Social Engineering Capture the Flag Results

Defcon 20

www.Social-Engineer.Org

Written by:
Christopher J. Hadnagy
& Eric Maxwell

Social-Engineer.Org

Social Engineering Capture the Flag Results

Defcon 20

defcon@social-engineer.org

Written by:
Christopher J. Hadnagy
& Eric Maxwell

Table of Contents

Executive Summary

This year at Defcon 20 in Las Vegas, NV, the team at Social-Engineer.org arranged and ran the third consecutive Social Engineering Capture the Flag contest dubbed, “The Battle of the SExes”. Our focus was to answer the age old question, “Who are better social engineers, men or women?”

We started out with twenty contestants, ten men and ten women. We then selected ten companies, many new and some that were targets in the past. Unlike previous years, the same company was assigned to more than one individual. We assigned both a male and female contestant to each target company. A coin toss provided the winning contestant the choice of going first or last and the company was called back-to-back by the contestants.

The event’s goal, as in previous years, was to raise awareness of the current and ongoing threat that social engineering poses for companies and their customers. The contest served as a demonstration of commonly used tactics and attack vectors employed by malicious social engineers, but without being malicious. Very strict rules were put in place, which prevented any contestant from breaking the law, obtaining sensitive personal information, or leaving their targets feeling poorly. The contest drew contestants from all walks of life and all skill levels.

Primary Findings

As previously mentioned, this year’s competition was focused on trying to determine not only if social engineering threats have received more attention from corporations in the USA over the last 12 months, but to see if there was a way to determine which gender may be better in a head-to-head social engineering competition.

Listed below are the basic statistics of the Defcon 20 Social Engineering Capture the Flag Contest:

Target Companies	10
Contestants	20
Completed Calls	18
Possible Flags	37
Total Points by Female	1675
Total Points by Male	2329.5
Industries Represented	5

The point values listed above do not always indicate a company's true weakness or strength. The "X factor" is the skill of the caller and the employee they get on the phone. In this report, we will use data collected during the live call to determine the way the companies handled the social engineering attack.

The companies that callers had the most difficulty extracting data from were companies in the oil industry. Companies, like Mobil and Shell, tended to be more cautious and reluctant to answer questions and inquiries. Companies that had a large presence, such as the Wal-Mart and Target, seemed to be the weakest, unlike last year. Therefore, we can speculate that security awareness training is less prevalent and less effective in retail and customer service organizations as opposed to gas/oil companies.

Another preliminary finding was that in all cases where the caller asked the target to visit a website, even in the cases where there was some reluctance, the target ended up visiting the site. The following pages will outline this in greater detail.

Background and History of CTF Event

The core rules remained the same as in previous years. We forbid collecting of sensitive data such as credit card information, social security numbers, and passwords. Only Open Source Information

(OSI) was allowed to be gathered. We did not allow physical penetration into companies nor did we allow digital penetration. In addition, we did not allow the contestant to visit a location of their target or interact with any person from the target before the call at Defcon. We also specifically avoided sensitive industries such as Government, Education, and Finance.

Months prior to the Defcon 20 event, we solicited for contestants who wished to participate in the contest. We were quickly overwhelmed with responses and applications. We selected twenty contestants, ten men and ten women, and assigned a Fortune 500 company to each set of contestants. This year, we wanted to see who would do better in a social engineering scenario, men or women. Our longest running poll on Socal-Engineer.org clearly indicated the majority of people thought women would make the best social engineers. We wanted to find out if this was accurate. We randomly paired a male contestant with a female contestant and assigned a single company to the random pair. Contestants were unaware of each other and unaware of whom they were paired with previous to showing up at their time slot at Defcon 20.

Contestants were given two weeks to gather as much intelligence about their company. The contestants were allowed to use only Open Source Information that could be obtained by Google, LinkedIn, Flickr, Facebook, Twitter, WhoIs, etc. During this information-gathering phase, contestants could try and capture as many of the pre-defined flags as possible. Flags captured during this phase of the contest were worth half points. The information gathered was to be assembled into a professional social engineering report. Contestants were provided with a sample report, but they were not required to use this template. Points were awarded for the professionalism and the quality of the report submitted.

The contestants were then assigned a time slot to perform their live calls on either Friday or Saturday during Defcon 20 in Las Vegas, NV. We scheduled the time slots so that the male and female contestants went back-to-back. The order of who went first was decided by a coin toss for each pair. Great care was made in the development of the contest to ensure maximum success for the contestants. Since the contest was held on the West Coast, companies whose headquarters were located on the East Coast were assigned earlier time slots. Furthermore, companies who were easily reachable during non-standard business hours, such as retail, were given Saturday time slots.

Contestants were placed in a soundproof booth and were required to provide us with a list of phone numbers to call along with phone numbers they wanted for us to spoof. (Spoofing was not required, but was permitted if they wanted to use it.)

Caller ID spoofing is a trick used to fake or spoof your caller ID. This allows the caller to forge the incoming phone number, a tactic commonly used by social engineers. The contestant was free to use the entire twenty-minute slot to perform as many or as few calls as they wanted. Flags captured during this portion of the event were awarded full points. The same flag could be captured multiple times from the same contestant by making multiple, consecutive calls within the allotted twenty minutes. For example, if the contestant called three different people and got all three to navigate to the website of the contestant's choosing, they would have received seventy-five points**.

Per Nevada law, no recording of any type was permitted. United States federal law requires only one party to be notified in the event a phone conversation is recorded; therefore, you can record a call without the person you are talking to providing consent. Many states, Nevada included, have created additional laws requiring both parties to consent. Since we could not obtain consent without jeopardizing the integrity of the contest, no recording of any type was performed.

**see flag values below

NOTE: It's important to note that all contestants were required to place a $20 *fully refundable* deposit down to ensure they completed the contest. All contestants were refunded this deposit immediately after completing their call at the Defcon portion of the contest.

Flags

The flags were pieces of information based on non-sensitive data pertaining to the inner workings of a company. Each flag was given a point value based on the degree of difficulty in obtaining the information. The contestant's job was to develop a believable pretext along with a real world attack vector that would enable them to obtain as many flags as possible. The vector was then performed live at Defcon 20 during their 20-minute time slot. The same flag could be captured multiple times during the 20-minute time slot if the contestant made multiple phone calls

DEFCON 20 Social-Engineer.Org SECTF Flag List

Logistics	Pts	Company Wide Tech	Pts
Is IT Support handled in house or outsourced?	5	What operating system is in use?	10
Who do they use for delivering packages?	7	What service pack/Version?	15
Do you have a cafeteria?	5	What program do they use to open PDF documents and what version?	10
Who does the food service?	7	What browser do they use?	10
Do you use disk encryption? If so which type?	7	What version of that browser?	15
Other Tech		What mail client is used?	10
Is there a company VPN?	7	What version of the mail client?	10
Do you block websites? (Facebook, EBay, etc)	3	Fake URL(getting the target to go to a URL)	25
Is wireless in use on site?	3	**Employee Specific Info**	
ESSID Name?	7	How long have they worked for the company?	5
What make and model of computer do they use?	5	What days of the month do they get paid?	5
What anti-virus system is used?	10	Employee termination process?	5
Can Be Used for Onsite Pretext		New hire orientation information?	3
Do you have a cleaning/janitorial service?	5	Employees schedule information	5
What is the name of the cleaning/janitorial service?	7	- (start/end times, breaks, lunches)	5
Do you have a bug/pest extermination contract	5	Do they have a PBX system?	5
With Whom?	7	What sort of phone system is used?	7
What is the name of the company responsible for the vending machines onsite?	7	When was the last time they had awareness training?	10
Do they have trash handling?	5		
Who handles their trash/dumpster disposal?	7		
Do you have a 3rd party security guard company?	9		
Who is it?	10		

Results and Analysis

Companies & Industries Called

Similar to last year, we wanted to target a wide range of industries to see how the different industries fared against others in their own industry as well as how they would do against other companies in different industries. The companies were not aware that they were being targeted. We included some companies from last year and added some new ones.

While the actual number of companies targeted decreased, we had two contestants (one male, one female) assigned to each company for an initial total of twenty phone calls.

Below are the targets and industries:

- Freight
  - UPS
  - FedEx
- Telecom
  - Verizon *
  - AT&T *
- Oil
  - Shell
  - Mobil
- Retail
  - Target *
  - Wal-Mart *
- Tech
  - Cisco
  - HP

* Designates that the company was targeted last year.

Open Source Information Gathering

The initial information-gathering phase is the most crucial in any social engineering engagement. This phase is the most laborious, least “sexy”, but most important. This is where professional social engineers spend the majority of their time. The time and effort you put into this phase can determine if your social engineering engagement will succeed or fail. It is important to understand the valuable information that can be obtained by simply making use of the tools available to us on the Internet. Tools such as Google, Facebook, LinkedIn, Flickr, etc. are a social engineer’s best friends.

The following is a list of tools most commonly used by our contestants during the information-gathering phase.

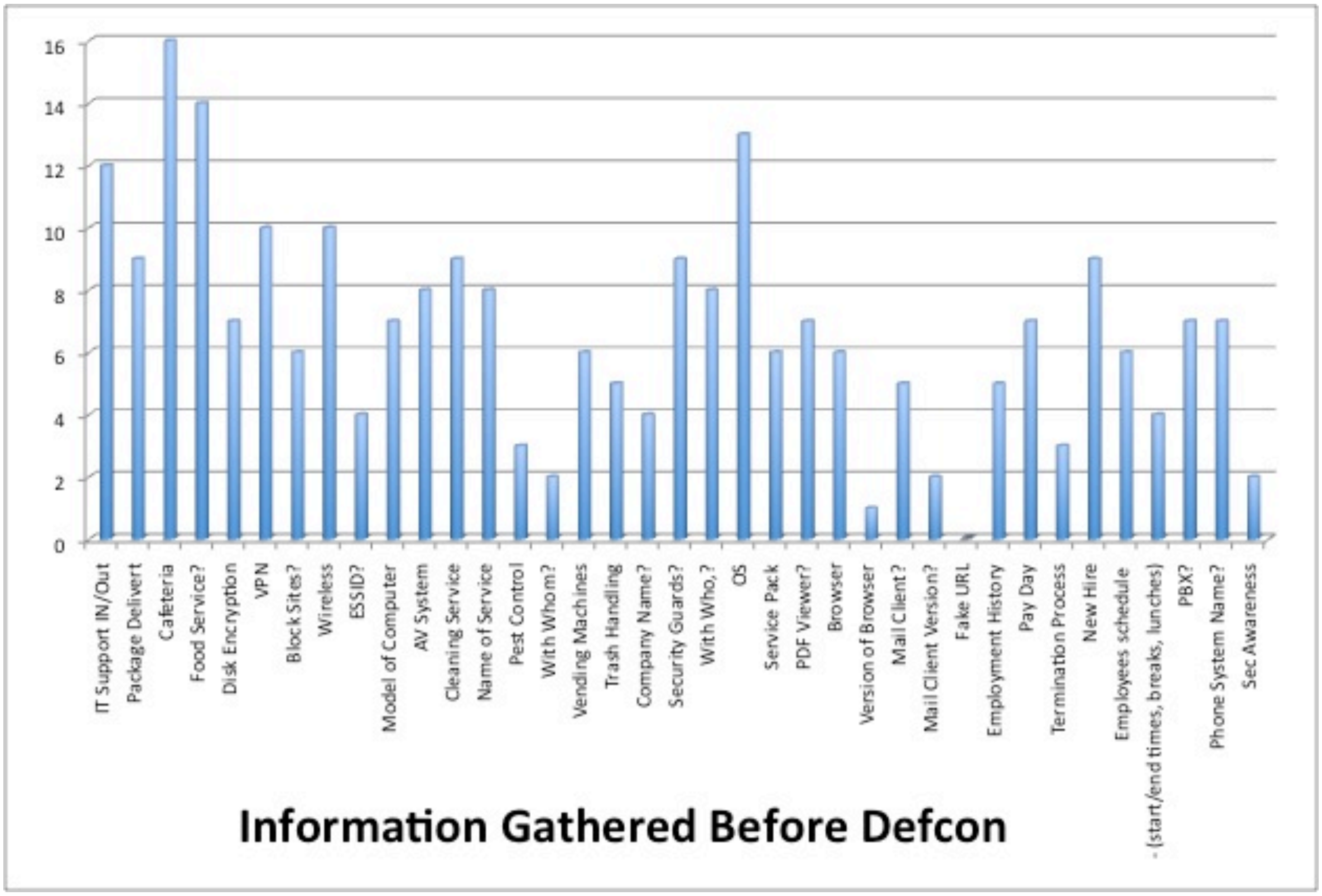
- Google
- Maltego
- FriendFinder
- Bing
- Twitter
- PiPl
- Bing Images
- Facebook
- Plaxo
- Google Maps
- Wordpress
- Shodan
- PicasaWeb
- Whois
- WGet
- Vimeo
- Tineye
- Wayback Machine
- LinkedIn
- Monster
- GlassDoor
- Yelp
- Craigslist
- Jigsaw
- Spokeo
- Misc
- YouTube
- Foursquare
- Friendster
- NetCraft
- Wikipedia
- MySpace
- Google Images
- Blogspot
- Telnet

In fact, as you will see, with very specific exceptions, most of our flags were more frequently captured during the information gathering and report creation phase.

	Found During OSI	%	Found At Defcon 20	%
IT Support In/Out	12	60%	4	20%
Package Delivery?	9	45%	2	10%
Cafeteria?	16	80%	7	35%
Handle Food Service?	14	70%	7	35%
Disk Encryption	7	35%	2	10%
VPN?	10	50%	6	30%
Website Blocking?	6	30%	8	40%
Wireless In Use?	10	50%	6	30%
ESSID?	5	25%	1	5%
Make of Computer	7	35%	4	20%
Anti Virus?	7	35%	6	30%
Janitor service?	9	45%	5	25%
Janitor Name?	8	40%	5	25%
Exterminators?	3	15%	5	25%
With Whom?(pest)	1	5%	1	5%
Vending Machines?	6	30%	4	20%
Trash Handling?	5	25%	5	25%
Company for Trash removal	4	20%	1	5%
3rd Party Security?	9	45%	6	30%
Who does Security?	8	40%	2	10%
OS	13	65%	11	55%
Service Pack	6	30%	2	10%

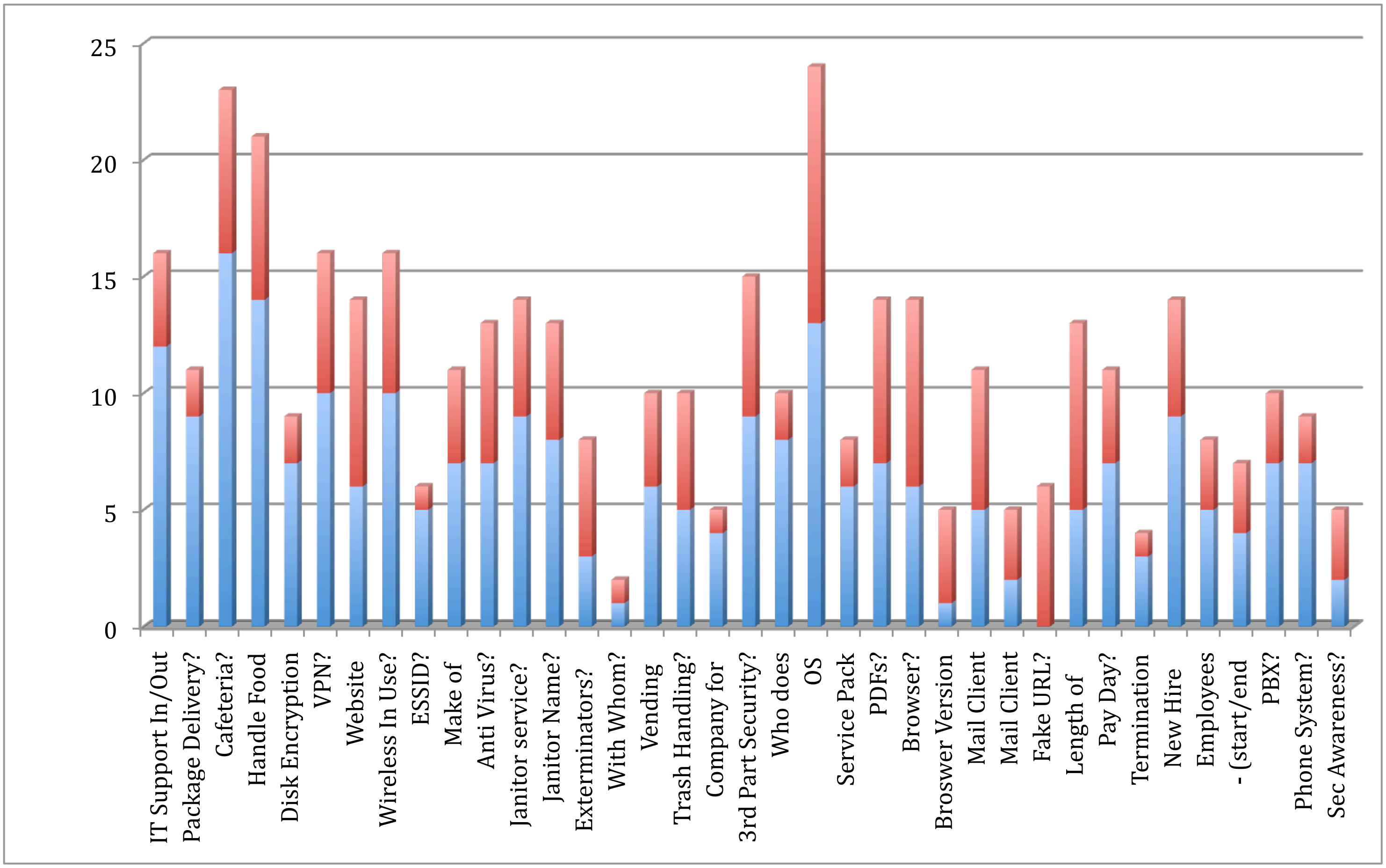
PDFs?	7	35%	7	35%
Browser?	6	30%	8	40%
Browser Version	1	5%	4	20%
Mail Client	5	25%	6	30%
Mail Client Version	2	10%	3	15%
Fake URL?	0	0%	6	30%
Length of Employment	5	25%	8	40%
Pay Day?	7	35%	4	20%
Termination Process	3	15%	1	5%
New Hire Orientation?	9	45%	5	25%
Employees schedule	5	25%	3	15%
- (start/end times, breaks, lunches)	4	20%	3	15%
PBX?	7	35%	3	15%
Phone System?	7	35%	2	10%
Sec Awareness?	2	10%	3	15%

This graph shows a breakdown of the flags and the amount they were captured prior to Defcon utilizing only OSI sources.



Information Gathered Before Defcon

In the chart below, the blue line represents the flags captured prior to Defcon using Open Source Information and the red line represents flags captured during the calls at Defcon.



The above table and chart show that leakage of information into the public domain is a big problem for companies. The fact that most flags could be obtained through publicly available information speaks volumes to the problem. Companies and their employees are primarily responsible for this leakage.

Often these leaks were not due to confidential documents or ex-employees, but well meaning employees tweeting or blogging about things on LinkedIn or other social media sites. In addition, photos can be very revealing. Photos can include a lot of details about the employee, the company, and the technology used.

Noteworthy Information Leakage

To illustrate the dangers of information leakage, without outing the offending companies, we've assembled some of the more noteworthy and egregious incidents of information leakage. These accounts are taken directly from the reports we collected from the contestants prior to Defcon. An overwhelming theme this year was employees posting pictures of their badges and a gross misuse of location-based services and social media. Mixing business social media and personal social media seems to have increased from years past. This is not surprising given how ubiquitous social media has become in our daily lives. Couple that with the increasing trend of "Bring Your Own Device (BYOD)" and we have some serious threats to security.

One large retailer targeted by our contestants had full pictures of employee badges published online for all to see. Using a simple badge-cloning machine, available for about $1000 on the Internet, a criminal could use the published photo to clone a badge and gain access to the facilities. During one of our 5-day training courses held this year, we had a student from a major computer company in attendance. To illustrate a point, during our break, we scanned the Internet for a badge picture, cloned it, and when class resumed, showed it to the employee. The employee was shocked and stated that our cloned badge would definitely allow us access to their facilities. We accomplished this during a 15-minute break and a simple Google search.

This same retailer went one step further and published pictures of a new warehouse facility being built. These pictures were not only of the exterior building, but also contained detailed photos of the locations of server rooms, alarm locations, and the location of security cameras!

One report of a large telecom company showed pictures that an employee tweeted that contained the employee's cell phone settings. The phone settings showed the Wi-Fi ESSID of his organization. This information saves the attacker time, effort, and basically shows him which ESSID may be used. It also gives the attacker information he could use on a call to pretext past an unsuspecting employee.

An executive at this same organization tweets his location, both professionally and personally, via Foursquare. This company's report is a perfect illustration of why strict social media policies need to be put into place. It would be very easy to build an extensive profile on the executive that could be used for a highly targeted spear phishing attack or in person elicitation attack.

Another large retailer had pictures posted to the Internet detailing their internal employee work areas. These pictures featured images of their computers, some containing pictures of the computer screens. These pictures clearly showed the operating systems in use and which applications were in use. This information can be used, by an attacker, to tailor exploits sent to the organization. If an attacker knows you're using Windows XP, the attacker won't waste time sending a Windows 7 exploit. In addition, some software versions can be deduced simply knowing the operating system. This information can further aid the attacker in their quest. This retailer also had some employee badges visible in pictures. As with the other retailer discussed above, the images for this retailer's badges were clear and prominent enough to easily clone.

One report outlined findings of multiple documents clearly marked CONFIDENTIAL. These documents were published 'live' to the Internet and indexed freely by search engines. The documents discovered contained detailed information about the internal policies and procedures of the company. This information can be used in a variety of ways by an attacker to successfully infiltrate an organization.

Men vs. Women

This year's theme, Battle of the SExes, was originally conceived a year ago, after Defcon 19. Having a competition where men battled the women was a great idea... on paper. The problem was, historically, we had a maximum of three women sign up for the contest in two years. How could we possibly get enough women interested in the contest to fill ten slots, seven more than we had received in the previous two years?

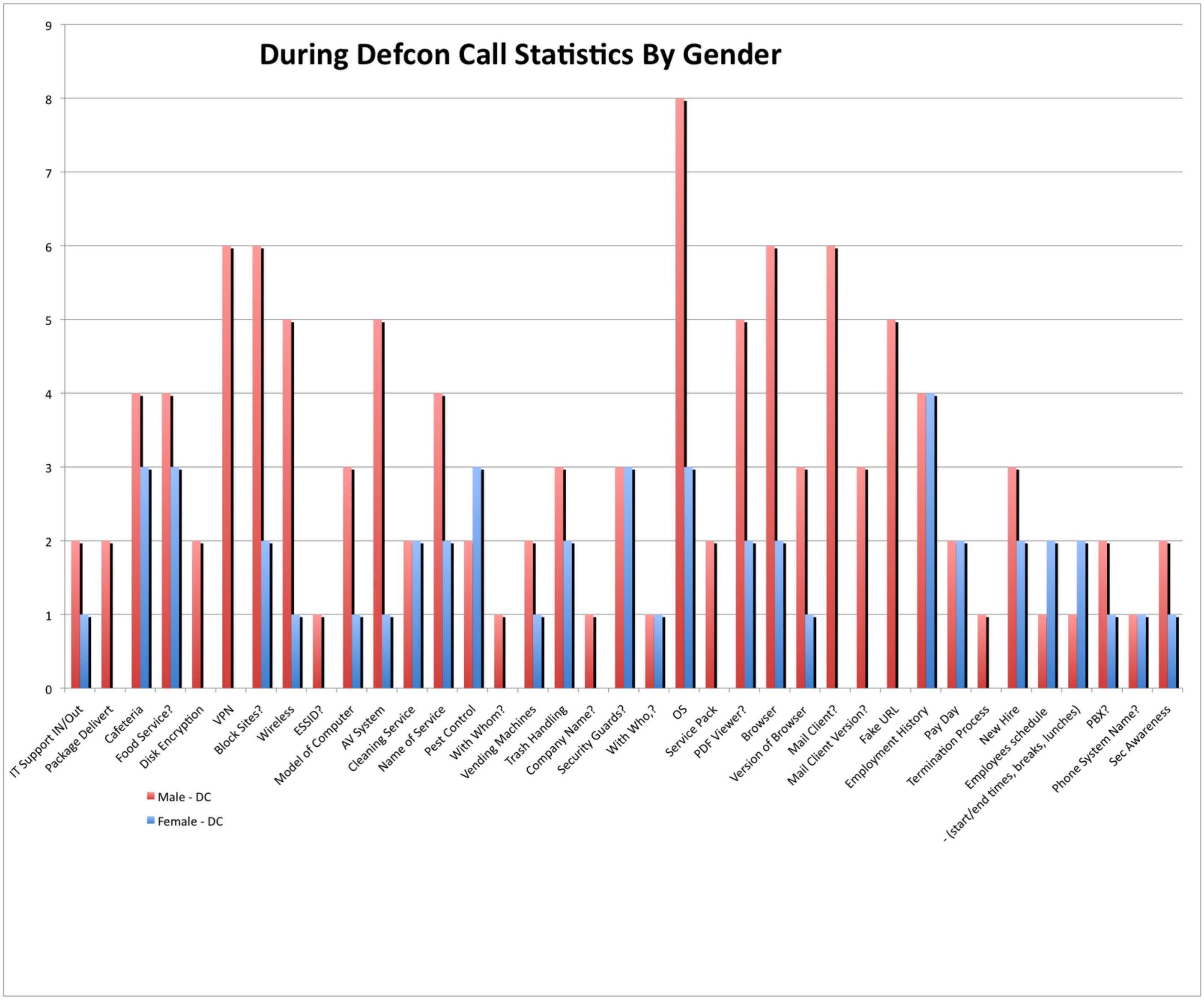
We worked on reframing the community. In the time between Defcon 19 and the Defcon 20 SECTF sign up going live, Social-Engineer.org was engaged in a deliberate effort to get women interested in social engineering, to get women who were already interested to be willing to do so publicly, and to get the world thinking about who truly makes the better social engineer, men or women?

Through a series of blog posts, podcasts, and the longest running poll in Social-Engineer.org history, we believe we were successful. We received so many applications this year for the SECTF, we spent week's just selecting contestants and in the end, had a full roster of men vs. women. Ten men and ten women were selected along with ten companies as targets. Coming into the contest, it was our hypothesis, based on our observations in the field and the results of the above-mentioned poll (not to mention the power our wives hold over our psyche!), that women would be the clear victors in the SECTF contest.

The graph below titled, *During Defcon Call Statistics by Gender,* shows the flags captured at Defcon 20. Only three flags were captured more by women than men:

- Discovering the target’s pest control company
- The target company’s employee’s schedule
- The employee’s lunch and break schedule

Five of the flags were captured the same amount of time by men and by women. The rest of the flags were captured significantly more frequently by the men than by the women. Some flags, such as whether the company uses disk encryption or information about the company VPN, were never captured by any female contestant. It should also be noted that the flags captured more by women had significantly less point value than some of the flags captured by the men. The point value of a flag is in direct correlation with the risk surrounding leakage the information. The data clearly shows that men dominated the competition, much to our surprise.


During Defcon Call Statistics By Gender
9
8
7
6
5
4
3
2
1
0
IT Support IN/Out
Package Delivert
Cafeteria
Food Service?
Disk Encryption
VPN
Block Sites?
Wireless
ESSID?
Model of Computer
AV System
Cleaning Service
Name of Service
Pest Control
With Whom?
Vending Machines
Trash Handling
Company Name?
Security Guards?
With Who,?
OS
Service Pack
PDF Viewer?
Browser
Version of Browser
Mail Client?
Mail Client Version?
Fake URL
Employment History
Pay Day
Termination Process
New Hire
Employees schedule
- (start/end times, breaks, lunches)
PBX?
Phone System Name?
Sec Awareness
🟥 Male - DC
🟦 Female - DC

Pretexts

After the crucial information-gathering phase is complete, the next step is to develop a pretext. A pretext is a believable story the social engineer crafts in order to gain trust and legitimacy from the target. Due to the nature of the Capture the Flag event, we see the frequent use of the customer pretext. This is due, in part, to the fact that some contestants must perform on a Saturday and for some companies, a customer service line is the only entry point during non-standard business hours. Another reason for the frequency of this pretext is the fact that it’s usually the easiest pretext to develop and carry out. Since a majority of the contestants have never tried anything like this in the past, this pretext is an attractive one. That being said, only two people used the customer pretext this year and it was in the form of a student. The other student pretexts used were collecting information in order to make informed scholastic decisions.

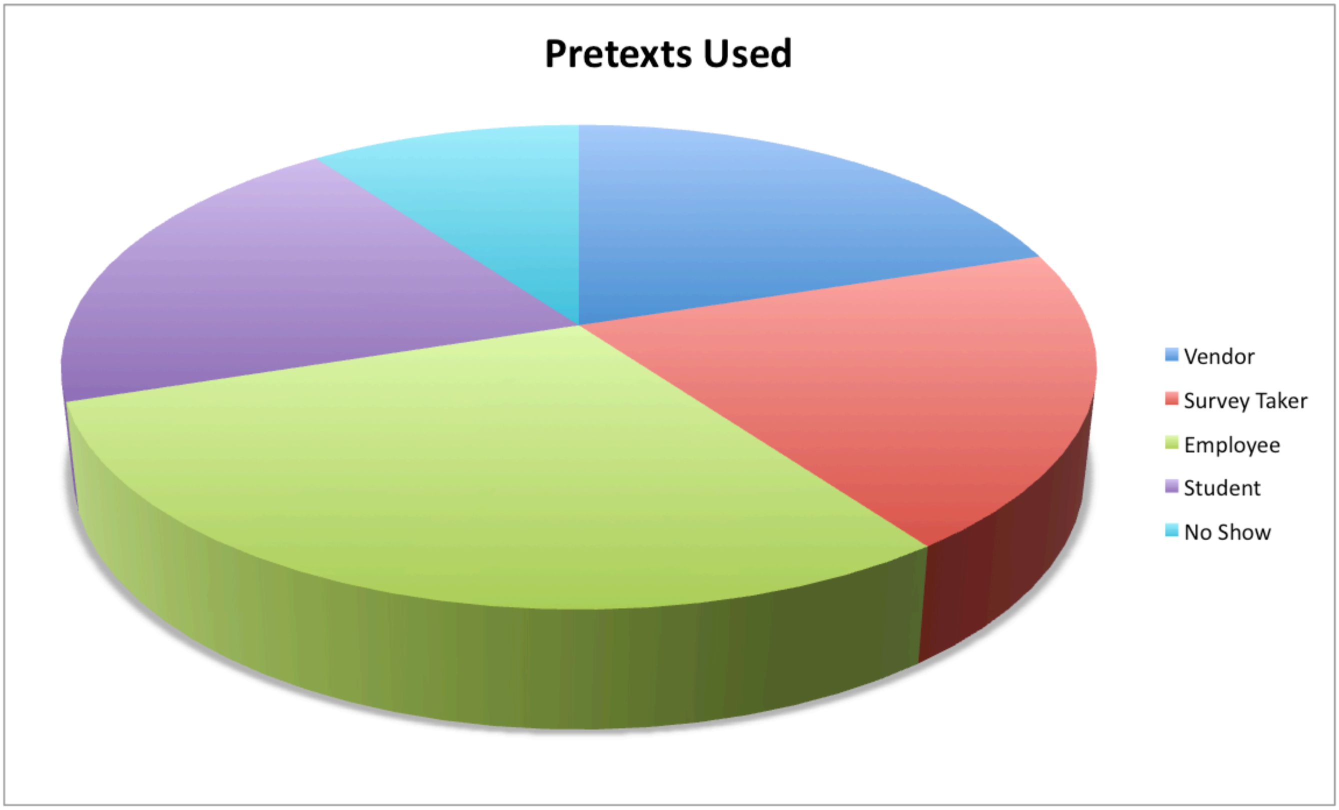
As we’ve seen in the past, the hardest pretext to use and pull off is that of an internal employee. This is also the most efficient and fruitful pretext used in the contest. This year, the top three contestants used this pretext with devastating results. For the first time in the history of the Social Engineering Capture the Flag competition, one contestant, using this pretext, captured all the flags! Utilizing caller ID spoofing, this pretext can build immediate trust. Assuming the social engineer has done the appropriate information gathering (homework) and can “walk the walk”, this level of perceived trust can and does go a long way.

We saw three pretexts used this year that had not been used last year: the student, the survey taker, and the vendor. To our surprise, the survey taker was used 20% of the time. What was not surprising was this pretext’s limited success. The issue is that people don’t want to take time out of their day to answer questions from a total stranger over the phone. There was no psychological motivation created to take the survey. Had the caller given a gift, the success rate would have undoubtedly gone up. Unfortunately, the contest rules do not allow for gift offering, as we feel that victimizes the targets feelings and emotions too much.

The student pretext worked a little better because the social engineer used sympathy and played on people’s natural instinct to be helpful. In one case, our youngest contestant (17 years old) used this pretext very well and, in our opinion, very appropriately. This female contestant sounded young so playing the role of a student was the perfect pretext for her. Not only because it was closest in line with reality and therefore the easiest to “act out”, but because choosing the pretext of an IT Director would have presented some large psychological hurdles for the target to overcome before trust could be established.

The vendor pretext had more success than the survey taker, but not as much as the employee or student pretexts. The vendor pretext allowed the caller to assume certain trusts and also have good excuse for not sounding or acting like an insider. In addition, one caller used this pretext to offer "services" her company offered and in turn, finding out who the company presently used. Even though, by the end of the call, she had basically told the target she was a janitorial service that offers vending machines, security guard services, pest control, and a few other key business services, the target never seemed uncomfortable handing over this information to her. This pretext, when used skillfully, can yield a great bounty.

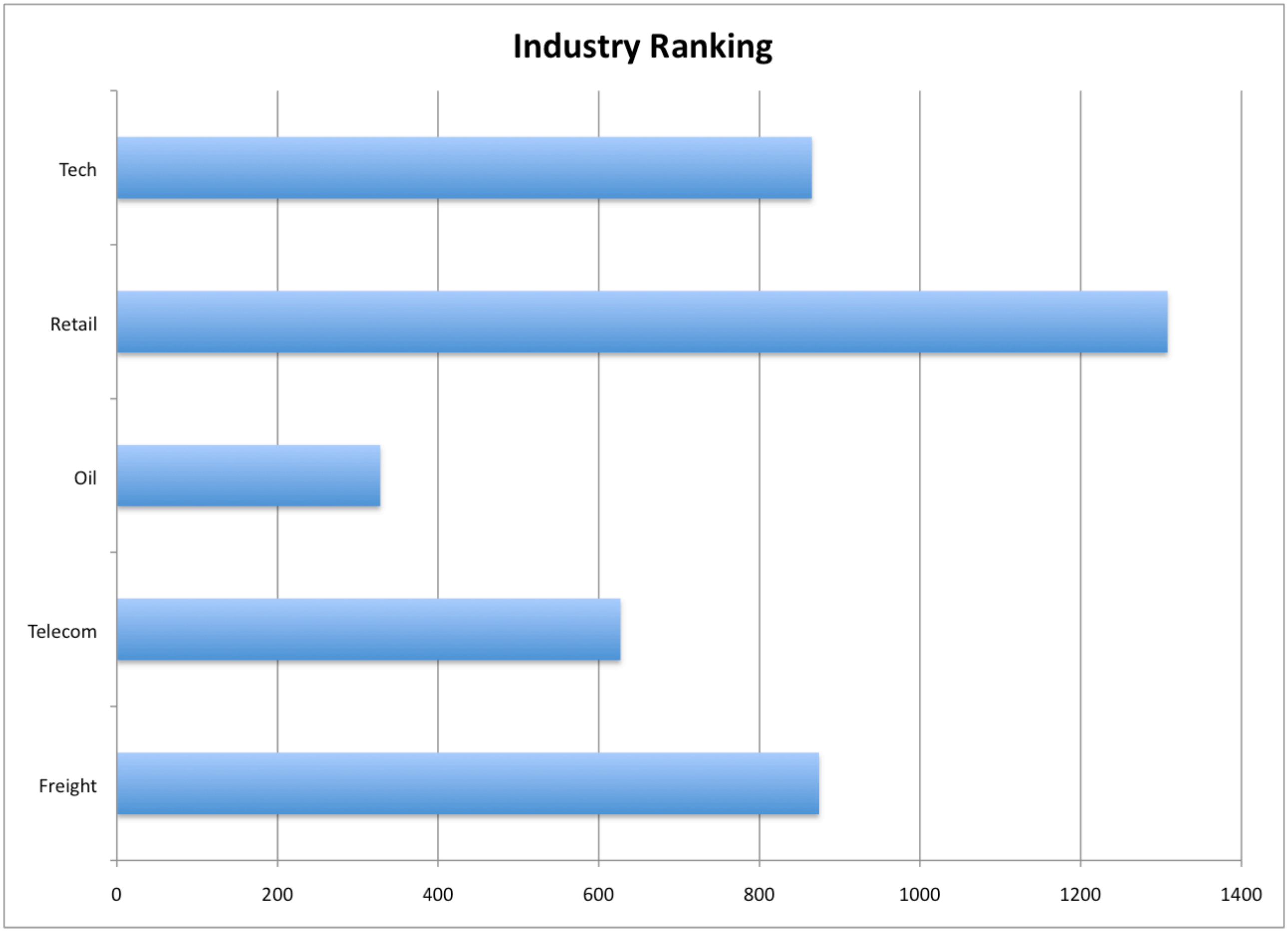
The following chart shows the breakdown of pretexts used :



Industry Performance and Target Ranking

As an industry, Oil and Gas put up the most resistance. Both Shell and Mobil yielded relatively low pre-Defcon flags and, amazingly, out of three phone calls (we had one no-show), only gave up **five points** total! This year, Shell gave up the least points before and during Defcon, followed closely by Mobil.

As you can see in the charts below, Oil and Gas fared the best and Retail did the worst. This is shocking since retail was one of the best in previous years. The numbers represent the amount of points captured in each industry. **The higher the number of points, the worse the industry did**.

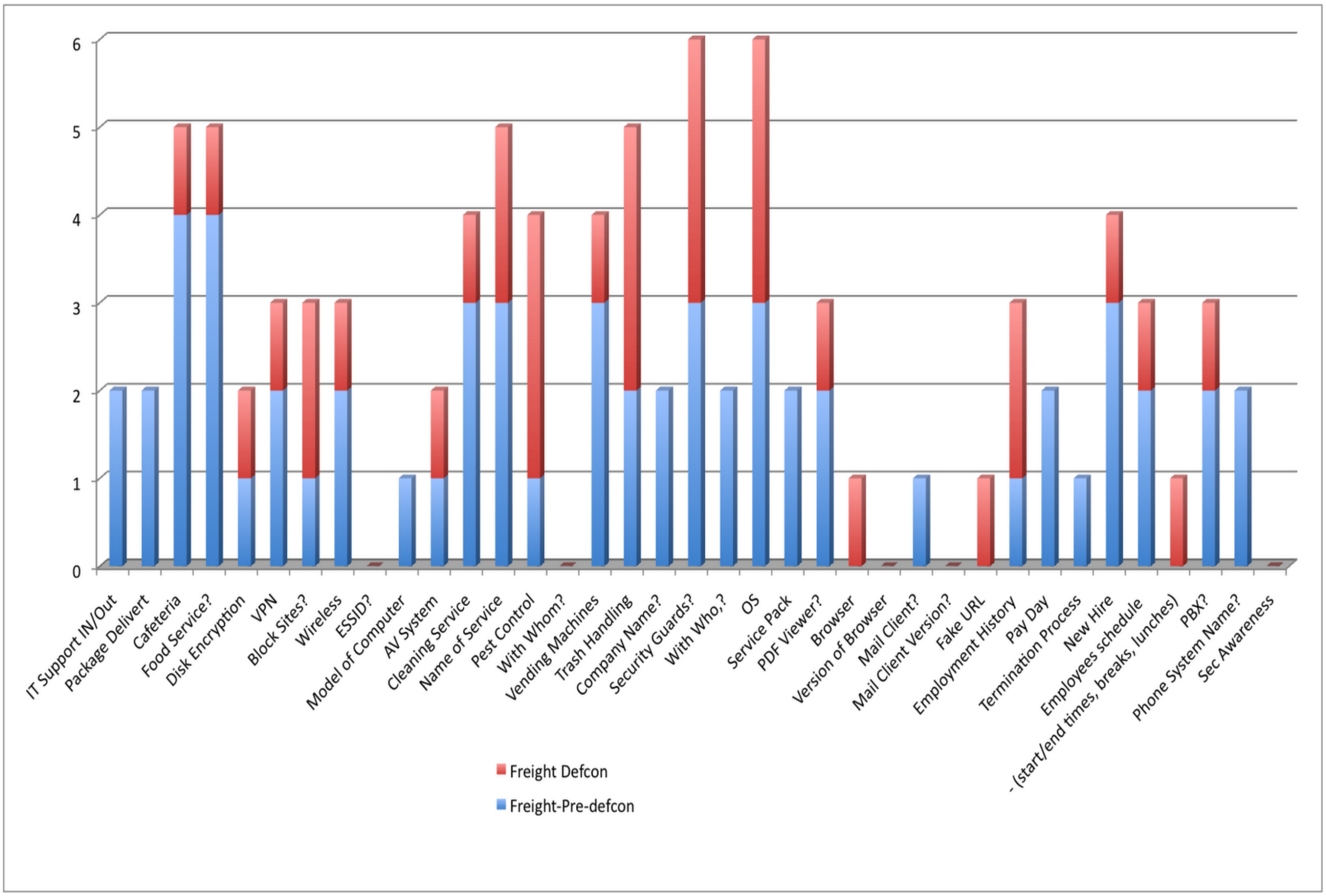


The charts below show a more detailed perspective about how the targets fared by industry. Each industry is broken down by information gathered "Pre-Defcon" and then the actual call during "Defcon".

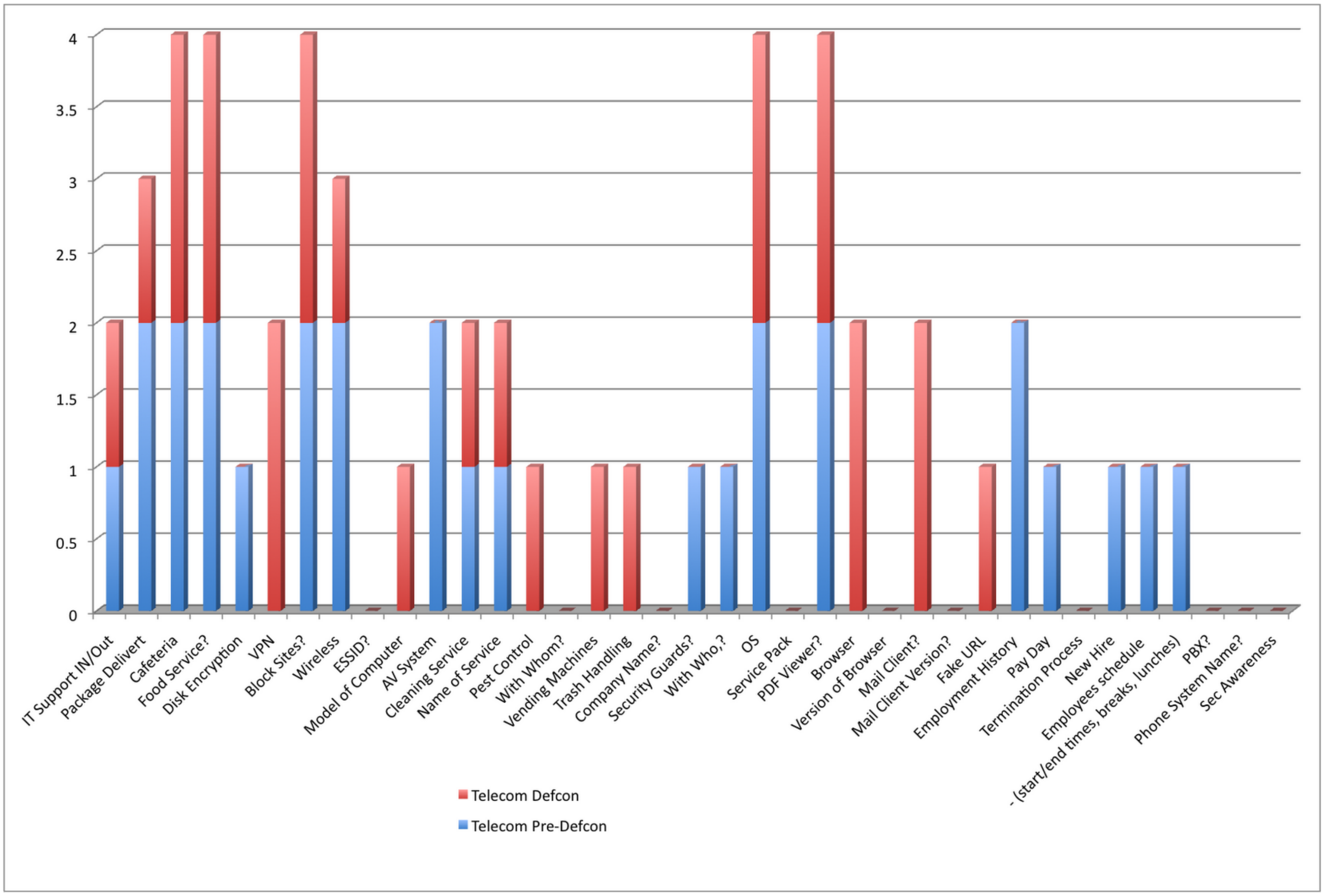
One shocking detail on this chart is how many industries willingly went to a website provided by the caller. In many cases, the site was obviously fake, but did not raise red flags in the minds of the employees.

The most gathered piece of data was if the targets have cafeterias or not, followed by the company who provides food service to these companies. Again, data that could lead to a breach should be more tightly guarded.

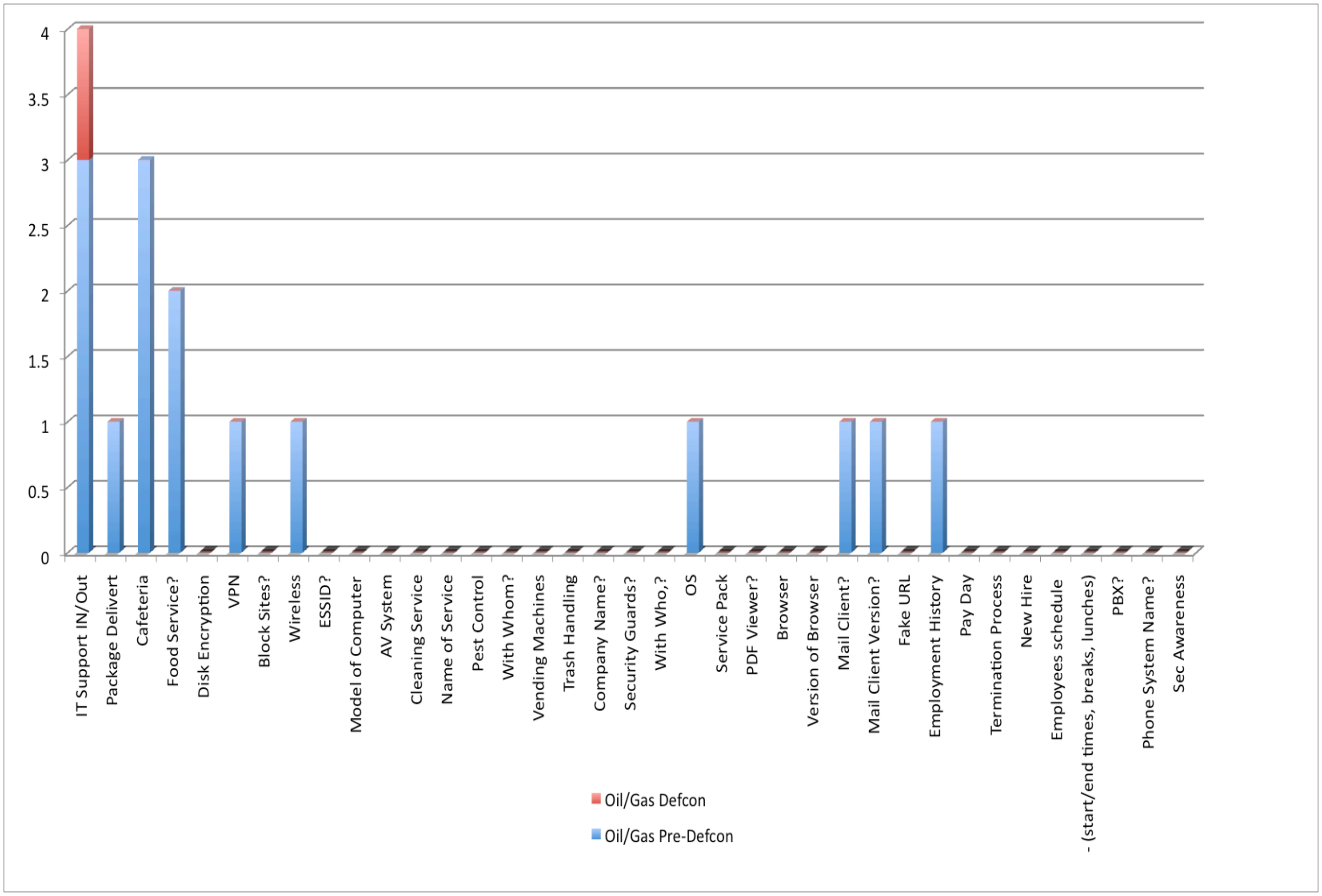
Freight



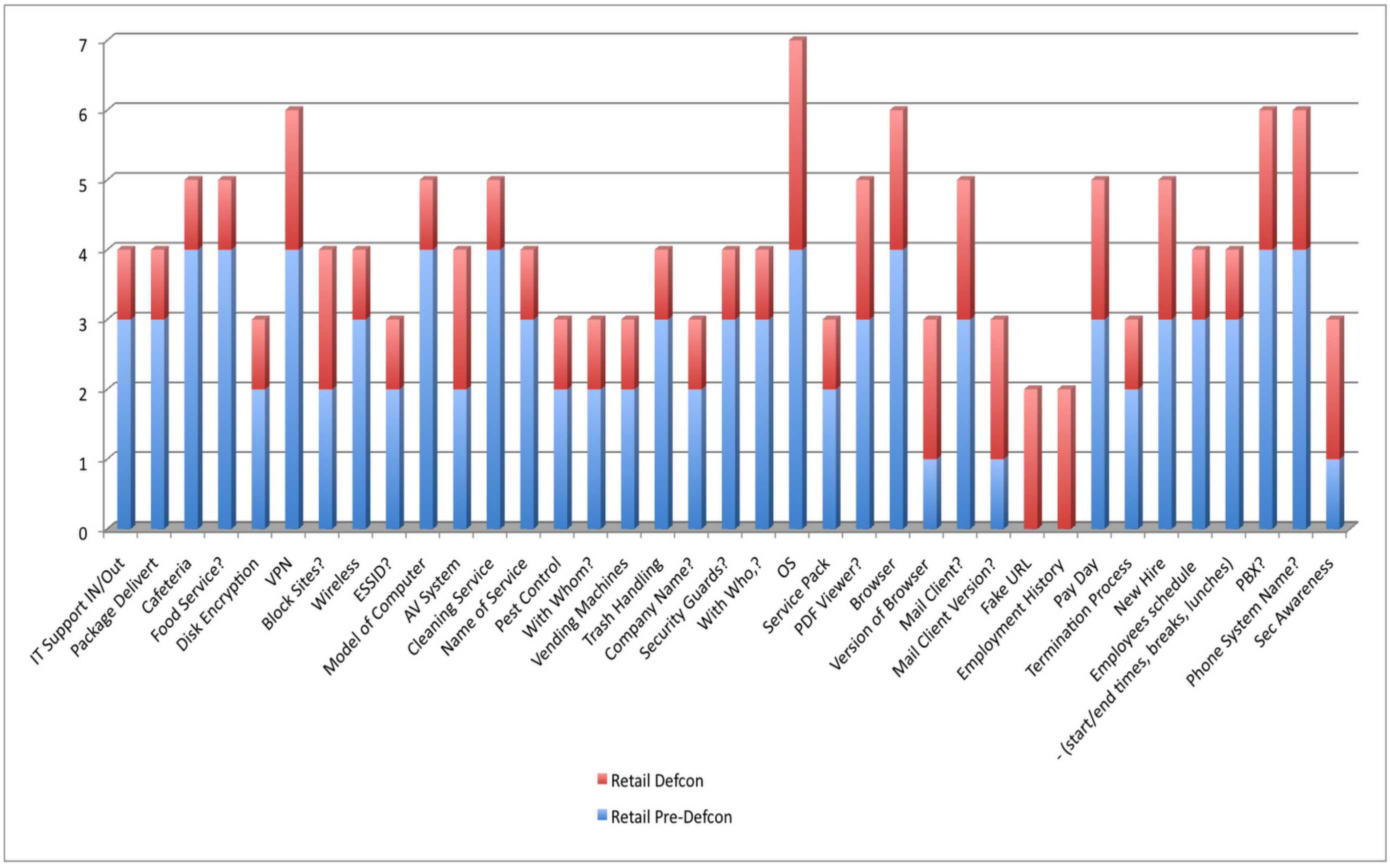
Telecom


4
3.5
3
2.5
2
1.5
1
0.5
0
IT Support IN/Out
Package Delivert
Cafeteria
Food Service?
Disk Encryption
VPN
Block Sites?
Wireless
ESSID?
Model of Computer
AV System
Cleaning Service
Name of Service
Pest Control
With Whom?
Vending Machines
Trash Handling
Company Name?
Security Guards?
With Who,?
OS
Service Pack
PDF Viewer?
Browser
Version of Browser
Mail Client?
Mail Client Version?
Fake URL
Employment History
Pay Day
Termination Process
New Hire
Employees schedule
- (start/end times, breaks, lunches)
PBX?
Phone System Name?
Sec Awareness
Telecom Defcon
Telecom Pre-Defcon

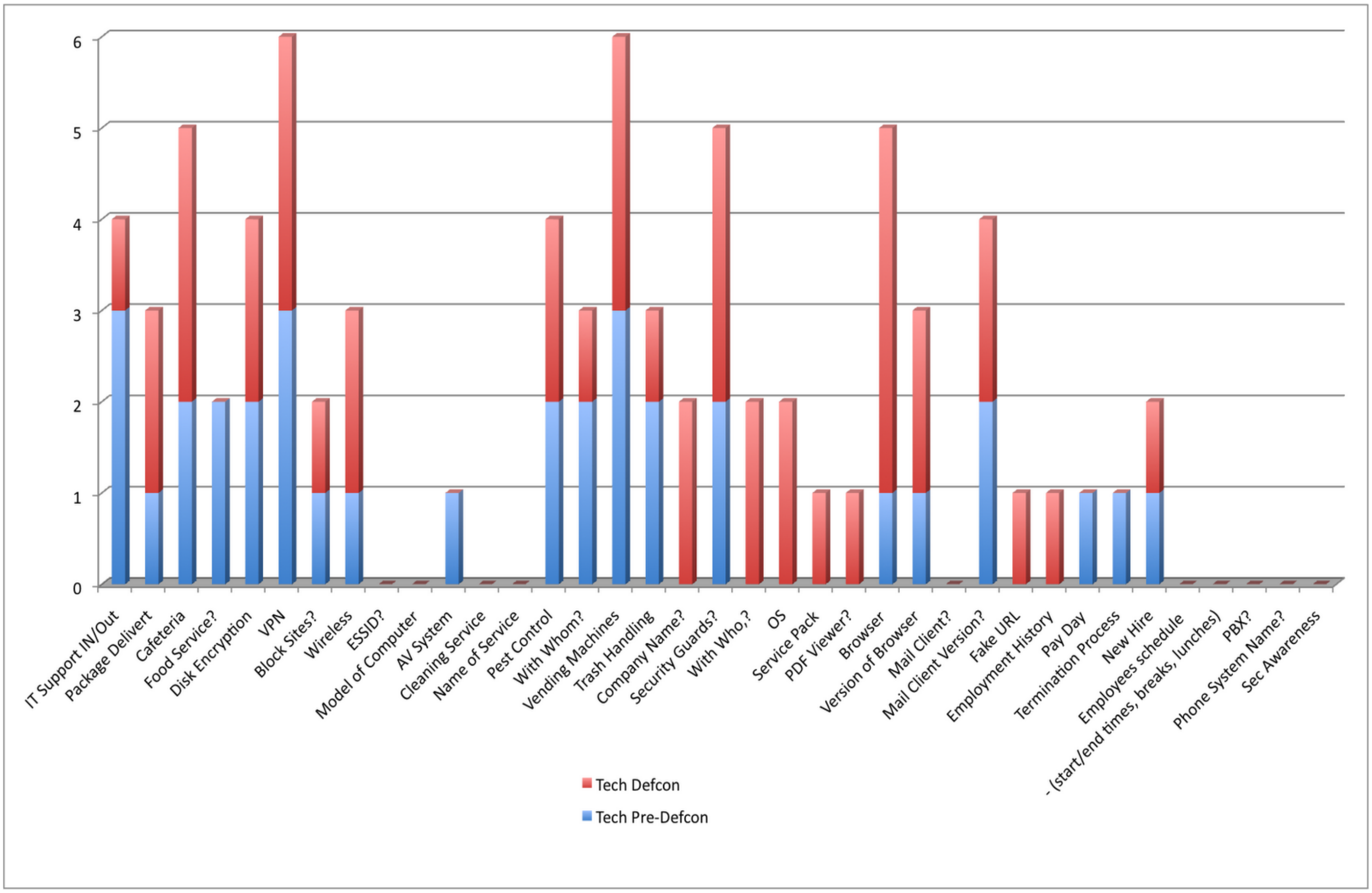
Oil & Gas


4
3.5
3
2.5
2
1.5
1
0.5
0
IT Support IN/Out
Package Delivert
Cafeteria
Food Service?
Disk Encryption
VPN
Block Sites?
Wireless
ESSID?
Model of Computer
AV System
Cleaning Service
Name of Service
Pest Control
With Whom?
Vending Machines
Trash Handling
Company Name?
Security Guards?
With Who,?
OS
Service Pack
PDF Viewer?
Browser
Version of Browser
Mail Client?
Mail Client Version?
Fake URL
Employment History
Pay Day
Termination Process
New Hire
Employees schedule
- (start/end times, breaks, lunches)
PBX?
Phone System Name?
Sec Awareness
Oil/Gas Defcon
Oil/Gas Pre-Defcon

Retail


7
6
5
4
3
2
1
0
IT Support IN/Out
Package Delivert
Cafeteria
Food Service?
Disk Encryption
VPN
Block Sites?
Wireless
ESSID?
Model of Computer
AV System
Cleaning Service
Name of Service
Pest Control
With Whom?
Vending Machines
Trash Handling
Company Name?
Security Guards?
With Who,?
OS
Service Pack
PDF Viewer?
Browser
Version of Browser
Mail Client?
Mail Client Version?
Fake URL
Employment History
Pay Day
Termination Process
New Hire
Employees schedule
- (start/end times, breaks, lunches)
PBX?
Phone System Name?
Sec Awareness
Retail Defcon
Retail Pre-Defcon

Tech

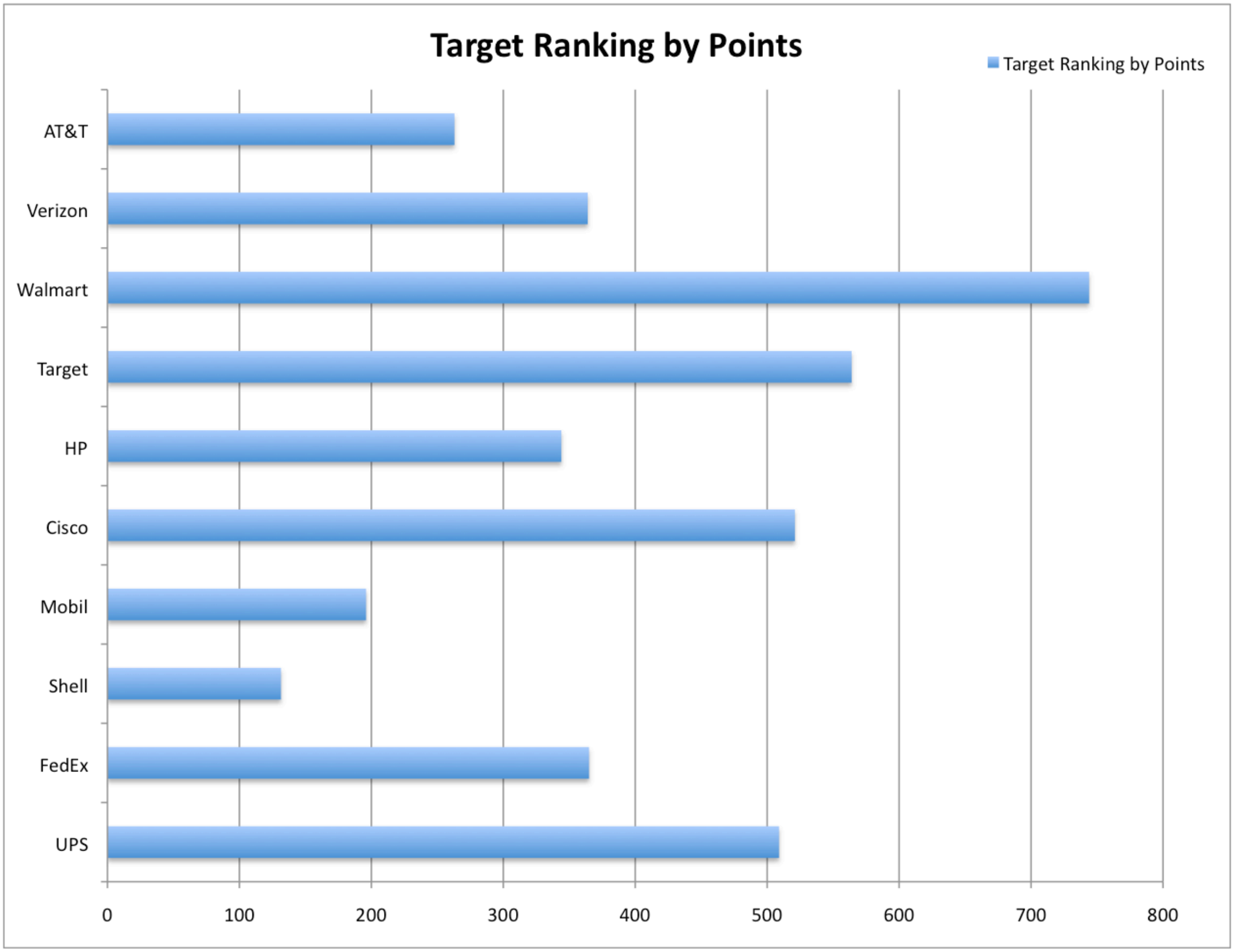

6
5
4
3
2
1
0
IT Support IN/Out
Package Delivert
Cafeteria
Food Service?
Disk Encryption
VPN
Block Sites?
Wireless
ESSID?
Model of Computer
AV System
Cleaning Service
Name of Service
Pest Control
With Whom?
Vending Machines
Trash Handling
Company Name?
Security Guards?
With Who,?
OS
Service Pack
PDF Viewer?
Browser
Version of Browser
Mail Client?
Mail Client Version?
Fake URL
Employment History
Pay Day
Termination Process
New Hire
Employees schedule
- (start/end times, breaks, lunches)
PBX?
Phone System Name?
Sec Awareness
Tech Defcon
Tech Pre-Defcon

Last year, AT&T gave the most resistance of any company targeted. This year, they did well again showing a fair amount of resistance. In fact, during one of the calls that we thought was going to go very well for the caller, as soon as extraction of sensitive information was attempted, the employee immediately became suspicious and refused to give any further information. What is one contributing factor to this? We know that AT&T provides monthly awareness training for it's employees and it shows.

The company that offered the most resistance was Shell. The pre-Defcon information gathering and the actual phone calls did not give enough insight to know why, but it seems the employees are well trained to detect and avoid these types of attacks.

Unlike previous years, where retail seemed to have a wall around their defenses, they gave up the most information, both during the information gathering and during the call phases of the contest.

The chart below ranks each target based on the total points collected against the target, both in the information gathering stage and the call stage; **the higher the score, the worse a company did**.


Target Ranking by Points
Target Ranking by Points
AT&T
Verizon
Walmart
Target
HP
Cisco
Mobil
Shell
FedEx
UPS
0
100
200
300
400
500
600
700
800

Defense

Sadly, even after all the exposure of last year's Social Engineering Capture the Flag contest, not much seemed to change. Although some companies showed resistance this year and some employees hung up or refused to answer questions, total resistance was never seen. In a real social engineering penetration test, or during a nefarious social engineering attack, this action could have been "game over" for the company's social engineering defenses.

Some companies showed resistance while on the phone; however, enough information was gathered using publicly available information that a realistic social engineering attack could have been launched with a high probability of success.

As a whole, when we did see defense, it primarily came in the form of confusion. The target either didn't know the answer or understand the question that was asked., A secondary form of defense we saw was the target not answering questions due to discomfort.

Mitigation

The purpose of the SECTF is to raise awareness to the threat that social engineering presents in America, and globally. The crux of this report is to inform companies of the dangers associated with nefarious social engineers as well as how companies can mitigate and protect against these attacks.

Without concerted mitigation effort on the part of companies, each year will see increases in the ability for unskilled and untrained people being able to collect amazing amount of data from unsuspecting targets.

Below are a few suggestions for potential mitigation of this threat.

1: Social Media Policies

The open source information-gathering piece of the contest revealed how much data target companies are releasing on the web. It is staggering.

Companies need to set clear definitions of what is allowed and what is not allowed with regard to the use of social media. If hobbies, vacations, and other parts of personal life are being discussed on these sites, business should not be mixed in. Guidelines, policies, and education can help the employees understand the risks associated with social media usage. In addition, clearly defined policies on how, where, and what kind of documents can be uploaded to unsecured areas of the Internet can go a long way to safeguarding companies.

2: Consistent, Real World Education

One of the areas that appear to be lacking across the board is quality, meaningful, security awareness education. There is a direct correlation between companies that provide frequent awareness training and the amount of information a company gives up. The more training, the less information is given.

Security awareness training needs to be consistent, frequent and personal. It doesn’t mean that a company needs to plan large events each month, but annual or biannual security reminders should be sent out to keep the topic fresh in the employees’ minds. There has been success at making it a “game” where employees compete to find, identify, and notify the proper channels in regards to social engineering attempts on the company. Security education really cannot be from a canned, pre-made solution. Education needs to be specific to each company and in many cases, even specific to each department within the company.

3: Regular Risk Assessment and Penetration Test

Still one of the most necessary aspects of security is the social engineering risk assessment and the social engineering penetration test. When we perform social engineering risk assessments, we identify all areas where a company is vulnerable to attack. Leaked information, social media accounts, and other parts of the company are identified, cataloged, and reported. Potential vectors are presented and mitigations are discussed.

A social engineering penetration test takes things to the next level; vectors are not just written about, but tried and executed. The results are used to develop awareness training and can truly enhance a company’s ability to be prepared for these types of attacks.

It is easy to see that if these companies had regular social engineering penetration tests, they would have seen these vectors. They would have been able to implement education and fixes to avoid these potential threats.

These are just three of the many strategies that can be utilized to help maintain security and prepare for the attacks being launched on companies every day. Our hope is that this report helps shed light on the threats presented by social engineering and opens the eyes of corporations to how vulnerable they really are. If you, or your organization, have any questions regarding any aspect of this report please contact us at: defcon@social-engineer.org

Conclusion

Many of you who have been following the contest and our report will recall how much fear mongering there was surrounding the competition. There was a distinct paradigm shift. Having CNN cover the competition and having the director of the NSA, General Alexander, meet us and congratulate us for the work we are doing helped to validate this contest.

Similar to last year, there were some industries and companies that stood out from the rest as being more secure than others. In the end, all of the companies would have received a failing mark in a real social engineering penetration test. While there are many conclusions that can be drawn from our results, the most important is: There is ample information floating out there that malicious social engineers can use to target the average company. This information can be put to use by even an inexperienced social engineer to bear devastating results. This is consistent across all tested industries, with professional organizations appearing to be the most vulnerable.

The barrier of entry for social engineering attacks is very low. Criminal enterprises are like any other business; return on investment is important. The investment required for social engineering attacks is far lower than other attacks, making them the most likely approach. Due to the lack of attention paid to this threat, there is no indication that this situation will change soon.

In light of this information, you would expect to see companies, especially Fortune 500/1000 companies, regularly conduct social engineering penetration tests and risk assessments.

Sadly, that is not the case. Why?

Many companies have the mentality of: "It won't happen to us" or "Our people won't fall for that". The sad truth is, those are the very people that will and do fall victim to these attacks, as demonstrated by the contest.

About Social-Engineer.org & Social-Engineer.Com

Our goal is simple, “Security through education”.

Social-Engineer.org and Social-Engineering.com have become the world authority on all things social engineering. Through our Contests, Framework, Toolkit, Newsletters, Blogs, Podcasts, Books, and intensive Social Engineering for Penetration Testers live course, we strive to educate companies and the community, as a whole, about the risks of social engineering. We dig deep into the social psychology to explain, scientifically, how and why social engineering works with such great success.

We will continue to bring you the highest possible quality content as we slide into 2013. Expect nothing less than the same research, interviews, and analysis you’ve come to expect from us.

We offer social engineering analysis, training, and penetration testing for companies that wish to protect their and their customer’s information.

We hope this contest continues to raise awareness about social engineering and the risks that social engineering poses to companies and individuals every day.

About the Authors:

Chris Hadnagy, aka loganWHD - Chief Human Hacker

- @humanhacker
- logan@social-engineer.org

Eric Maxwell, aka Urbal - Junior Human Hacker

- @urbal
- urbal@social-engineer.org

Social-Engineer.Com
Security Through Education

- ✓ The Webs First Social Engineering Framework
- ✓ SE Resources
- ✓ Free Monthly SE Newsletter
- ✓ Free Monthly SE Podcast
- ✓ SE Videos
- ✓ Social Engineering Tool Kit

And now a top ranking book, *"Social Engineering: The Art of Human Hacking"*
(Available in All Major BookStores)

www.Social-Engineer.Com

Now offering professional Social Engineering Services
Contact us today to learn more
info@social-engineer.com

Sponsors

The Social-Engineer.org CTF event was made possible through the support of the following organizations:

Professional
Social Engineering
Services and Training
SOCIAL-ENGINEER.COM

ELECTRONIC FRONTIER FOUNDATION