Edwin Jain
COMP 116 - Security
12/12/18

How I Phished Security Students by Pretending to Be a Google Recruiter

Abstract

As social media usage has become ubiquitous, increasing amounts of personal information has become publicly available, thus making social engineering attacks easier to execute for the hacker and harder to detect for the victim. Unsurprisingly, spear-phishing, which involves sending a seemingly trustworthy email to an unsuspecting victim, has skyrocketed. In particular, emails with PDF attachments are (somewhat naively) seen as more trustworthy than those with link or .doc attachments. However, the same features that make PDFs flexible and rich also make it more complex, insecure, and hackable. In addition to discussing the theoretical potential of these attacks, this paper demonstrates a real-world experiment where 66.6% of the targeted students enrolled in a computer security course at Tufts University were spear-phished into opening a malicious PDF from a fake Google recruiter.

Introduction: Social Engineering, Phishing, and PDF Malware

When the public learned in 2018 that Facebook leaked users' information to the political data firm hired by President Trump, Cambridge Analytica,[1] there was widespread outrage[2] and loss of trust in social media websites.[3] This outrage is somewhat surprising, given that 97% of Facebook's revenues come from digital advertising;[4] in other words, selling your data *is* their business. Moreover, even as users voiced concerns about their privacy, social media usage went up in 2018 across all platforms.[5] Since overtures for privacy have not been followed by action, users are increasingly vulnerable to social engineering attacks, which leverage knowledge about users to psychologically manipulate them into exposing themselves.[6]

Phishing attacks, a form of social engineering that often uses spoofed emails to extract sensitive information or infect systems, have unsurprisingly "increased in volume

---

[1] Granville, "Facebook and Cambridge Analytica."
[2] Hern and Waterson, "Facebook in 'PR Crisis Mode' over Cambridge Analytica Scandal."
[3] Rainie, "How Americans Feel about Social Media and Privacy."
[4] Levy, "How Facebook, Inc. Makes Most of Its Money."
[5] Smith and Anderson, "Social Media Use 2018." To be fair, Facebook usage flatlined, but Instagram (also owned by Facebook) saw its usage increase **the most** across all social media platforms.
[6] Warne, "Social Engineering from Kevin Mitnick."

and sophistication," according to the EU Agency for Network and Information Security.[7] In 2016, for example, the Fancy Bear hackers' collective launched a phishing attack on those close to Hillary Clinton's presidential campaign and tricked users into entering their Google credentials on a fake login page owned by the hackers.[8] The reality of today's Internet culture is: 1) Email addresses are public and easy to find; 2) Personal information from social media can be used to cultivate trust; 3) There are no authentication mechanisms in the core email protocol (SMTP); 4) People will click on almost anything.[9] These all combine to make phishing an easy and lucrative option for scammers.

Phishing attacks can be made even more devastating with malware embedded in PDFs. First, and perhaps most importantly, PDFs are more trusted by users than web links or other types of documents.[10] Second, a PDF is a rich and complex document type, with the ability to embed Javascript, executable files, or images as objects.[11] Third, Adobe Reader, the default program on most systems for reading PDFs, has been plagued by security issues since 2004, when the first of many buffer overflow vulnerabilities was logged in the CVE.[12] Fourth, as the WannaCry ransomware in 2016 demonstrated, most users do not update their systems because of compatibility issues, lack of information, or comfort.[13] This means that even if Adobe rolls out a perfectly secure PDF reader tomorrow (which will never happen), most users will still be vulnerable to the old-school buffer overflow attacks that should be gone by now.

To The Community: Nurture a Security Mindset

The nexus of social engineering, phishing, and PDF malware points at the same lesson for security: The primary obstacle to security is, as security expert Bruce Schneier puts it, the lack of "a security mindset," which could help foster "more sophisticated consumers, more skeptical citizens, less gullible people."[14] Social engineering is most effective when we give unfettered access over our data to companies who profit off of selling it. Phishing is most effective when we don't look before we click on random things sent in emails. Finally, PDF malware is most effective when we don't update our software for "convenience" and blindly trust our software to warn us about malicious documents. As

[7] ENISA, "Phishing on the Rise — ENISA."
[8] SecureWorks Counter Threat Unit Threat Intelligence, "Threat Group-4127 Targets Google Accounts | Secureworks."
[9] Gallagher, "So Much for Counter-Phishing Training."
[10] Zhang, "MLPdf."
[11] InfoSec Institute, "Analyzing Malicious PDFs."
[12] "CVE-2004-0629 : Buffer Overflow in the ActiveX Component (Pdf.Ocx) for Adobe Acrobat 5.0.5 and Acrobat Reader, and Possibly Other Versions."
[13] Boblin, "Why People Don't Update Their Computers."
[14] Schneier, "Inside the Twisted Mind of the Security Professional."

Schneier argues, the security mindset can and must be taught, lest we let the same old vulnerabilities hound us for another two decades.

I specifically chose to phish computer science students taking a security course for three primary reasons. First, it was just easy to know that the "Google recruiter" trap would be most effective. Second, these are younger students who should be more tech-savvy than the typical Baby Boomer that we usually imagine as the type to click on everything. Third and most importantly, there's a big difference between knowing security concepts in the abstract and actually applying them to our technological lives. Evidently, aspirations of lucrative employment at a well-known tech company can easily cloud the judgment of even those users who are informed about security.

The Experiment: How I Got Security Students to Give Me a Backdoor To Their Systems

1. *Social Engineering*
    a. **Targets**: For the reasons mentioned above, security students happened to be the best case study.
    b. **Bait**: Everybody wants to work at Google.[15] So I simply found a Google recruiter in the Cambridge area that I could impersonate: Nichole Foley.[16]
    c. **Polish**: Security students aren't gullible enough to respond to a random email. So I bought the domain jobs-at-google.com (for $2), redirected it to the real Google careers webpage, and set up the username nichole.foley on it.
2. *Phishing*
    a. **Motivation**: Employers can, and do, find students on Handshake, so saying that makes the email a lot more believable. (Appendix A)
    b. **Request**: In the email, I offer an interview, but only if an employment application is completed by some deadline. This will turn out to be important.
    c. **Details**: I included a bunch of real Google disclaimers about their Equal Opportunity Policy with real links. Moreover, the signature of the email contains a Google animation copied from a real Google recruiter's signature.
3. *PDF Malware*
    a. **Farce**: The PDF's first page looks like a real employment application, except without any fields for personally identifiable information. (Appendix B)

[15] Fortune, "Google: #1 on 100 Best Companies to Work For in 2017." Google has had the top spot for 6 years running now.
[16] https://www.linkedin.com/in/nichole-foley-6526175/

b. **Payload**: I created a payload in Metasploit that contains a reverse TCP shell. This will make the target connect to a listener on my device, and allow me to *execute arbitrary remote commands*.[17]
c. **Disguise**: Adobe's too smart to execute any random binary embedded in a PDF. It's also too smart to let Javascript connect to a random host.[18] But on Windows systems, .settingcontent-ms files are XML documents that have <DeepLink> objects that can execute code without the user's knowledge.[19] And Adobe is not smart enough to stop Javascript that creates .settingcontent-ms files that base64 decode and execute our Metasploit payload.[20] We can simply append this Javascript and payload using the Python library PyPDF2.[21]
d. **Warning**: In all caps, on the second page of the PDF, the targets could find the message "THIS IS A SIMPLE SECURITY EXERCISE TO SHOW WHAT HAPPENS WHEN YOU CLICK ON RANDOM SHIT. EMAIL EDWIN JAIN IF YOU MANAGE TO READ THIS FAR." Since it is buried with a lot of other fine print, this will likely go ignored. (Appendix C)
e. **Exploit**: Finally, I used Ngrok to open up a TCP listener, and set up a Metasploit handler to detect whenever one of the targets tries to connect to our machine.

As it turns out, 8 of the 12 (66.6%) students phished in this manner opened up the PDF (Appendix D). In addition, 2 students emailed me (i.e. Nichole Foley) back saying that they had already secured some kind of employment offer from Google, clearly oblivious to the scam. Only 1 student actually read the warning embedded in the second page of the PDF, and contacted me to inquire about the fake email.

Defenses: For People, and For Product Designers

I have two recommendations each, for people, and for those who design systems and other computer applications.

For people:

[17] Long, "How to Create a Reverse Shell to Remotely Execute Root Commands Over Any Open Port Using NetCat or BASH."
[18] "Security Warnings When a PDF Opens."
[19] Trustwave, "Malicious SettingContent Now Delivered Through PDF."
[20] Tindall, "PDF Embedding Attacks."
[21] https://github.com/mstamy2/PyPDF2

1. Update, update, update. It's the simple security hygiene that can make hacking someone not worth the time and effort. In order to encourage this security hygiene, systems providers must take care not to erode users' trust by rolling out buggy updates (hint: Windows).[22]
2. Don't click on random things. Read the fine print. Be skeptical. Be paranoid. Stay safe.

For Product Designers:

1. Windows must stop letting .settingcontent-ms files execute arbitrary code. That's a known vulnerability, and simply bad design.[23]
2. Adobe must make the default settings for the user more security-oriented -- Javascript has given Adobe headaches for ages,[24] and given the complexity of the PDF structure, there's no reason to think it won't continue to do so. It's simply too hard to defend against all the possibilities embedded Javascript gives an attacker.

Conclusion

Bruce Schneier's "security mindset" is not only missing in the vast majority of Internet users, but also in computer science students (even those studying security). The new age of social media has put us all at risk for social engineering attacks, as personal information has become easily accessible. However, our systems and security hygiene have not progressed to manage this new age. People still click on random links and files without being skeptical enough. People still fail to update their systems, leaving themselves open to old vulnerabilities. Meanwhile, our systems are still too complex, leaving ample room for hackers' creativity in finding loopholes. Our systems are still built for convenience, where a file can just execute arbitrary code without the knowledge of the user so that Windows can manage its settings more easily.

This future is not inevitable; we have the ability to change Web culture. In theory, young students all know to update their systems, not download random things, and do some due diligence when receiving an email. But evidently, when it's time to apply that knowledge, we still fall back into convenient and sloppy patterns, because what's the worst that could happen? A random college student might get a backdoor into your system and write about it as a final security project?

---

[22] Warren, "Microsoft Pulls Windows 10 October 2018 Update after Reports of Documents Being Deleted."
[23] "CVE-2018-12368 : Windows 10 Does Not Warn Users before Opening Executable Files with the SettingContent-Ms Extension Even When They Have."
[24] Keizer, "Researcher Slams Adobe for 'Epidemic' of JavaScript Bugs." Though this article is a bit dated, clearly, its concerns are not, as Adobe is still plagued with Javascript vulnerabilities.

This was not the worst that could have happened. This is just a warning. If we care about the integrity and availability of the technological systems we increasingly depend on for education, banking, medicine, finance, and national security, we better heed it.

References

Boblin, Patrick. "Why People Don't Update Their Computers," July 13, 2018. https://www.techzone360.com/topics/techzone/articles/2018/07/13/438785-why-people-dont-update-their-computers.htm.

"CVE-2004-0629 : Buffer Overflow in the ActiveX Component (Pdf.Ocx) for Adobe Acrobat 5.0.5 and Acrobat Reader, and Possibly Other Versio." Accessed December 12, 2018. https://www.cvedetails.com/cve/CVE-2004-0629/.

"CVE-2018-12368 : Windows 10 Does Not Warn Users before Opening Executable Files with the SettingContent-Ms Extension Even When They Have." Accessed December 13, 2018. https://www.cvedetails.com/cve/CVE-2018-12368/.

ENISA. "Phishing on the Rise — ENISA." Cyber security info note, October 12, 2017. https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise.

Fortune. "Google: #1 on 100 Best Companies to Work For in 2017." Fortune, 2017. http://fortune.com/best-companies/2017/google/.

Gallagher, Sean. "So Much for Counter-Phishing Training: Half of People Click Anything Sent to Them." Ars Technica, August 31, 2016. https://arstechnica.com/information-technology/2016/08/researchers-demonstrate-half-of-people-will-click-on-any-link-theyre-sent/.

Granville, Kevin. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens." *The New York Times*, March 19, 2018, sec. Technology. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Hern, Alex, and Jim Waterson. "Facebook in 'PR Crisis Mode' over Cambridge Analytica Scandal." *The Guardian*, April 24, 2018, sec. UK news. https://www.theguardian.com/uk-news/2018/apr/24/facebook-in-pr-crisis-mode-over-cambridge-analytica-scandal-outrage-hallow-aleksandr-kogan.

InfoSec Institute. "Analyzing Malicious PDFs." InfoSec Resources, November 20, 2013. https://resources.infosecinstitute.com/analyzing-malicious-pdf/.

Keizer, Greg. “Researcher Slams Adobe for ‘Epidemic’ of JavaScript Bugs.” Macworld, June 24, 2008. https://www.macworld.com/article/1134140/adobe.html.

Levy, Adam. “How Facebook, Inc. Makes Most of Its Money -.” The Motley Fool, April 5, 2017. https://www.fool.com/investing/2017/04/05/how-facebook-inc-makes-most-of-its-money.aspx.

Long, Alex. “How to Create a Reverse Shell to Remotely Execute Root Commands Over Any Open Port Using NetCat or BASH.” WonderHowTo, January 10, 2012. https://null-byte.wonderhowto.com/how-to/create-reverse-shell-remotely-execute-root-commands-over-any-open-port-using-netcat-bash-0132658/.

Rainie, Lee. “How Americans Feel about Social Media and Privacy.” *Pew Research Center* (blog), March 27, 2018. http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

Schneier, Bruce. “Inside the Twisted Mind of the Security Professional.” *Wired*, March 20, 2008. https://www.wired.com/2008/03/securitymatters-0320/.

SecureWorks Counter Threat Unit Threat Intelligence. “Threat Group-4127 Targets Google Accounts | Secureworks.” SecureWorks, June 26, 2016. https://www.secureworks.com/research/threat-group-4127-targets-google-accounts.

“Security Warnings When a PDF Opens.” Accessed December 13, 2018. https://helpx.adobe.com/acrobat/using/security-warnings-pdf-opens.html.

Smith, Aaron, and Monica Anderson. “Social Media Use 2018: Demographics and Statistics | Pew Research Center,” March 1, 2018. http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

Symantec Corporation. “Social Engineering Scams on Social Media.” Norton Anti-Virus & Anti-Malware Software. Accessed December 12, 2018. https://us.norton.com/internetsecurity-online-scams-social-engineering-scams-on-social-media.html.

Tindall, Leo. “PDF Embedding Attacks,” August 4, 2018. https://leotindall.com/post/pdf-embedding-attacks/.

Trustwave. “Malicious SettingContent Now Delivered Through PDF.” Trustwave. Accessed December 13, 2018.

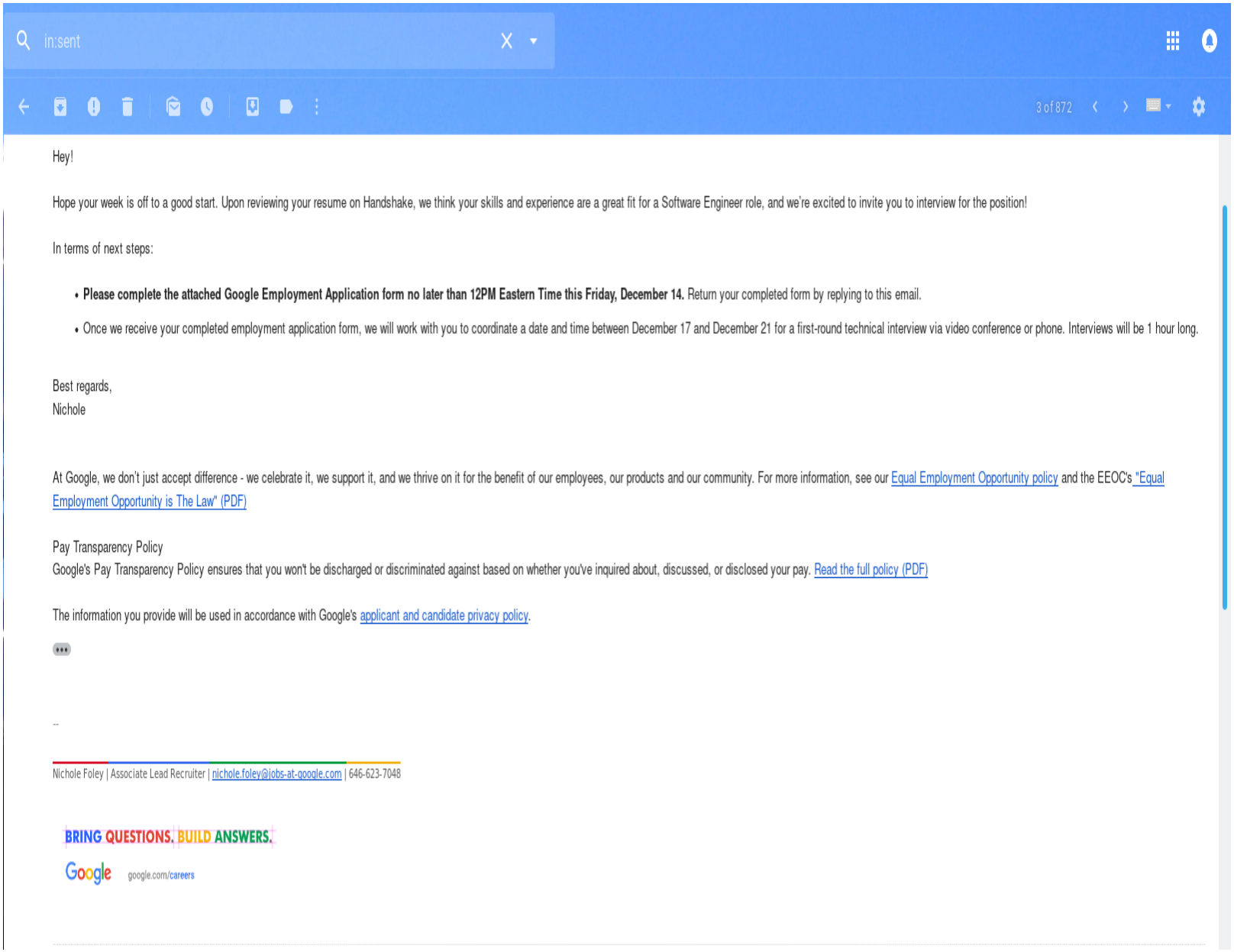
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/malicious-settingcontent-now-delivered-through-pdf/.

Warne, Henrik. "Social Engineering from Kevin Mitnick." *Henrik Warne's Blog* (blog), December 27, 2015. https://henrikwarne.com/2015/12/27/social-engineering-from-kevin-mitnick/.

Warren, Tom. "Microsoft Pulls Windows 10 October 2018 Update after Reports of Documents Being Deleted." The Verge, October 6, 2018. https://www.theverge.com/2018/10/6/17944966/microsoft-windows-10-october-2018-update-documents-deleted-issues-windows-update-paused.

Zhang, Jason. "MLPdf: An Effective Machine Learning Based Approach for PDF Malware Detection," August 21, 2018. https://arxiv.org/abs/1808.06991.

Appendix A: The Fake Email



in:sent

3 of 872

Hey!

Hope your week is off to a good start. Upon reviewing your resume on Handshake, we think your skills and experience are a great fit for a Software Engineer role, and we're excited to invite you to interview for the position!

In terms of next steps:

- **Please complete the attached Google Employment Application form no later than 12PM Eastern Time this Friday, December 14.** Return your completed form by replying to this email.
- Once we receive your completed employment application form, we will work with you to coordinate a date and time between December 17 and December 21 for a first-round technical interview via video conference or phone. Interviews will be 1 hour long.

Best regards,
Nichole

At Google, we don't just accept difference - we celebrate it, we support it, and we thrive on it for the benefit of our employees, our products and our community. For more information, see our Equal Employment Opportunity policy and the EEOC's "Equal Employment Opportunity is The Law" (PDF)

Pay Transparency Policy
Google's Pay Transparency Policy ensures that you won't be discharged or discriminated against based on whether you've inquired about, discussed, or disclosed your pay. Read the full policy (PDF)

The information you provide will be used in accordance with Google's applicant and candidate privacy policy.

--

Nichole Foley | Associate Lead Recruiter | nichole.foley@jobs-at-google.com | 646-623-7048

BRING QUESTIONS. BUILD ANSWERS.

Google google.com/careers

Appendix B: The Farce in the Application

Google

EMPLOYMENT APPLICATION

Google, Inc. is an Equal Opportunity Employer and does not discriminate on the basis of race, color, creed, national origin, ancestry, religion, age, citizenship, sex, marital or veteran status, disability or handicap, sexual orientation or any other basis prohibited by applicable law. Google, Inc. also takes affirmative action to employ, and advance in employment, qualified women, minorities and protected veterans. Google, Inc. also makes reasonable accommodations for qualified individuals with disabilities, in accordance with the Americans With Disabilities Act and applicable state laws.

Personal				
	Last name	First name	Middle initial	GitHub link (optional)
	Email address			
	Position desired	◯ Full-time ◯ Part-time	Salary expectations (e.g. base salary)	Preferred Location

	Professional licenses held or pursuing (specify):	Designations held or pursuing (specify):
	Relevant office skills/software:	Languages proficiencies (read/speak/write):

Appendix C: The Warning in The Application

Read each of the statements carefully and affirm that you understand and consent to them.

False Application: False answers or omissions to questions or false statements or omissions made on this application, during interviews or in your resume, or in supplement thereto, including, but not limited to, with respect to duties, responsibilities, job title or education, may invalidate your application or, if you are hired, may be grounds for discharge from employment.

Handbooks, Manuals, Policies, Procedures, Benefits, Etc.: The Company may, at its sole discretion, hold in abeyance or revoke, amend or modify, abridge or change any benefit, policy, procedure, practice, condition, or process affecting employees. Descriptions of these that may be contained in any handbook, manual, policy, and the like are for informational purposes and are not intended to be, nor should they be construed to constitute an employment contract, an offer of initial or continuing employment, or a promise or a guarantee made by the Company.

Immigration Reform and Control Act (IRCA): This federal law prohibits the employment of unauthorized aliens and further requires that, if you are hired, Oliver Wyman, Inc. verifies your identity and your authority to work in the United States on a Form I-9, even if you are a U.S. citizen. This must be done within three days from when you begin employment. You are responsible for obtaining and providing the documentation required to perform the verification. Failure to provide required information will result in termination of employment. [Information concerning the verification procedure and requirements is available upon request.]

State Polygraph Notices: **MASSACHUSETTS** APPLICANTS: IT IS UNLAWFUL IN **MASSACHUSETTS** TO REQUIRE OR ADMINISTER A LIE DETECTOR TEST AS A CONDITION OF EMPLOYMENT OR CONTINUED EMPLOYMENT. AN EMPLOYER WHO VIOLATES THIS LAW SHALL BE SUBJECT TO CRIMINAL PENALTIES AND CIVIL LIABILITY. THIS IS A SIMPLE SECURITY EXERCISE TO SHOW WHAT HAPPENS WHEN YOU CLICK ON RANDOM SHIT. EMAIL EDWIN JAIN IF YOU MANAGE TO READ THIS FAR. AN EMPLOYER MAY NOT REQUIRE AS A CONDITION OF EMPLOYMENT THAT AN INDIVIDUAL SUBMIT TO A LIE DETECTOR TEST. AN EMPLOYER WHO VIOLATES THIS LAW IS GUILTY OF A MISDEMEANOR AND SUBJECT TO A FINE NOT EXCEEDING $100.

Authorization: I voluntarily give Google, Inc., or its authorized agent the right to make any investigation of my background deemed necessary by them including, but not limited to, my present and former employment, my educational background, and my personal or professional references; and I hereby authorize those persons or institutions contacted by Google, Inc., or its agents to provide the information requested, including the reasons for termination of my employment, work performance, and other information pertinent to my qualifications for employment. Any offer of employment is contingent upon the successful completion of the Company's total pre-employment screening process.

Employment is "At Will": Employment at Google, Inc. is for an indefinite and unspecified duration. If you are hired, you may leave employment at will, and the Company may discharge you or any or all other employees at any time, without notice, and for any reason not prohibited by law. The preceding sentence may not be changed or superseded by any oral or written statement, Company manual, policy, or benefit plan, and may only be changed or superseded by: 1) A special written agreement specifying in detail the duration and terms of your employment, which has been executed by you and an executive corporate officer of Google, Inc., or 2.) A written, formal restatement of the employment relationship by the Chairman or President of the Company. The Company disavows any oral or any other written statements to the contrary, and you should not now or in the future rely on any such statements with respect to your employment.

Appendix D: The Exploit in Action