for each instance
 - Much more complicated to implement than polymorphism
 - More common to make decryptor for poly malware metamorphic
 - But makes signature-based detection useless



Getting Kicked in the Soft Bits



- Authors of modern malware are aware of available defenses
- Their challenge is to overcome these defenses
- Have a firewall?
 - Malware will infect files that are copied via removable media
- Email scanned for viruses?
 - Virus will be encrypted
 - May send you a password in a separate email!
- Everything locked up tight?
 - It may whisper in your ear



Ransom-ware

- Ransom-ware virus is introduced in the usual way:
 - Email attachment
 - Pirated copy of software
 - Malicious website
 - etc.
- When your computer gets infected, the virus selects important files and encrypts them
- You then receive instructions to deposit \$\$\$ into a foreign bank account in exchange for the encryption key
- If you don't send the \$\$\$, files are lost
- If you do send the money...

Has the Malware Got Me?



- Maybe.
- Manual Investigation
 - Time-consuming, expensive
 - Very likely to miss important details unless you're both brilliant and thorough
- Automatic scanning
 - Typical antivirus products
 - Mostly signature-based detection
 - Some heuristics
 - Must actually pay attention to alerts
- Products like Tripwire
- Research prototypes you can't have yet... 😊

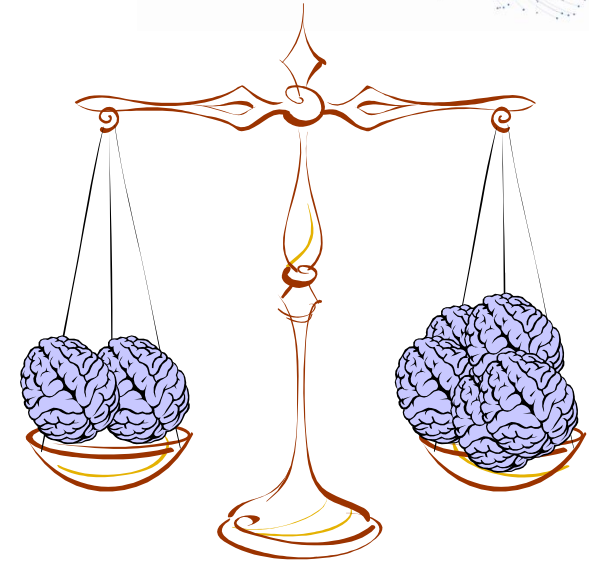


Is it Hopeless?

- Mostly.
- Be diligent.
 - Don't run software from unknown sources
 - Beware of social engineering attacks ← next up!
- Insist on better software
 - Modern software sucks
 - Easy target for malware
 - Hold software vendors accountable for their crappy software!
- Do run antivirus—it eventually is adapted to deal with older threats
- Just don't be the first to be attacked!
- Sorry, but this still won't always be enough

Aside: Benevolent Hacking

“Giving ammunition to the bad guys” position is intellectually arrogant



- “Offensive” research
- Benevolent researchers work on “offensive” tactics as proof of concept
- It is an arms race
- Defense is MUCH harder than offense
- Being surprised is bad



Bad Guys: Why Malware?

- Malware works
- Historically developed as programming challenges
- But big business now...
- Hackers in Eastern Europe / USSR that write custom malware
- Custom malware might cause denial of service, steal sensitive documents, ...
- Can be targeted at the resources of a particular individual, company or country

Bad Guys: Why Not Malware?

- Malware is high tech
- Requires discovery of exploits
- Potentially brittle since targets may have slightly (or very) different environments than bad guys
- There are other ways to get your stuff!

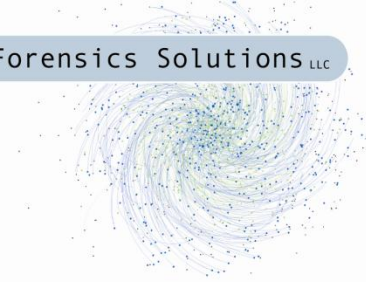


Social Engineering

- Let's be generous...
- Your Platonic Security Ideal (PSI) is realized:
 - Antivirus is working and 100% accurate
 - You have a firewall and IDS that's properly configured
 - Operating systems / applications are patched continuously
- Even in that fantasy world, **you're still at risk**
- Malicious actors don't have to attack your computer systems...
- They'll attack YOU (or your users)

Social Engineering: Overview

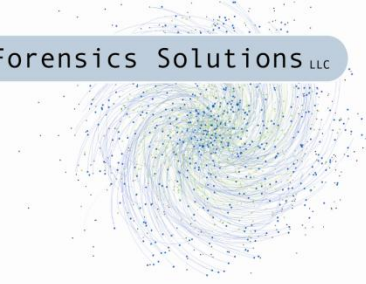
- Exploit the tendency of human beings to trust others, smile, be helpful
- Use psychological methods to relax the target's suspicion or reservations
- Essentially, simply ask (or manipulate) a person into:
 - Leaking information
 - Reconfiguring hardware or software
 - Executing code (which might be malware)



Overview (2)

- Root causes:
 - Humans tend to comply with requests from someone in charge
 - Fear of loss of job, reprimand, etc.
 - Humans like to trade favors: quid pro quo
 - Humans want to be helpful, especially to someone “nice” or courteous who is in need
 - Victims may be unaware of the value of information
 - May be unaware that aggregated leakage can result in serious loss

Kevin Mitnick



Common Methods: Physical / Online

- Pose as “someone who belongs”, revert to “I’m lost” if caught
- Pose as a fellow employee (play it through), especially a new employee who needs help
- Pose as someone in charge
- Pose as vendor, systems administrator, security personnel: “I’m here to help!”
- Use “insider” language or knowledge to build trust and credibility
 - Sources: Google, LinkedIn, company website, etc.
 - Drop names, refer to part #s, etc.



Common Methods (2)

- Send email attachments that are allegedly patches for “critical” problems
- Send emails that offer prizes
 - “Please provide your username and date of birth to win tickets to Don Julio’s Margarita Madness on June 28th!”
- Send password change emails
 - “Virus has compromised the network...please provide username, old password, new password”
 - Old password is sought, user may think it **provides** authentication and therefore protection!
- Ask for files to be transferred to apparently legitimate locations → <http://www.capitalone.com>
- Just call and ask for what you want...
- Disposable cell phones are cheap!

Phishing is Social Engineering



- Definition: Obtaining private or sensitive information through fraudulent means
- Examples:
 - Emails that request information that appear to come from a legitimate business
 - Bank, Credit Card Company, Paypal, etc.
 - Email may just explicitly ask for the information or warn that something bad has happened or will happen if info is not provided
- Spear Phishing is just targeted phishing
 - Specifically mentions, e.g., your name

The Problem is Real...



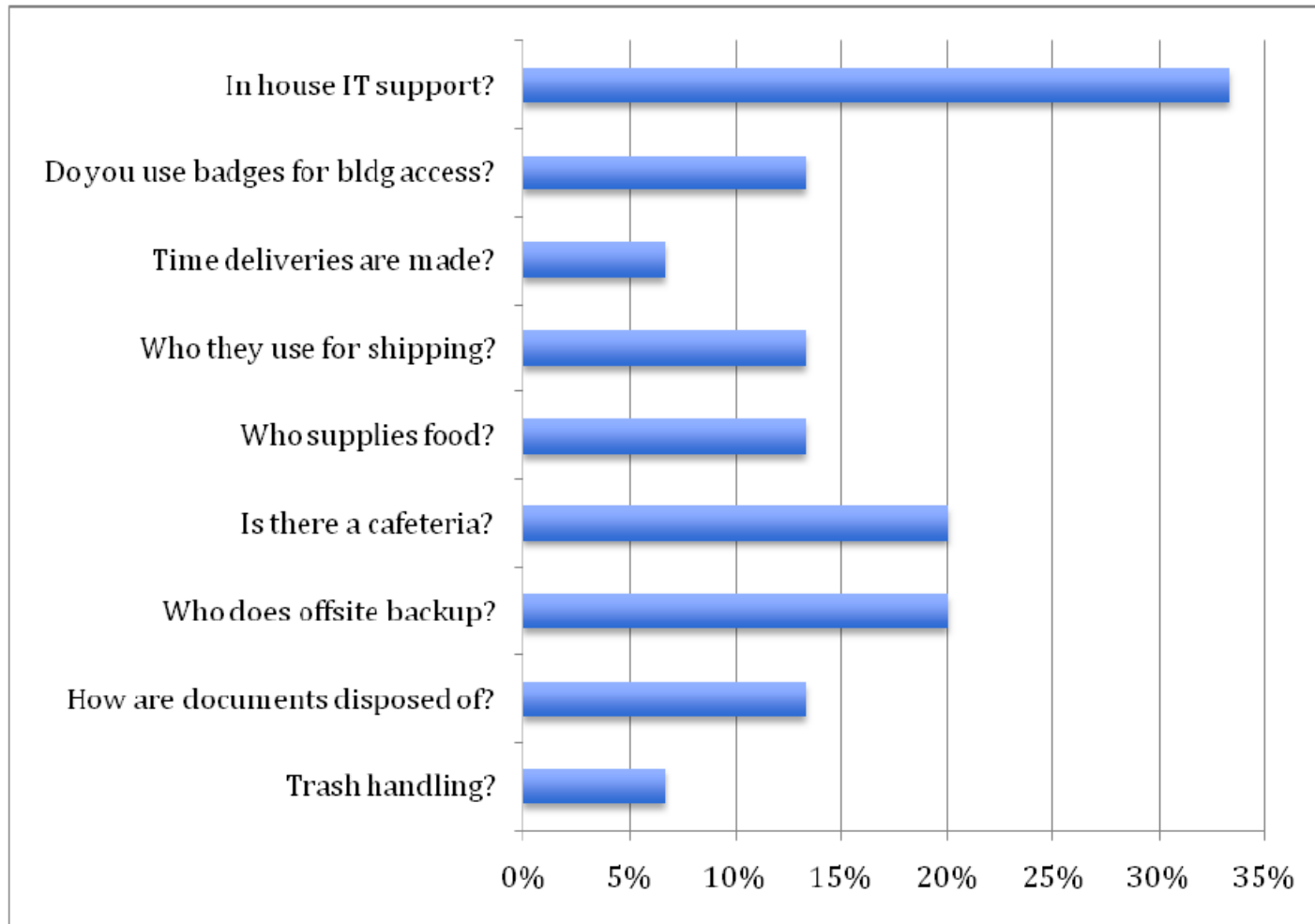
- DEFCON 18/19 Social Engineering CTF (Capture the Flag) Event
- Idea: Contestants have 2 weeks to research a company, but are not allowed to contact the company in any way!
- Then have 25 minutes to make phone calls to the company, in a soundproof booth, at the conference, audience can listen in
- **Goal: Get sensitive info from employees**
- Primary information sources: LinkedIn, Google, social networking sites

Sample Conversations

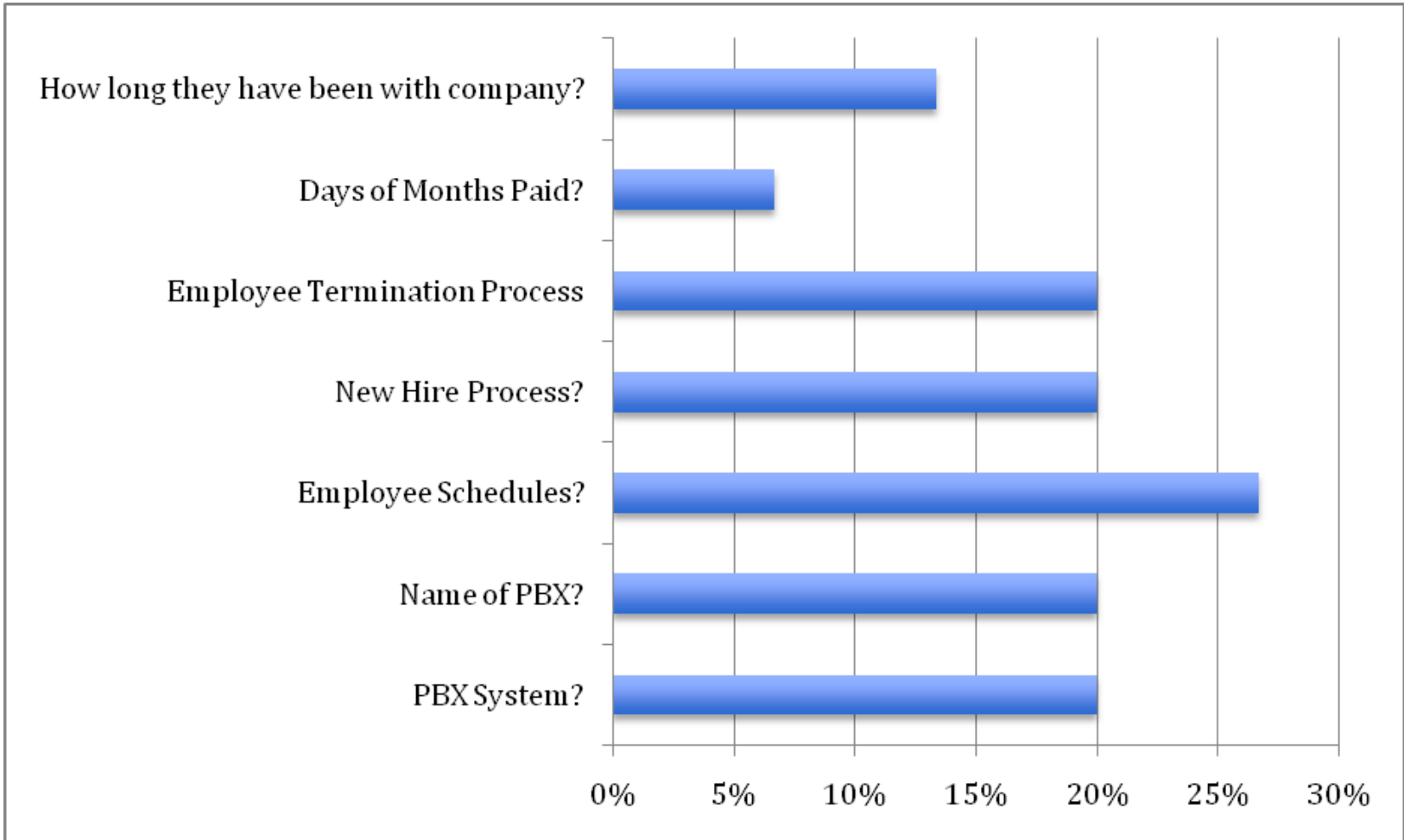


- **Caller:** “Oh, so you run wireless on site? You know, I always find it interesting what companies decide to name their wireless networks, as they are often something silly. Like at work, we call ours “NoMansLand”. What is yours called? Is it something funny?”
- **Company:** “No, we keep ours pretty simple, it's “XYZCorp”. I guess we don’t have a sense of humor around here.”

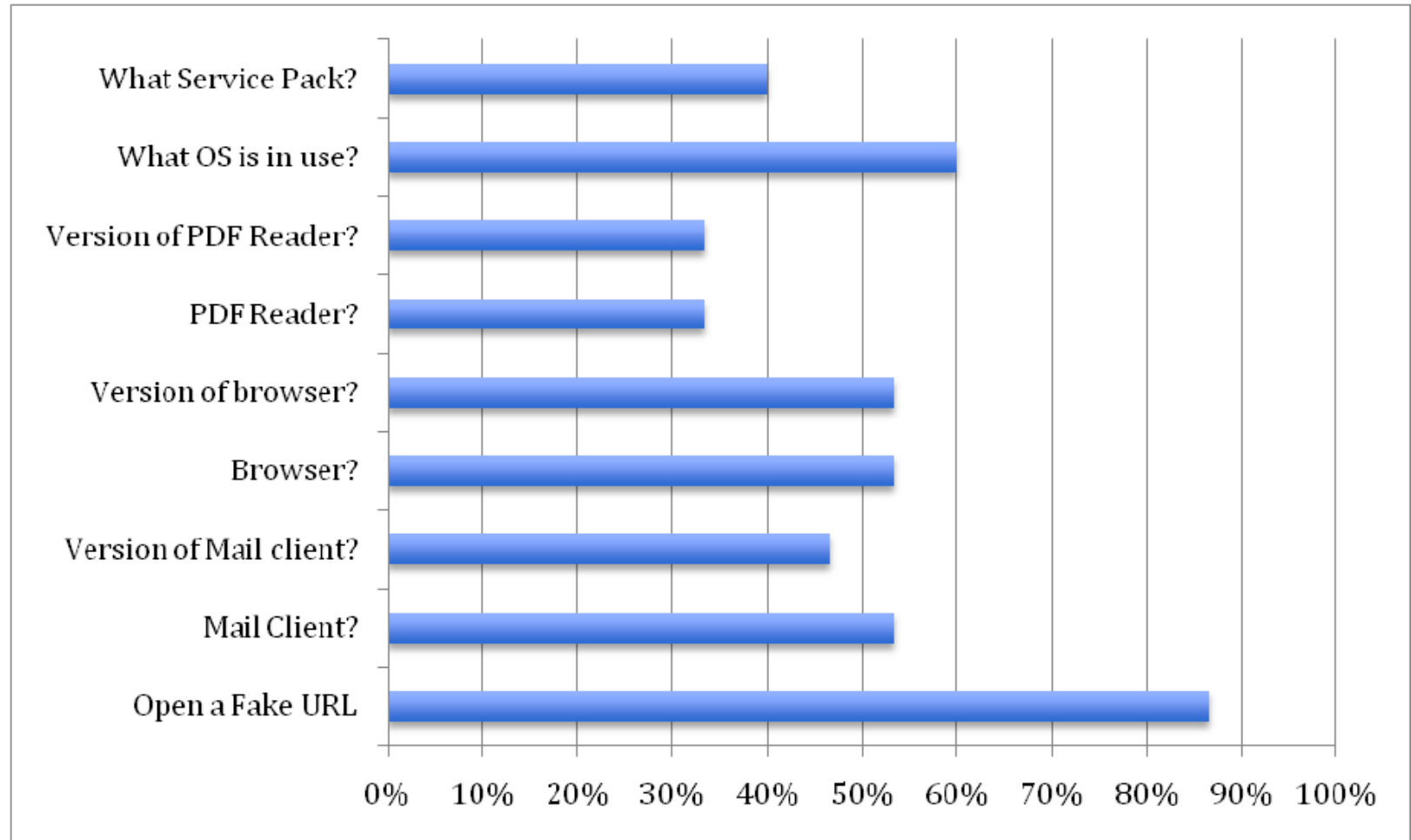
Non-Technical “Flags” Captured



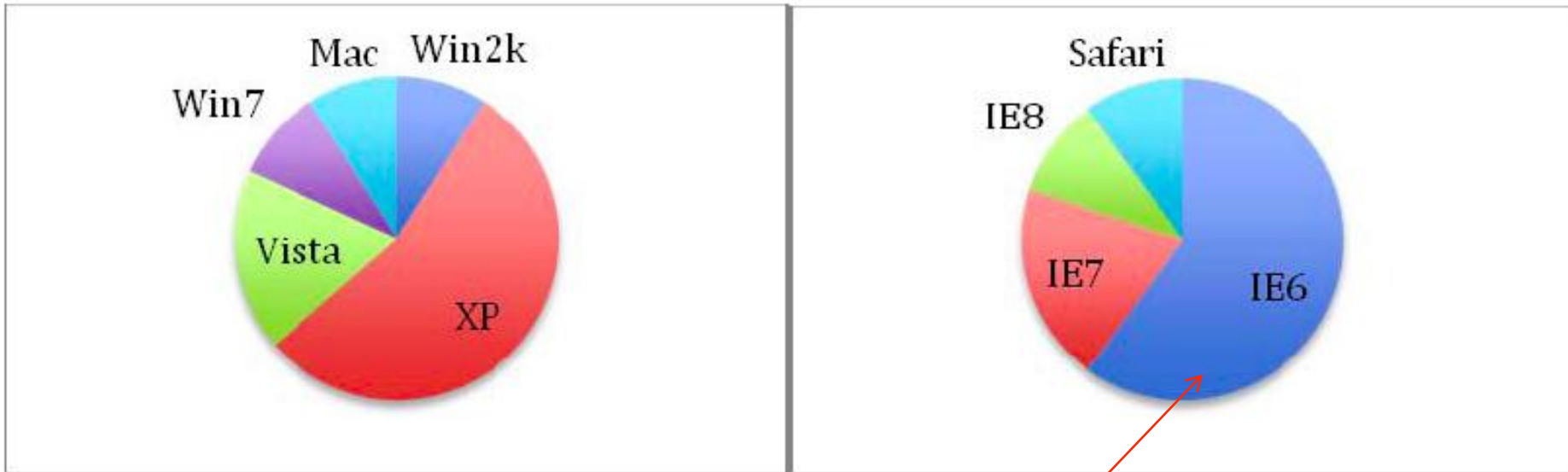
Non-Technical Flags, Cont.



Technical Flags Captured

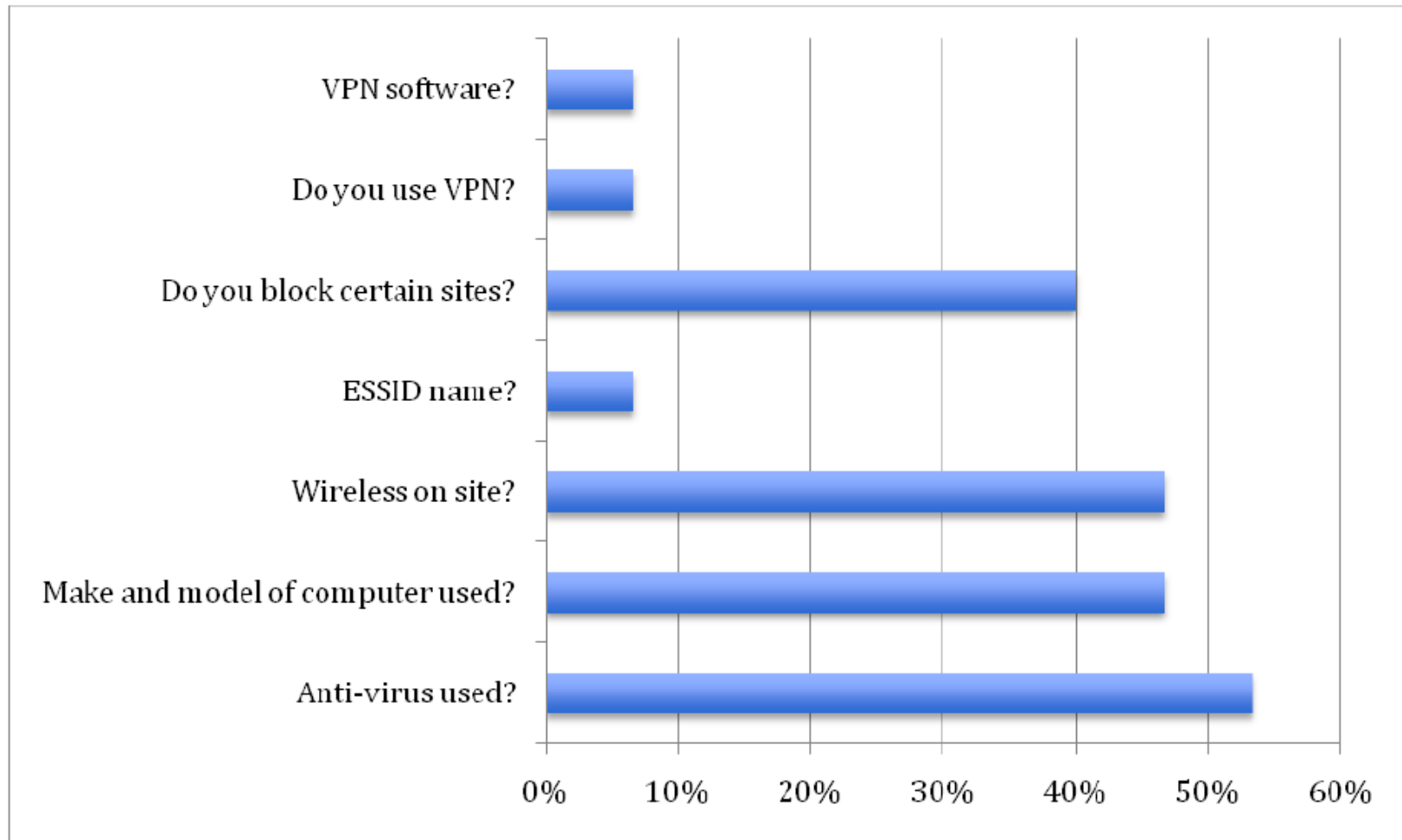
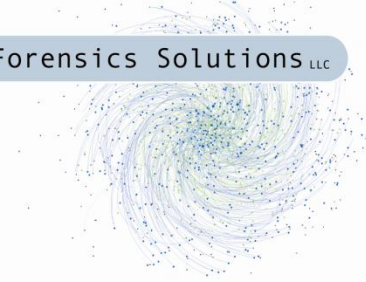


Old Systems are More Vulnerable!



!!!!!!!!!!!!

Technical Flags, Cont.



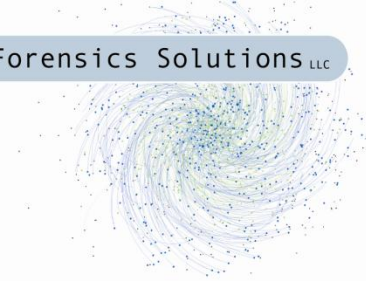
Ready to be Depressed?



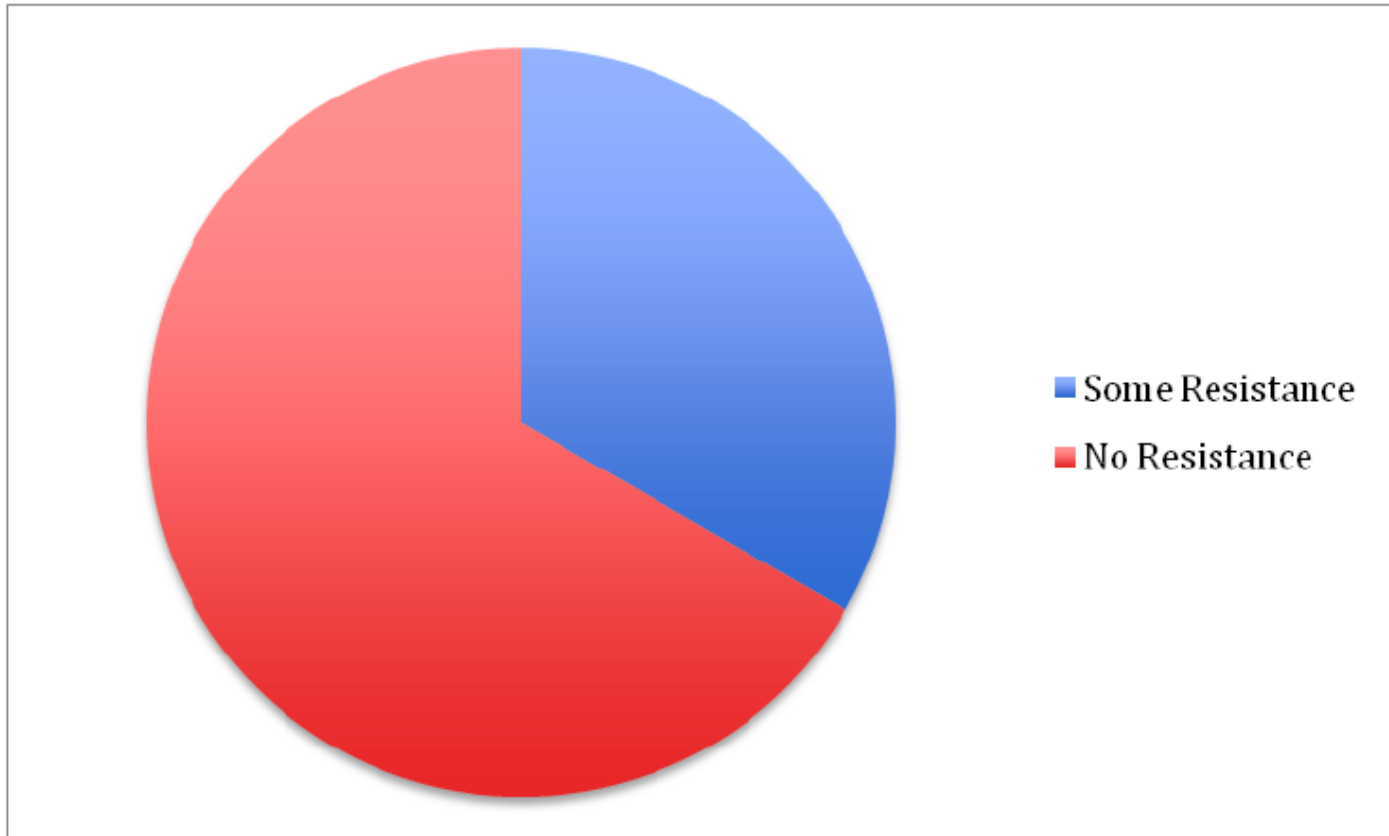
Number of Companies Called:	15
Possible Flags:	25
Number of Companies with Flags Captured:	14
Days Contest Was Held:	2
Total Phone Calls Made:	135
Companies Who Put Up Resistance:	7
Employees Who Put Up Resistance:	11

← *

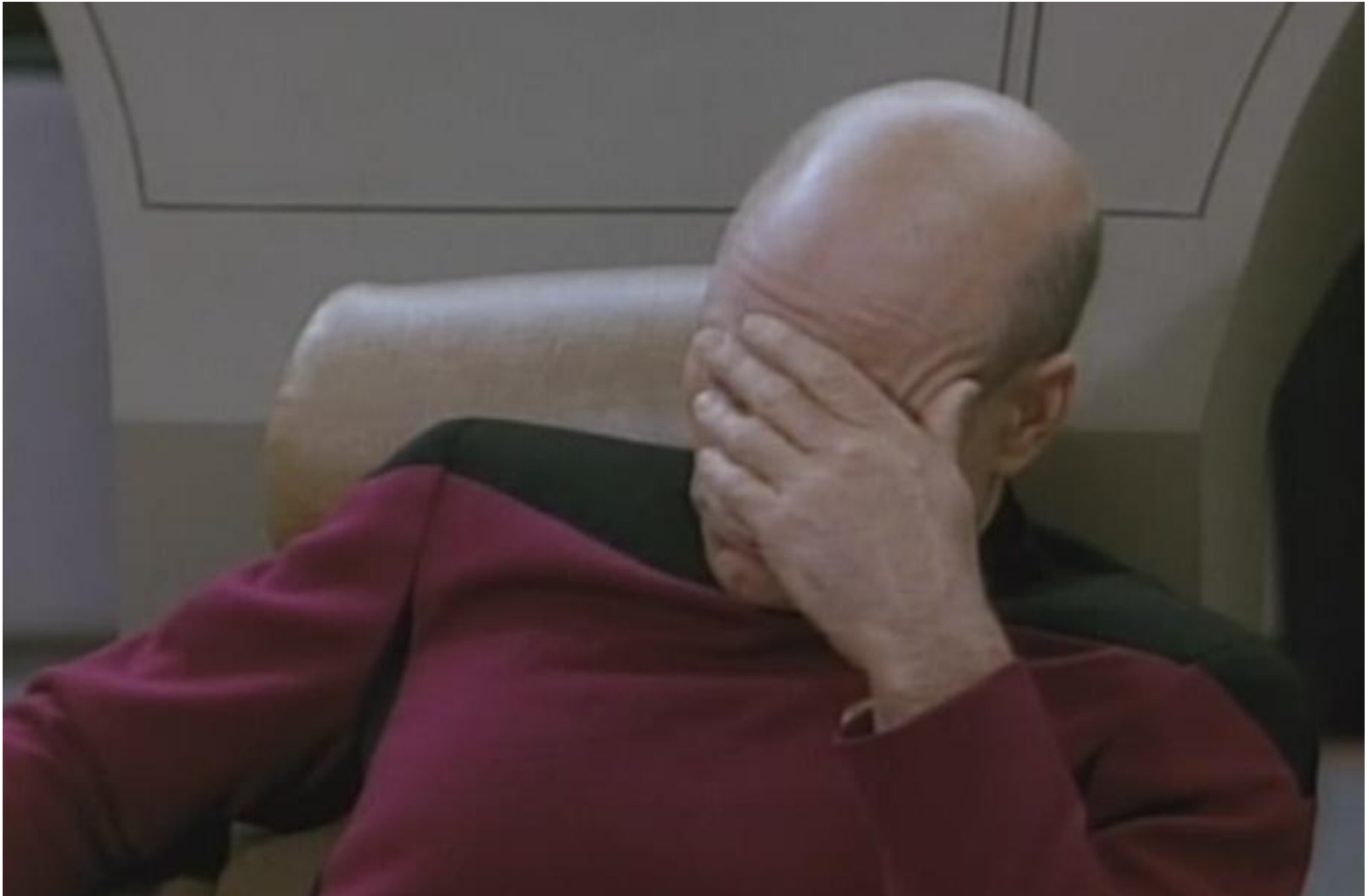
*** Company too busy to respond to questions!**



Depression: Part 2



Solution to resistance: Just hang up and call again. You'll get another employee.





Basic Defense

- Be suspicious of phone calls, emails, and visits from strangers if sensitive information is requested
- Verify the identity of the requestor
 - Don't just hand out sensitive information over the phone or through email
- Verify validity of suspicious requests
 - Go see the person in charge (if possible) or communicate with them directly to verify that the request should be granted



More Defense

- **SECURITY AWARENESS TRAINING for ALL EMPLOYEES!**
- Penetration tests
- Avoid falling for the “casual chatter” attack
- Before transmitting personal information over the internet, be sure the site is verified and the connection is secure (HTTPS)
- Company policies should not require (or even allow) submission of usernames /passwords / etc. through email

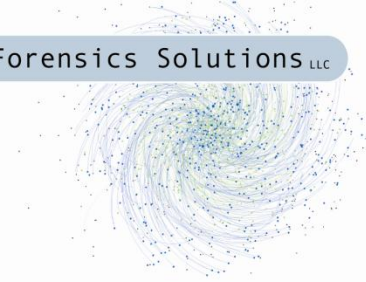
Be Suspicious (Paranoid, Even!)

- Warning signs:
 - Extreme urgency
 - “You’ll be sorry if you don’t...”
 - Refusal to provide verifiable information such as a callback number
 - Idle chatter, flattery, irrelevant distracting conversation if the person is unknown to you
 - Phone numbers / email addresses not directly attributable to the company
- And beware tricks (misspelled domain names, “phone system is down”, etc.)



Some Resources

- <http://www.social-engineer.org/>
- http://www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf
- CERT advisory: <http://www.us-cert.gov/cas/tips/ST04-014.html>
- The Art of Deception, by Kevin Mitnick
- Crimeware: Understanding New Attacks and Defenses, by Markus Jakobsson and Zulfikar Ramzan
- The Art of Computer Virus Research and Defense, by Peter Szor
- Blackhat, DEFCON, and other security conference presentations and proceedings
- (lots more—email me if you're interested)
- Your own paranoia!



Questions?

- Only defense against social engineering is education
- But everyone has to get it
- And everyone has to actually care (or at least be scared to death)
- One set of loose lips and (potentially) you're sunk!

Thanks!

daryl@digdeeply.com

joe@digdeeply.com