Teaching Case

Employing two factor authentication mechanisms: A Case Study

Cameron Lawrence
Cameron.Lawrence@business.umt.edu
School of Business Administration
The University of Montana

Eric Fulton
eric@subsectorsolutions.com
Subsector Solutions

Gerald Evans
Jerry.Evans@business.umt.edu

David Firth
David.Firth@business.umt.edu

School of Business Administration
The University of Montana

Abstract

This case study examines the life of a digital native who has her online accounts hacked, passwords reset, and is locked out of important online resources including her university email account and Facebook. Part one of the case study examines how the hack was perpetrated and the fallout of losing control of one's digital identity. Part two of the case study details how the main character recovered her accounts, simultaneously providing readers with the tools necessary to protect their own digital identities. Specifically, this case focuses on the use of two-step authentication schemes along with the generation, use and management of complex passwords. We then provide a set of discussion questions along with suggested lab activities that will show students how to implement the technologies discussed in the case. This case is intended to be used at both the undergraduate and graduate levels. This case complements the model curriculum objectives in IS 2010.1 and IS 2010.7.

Keywords: Information Security, Security, Privacy, Hacked, Two-Factor Authentication, Digital Native

1. Introduction

Kim West was born with newspapers in her blood. Her father was an acclaimed journalist who had authored a number of high-profile editorial pieces on government corruption, and Kim wanted nothing more than to follow in her father's footsteps. During her senior year in high school, Kim was admitted to a prestigious university with a top-five journalism program. As soon as Kim arrived on campus, she started working with the school paper. She began on the lowest rung of the paper's staff and started slowly working her way up. She received her big break during her junior year when she uncovered a story about how the student body president, Ryan Scott, had used student funds to pay for personal expenses and parties for his close friends. The article, along with subsequent stories, caused so much damage that the student senate impeached Ryan and forced him to resign after the winter break. Given the success of the story, West was hopeful she would win the coveted position as editor of the university newspaper, which would be announced at the end of the spring semester; however, there was no way for her to know that her breakthrough journalism work was about to lead to her digital life being turned upside-down.

2. The Take Down

Kim nestled into her favorite corner at the campus coffee shop to get some work done before her Advanced Reporting seminar. She had an hour to burn and wanted to put the finishing touches on an article for the school newspaper, which would be published the following day. As she had done hundreds of times during her college career, she powered up her Mac laptop seamlessly connecting to the coffee shop's wireless network, and logged into her university email account. This also gave her access to Google Docs, which she used to do all of her writing. A few years ago the university switched over to a service provided by Google that gave every student access to Google Apps, and she couldn't imagine how she worked without these tools. At that very moment, an anonymous student sitting in the same coffee shop was busy at work.

F4T4L (pronounced "fatal") occasionally hacked for money. His student loan debt was high while his interpersonal skills are low. The hacking world was a place where he can make extra money and get the support he hadn't found anywhere else. In hacking he found a community that accepted him and valued his skills. He tried to work a regular day job, but those didn't last very long; the low-level positions didn't pay nearly enough to support him while he was in college. People he knew occasionally approached him to "hack" someone they knew, but usually they couldn't afford the rates he charged. His services came at a high price because, if he was going to do something for which he might get caught, it was going to be worth his effort. It had been a while since anyone had approached F4T4L for his skills, which was why he was surprised when he received a message from the former student body president Ryan Scott. F4T4L had gotten to know Ryan in a freshman-level computer science class that all students were required to take. Ryan struggled with the class and came to rely on the quiet student, F4T4L, who sat next to him. It was clear to Ryan after a few weeks that this kid knew much more than the instructor and was a whiz with technology. Over the course of the semester, Ryan was surprised to learn that the quiet, low-key, computer whiz was proud to call himself a "hacker."

F4T4L had not seen Ryan much since class their freshman year. It didn't hurt his feelings that Ryan didn't keep in touch. F4T4L was used to making friends who needed his help, and once they didn't need help, disappeared from his life. Ryan never fully dropped F4T4L, but due to his popularity and involvement with student government, Ryan just didn't have time for many people in his life. Thus, F4T4L's curiosity was more than piqued when Ryan asked him to coffee seemingly out of the blue, prompting him to accept the invitation and meet Ryan the next day.

F4T4L didn't pay much attention to the politics on campus, but Ryan's impeachment was such a big story that it was almost impossible to be on campus and not hear about it. Ryan was not the forgiving type. Over the course of their conversation, F4T4L learned that Ryan wanted revenge on the reporter who had dealt a crushing blow to his life. He wanted F4TL to take down her email account, her Facebook account, and anything else F4T4L could access. Ryan wanted F4T4L to post embarrassing material to Kim's Facebook page. In addition, he was instructed to send offensive messages to all of her contacts after which he was to delete her saved messages and along with anything else he could get his hands on. Ryan wanted to humiliate Kim just as he had been embarrassed. They ultimately agreed on a price of $1,000.00, with $500.00 up-front and the last $500.00 after the job was done.

F4T4L went to work and was confident Kim would not know what hit her.

Kim went to the same coffee shop at a little after 2:00 PM every Tuesday and Thursday. As Ryan and F4T4L met on a Tuesday, F4T4L planned his attack for Thursday. He arrived 15 minutes before Kim and powered up a sticker-covered ThinkPad X1 Carbon, which was connected to an Alpha wireless card with a 10db antenna booster. After his laptop booted, F4T4L's fingers start to fly. There was no way for the coffee shop patrons to know a master was in their midst, quietly plying his craft. This thought always gave F4T4L a lot of personal satisfaction and was one of his favorite parts of hacking. He booted up a number of tools, like ARPSpoof, SSLSniff, and Ettercap. Each tool would play a part in the interception and decryption of Kim's password. Actually, every user of the coffee shop was being hacked, but he was only interested in one: Kim West, student reporter extraordinaire. Like clockwork, Kim entered the coffee shop and settled in to get some work done. He quickly identified her machine on the network and applied a filter that just displayed the traffic from her computer.

"That didn't take long," F4T4L mumbled to himself as he took a sip of coffee. A few seconds later "Bingo!" floated off of F4T4L's lips as he saw Kim's credentials fly by on his screen while he idly spun a pen in his right hand. He continued to watch, waiting, hoping to see more passwords appear on his screen. After an hour F4T4L saw Kim stand up to leave. "*Well, I guess my work is done*," thought F4T4L as he stopped intercepting the coffee shop's network traffic. At this point he was partially successful because he had only secured the credentials for Kim's email account. He did know, however, that there was a very good chance that Kim, like most users, daisy-chained her accounts and that the credentials used to login to her email account were probably the same as those used to login to other services such as Facebook. He opened a new tab in his web browser and browsed to Facebook. He then used the same email address and password he had collected earlier. A split second after he hit the enter key he was in. "I can't believe these people are so stupid..." F4T4L mumbled. Once he obtained the credentials and logged in successfully he knew the rest would be easy. F4T4L logged out of Facebook, closed his laptop bag, and stood, beginning the walk home with a smile on his face. Later that evening it took less than 20 minutes to accomplish what came next.

2. The Response

Every writer develops habits around writing; Kim is no exception. Early on she learned that she did her best writing early in the day and saved the evenings for editing her work. Following her usual evening ritual, Kim sat in her favorite chair and booted up her laptop as her best friend and roommate, Jenn Humphries, watched her latest obsession, *Downton Abbey*. At first Kim was annoyed since she couldn't login to her email account. Her fingers were cold, and she was trying to type too fast. She slowed down and typed her username and password carefully, annoyed at having to type so slowly. She pressed enter and saw a "Password or Username Incorrect" page. She tried typing her password in again, even slower this time. She received the same result, a "Password or Username Incorrect" page stared mockingly back at her. She knew she had typed the right password and was still denied. Panic started to set in. "*This has got to be a mistake*," thought Kim as she repeatedly tried to login to her account.

"No, no, no, no!" she cried frantically. From across the room she shouted, "Jenn, stop messing with me."

"I'm not doing anything Kim, can't you tell I am watching *Downton Abby*?" retorted Jenn.

"No seriously, if you aren't messing with me, I need help right now!" responded Kim in a nervous voice.

Jenn was always surprised that someone as smart as Kim didn't know anything about the technology she was so dependent upon. Jenn was majoring in Management Information Systems and was Kim's go-to tech person. Jenn had played little jokes on Kim in the past such as setting up the "Upside-Down-Ternet" on their network turning Jenn's Internet upside down, but Jenn knew she hadn't done anything recently. Moving over to Kim and her laptop, Jenn asked, "What's up?"

At about that time Kim's mobile phone lit up. She answered a call from an old friend from high school who told her that there was some wild stuff going up on her Facebook page and she wanted to make sure Kim was OK. Kim quickly assured her that she was fine, but it was clear that something terrible was going on.

Jenn quickly determined that Kim was being attacked. They went through the password reset

process on her university email account, but that didn't work as the backup email address had been changed. It was clear to Jenn that whoever was behind this attack knew what they were doing. Fortunately, Jenn worked part time on the university's help desk and knew the campus IT administrators. In fact, she played on the same ultimate Frisbee team as the lead administrator and had his mobile number. She called and explained the situation. He was able to remotely access Kim's account and clearly see there had been suspicious activity. They noticed a password change and a few other account configuration changes that happened almost simultaneously a few hours previously. In addition, they could see a mass email containing an offensive message was sent out to all of Kim's contacts, which included high ranking university officials. For Kim however, the worst was yet to come. After the message was sent, the attacker deleted all of her saved email messages, her entire address book, and all of her Google Drive documents. Effectively, her digital life was just deleted.

The IT admin could easily see that the account had been compromised. Fortunately for Kim the university had adopted the Google apps for education platform. This means Google hosts the university's email system and provides cloud-based productivity tools, ranging from word processing and spreadsheet applications to a private, cloud-based hard drive for every student on campus. The system had been successfully deployed two years ago and it changed how many students, faculty and staff work on campus. In addition to the email and productivity applications, the Google education platform also provides administrators with powerful tools to manage the technology, including the ability to recover data in the event an account has been compromised. He told Kim not to worry as they could recover her data and have it available in the next 30 minutes. Upon hearing this news Kim sighed in relief. Losing control of a Facebook account was bad, but losing all of her documents and emails was catastrophic. She was happy to have her documents back, although she was still frustrated at losing her Facebook. She silently added a mental note to buy a nice thank-you gift for the IT admin who saved her digital life.

The next challenge was to recover Kim's Facebook account. This was a little more difficult because they did not have a personal relationship with someone at Facebook to help recover the account. Visiting Facebook's help page, they realized account hacking is a fairly common problem on Facebook. Thankfully, Facebook has processes in place that enable legitimate account holders to recover their accounts in the event of profile hijacking. Jenn and Kim initiated the account-recovery process and by the next morning had regained control of Kim's account. It was easy for the Facebook staff to conclude the account had been compromised. First, there was the obvious clue of the inappropriate and obscene posts, but there were also other clues related to how the attacker accessed Facebook. The attacker had been very careful to cover his or her tracks so that security professionals could not track the perpetrator down. The attacker had used something called "Tor," a software add-on used to maintain anonymity online.

Kim was lucky. She had lost access to her accounts in the early evening and had recovered everything by the next morning. Over a late breakfast, Jenn and Kim pieced together what had happened the previous day. It was clear that Kim lost control of her university email and Facebook account at almost the same time. The last time she accessed her email account was at her favorite coffee shop, which must have been where it was stolen. She's had coffee there hundreds of times and written numerous newspaper articles in that coffee shop without having her accounts stolen. How and why did it happen this time?

Slowly, Jenn put it all together. There must have been someone in the coffee shop connected to the same Wi-Fi network who was monitoring Kim's network activity. Jenn had heard of students playing around with powerful Wi-Fi antennas and applications that intercept and monitor network traffic, but she had not heard of a specific student being targeted in such a vicious manner. When Jenn shared her hypothesis on what had happened, Kim didn't agree. Kim said she wasn't logged in to Facebook and was only briefly catching up on email while she was in the coffee shop.

"Let me guess," Jenn said, "you use the same password for all of your accounts, don't you?"

"Of course I do. Doesn't everyone? There is no way anyone can remember unique passwords for every site we log into," Kim responded.

"No, not everyone does!" said Jenn. "What you did is called "daisy-chaining", which means your various online accounts are linked together by a common email address and password. This

makes it MUCH easier for someone to hack into your account. I am going to help you configure your email and Facebook accounts so this will never happen again. The first thing we are going to do is set up two-step authentication on your accounts, then I am going to introduce you to an application called LastPass, which will help you manage all of your passwords. In under an hour we can make sure this will never happen again. The best news is these tools are free."

Kim looked at Jenn and said, "I am happy you know what you are doing because this is all kind of going over my head!" making a whoosh noise along with the hand-over-head gesture.

Jenn's first task for Kim was to set up two-step authentication on her email and Facebook accounts. "What in the world is two-step authentication?" asked Kim.

"It really is simple," Jenn replied. "I learned about this in my MIS security class last semester and set it up as soon as I could." Jenn continued, "Actually, I am surprised more people aren't using features like this. By default, when you login to your email or Facebook account you are using single-factor authentication, which is your password. Get it? It's only using one single thing to identify who you are. So if someone obtains your email address and figures out your password they can gain access to your account. Since most people use the same email address and password for all of their online accounts, this poses a serious security threat. When you implement two-factor authentication, the website requests two things from you to verify your identity. Usually this is something you know, like a password, and something you have, like a random number token or authentication application installed on your phone. When you activate the powerful two step-step feature built into our university email accounts, it almost eliminates any chance of your email account being hacked."

"I know it sounds a bit confusing, but it really is simple. Here, you can see for yourself. Let's watch this short video that Google put together that illustrates the concept" said Jenn as she played the video on her iPhone for Kim.

Link to Video:
http://www.youtube.com/watch?v=zMabEyrtPRg

After watching the video and spending 15 minutes getting two-step verification setup on Kim's email account, the two young women turned to securing Kim's Facebook account. Now that Kim was familiar with the two-step verification concept it didn't take any time to set up her Facebook account with the same level of protection. Facebook calls this level of security "Login approvals," and it works in almost the same manner as the two-step verification process that Google uses. Now Kim has Facebook's "Login Approvals" configured. When she logs in from a computer she hasn't used before with her Facebook account, she is required to enter not only her username and password but also a unique code that is sent to her cellphone via text message.

Once Kim had two-step activated for her Gmail and Facebook accounts, Jenn introduced her to the Google Authenticator application for her iPhone. Using the app Kim went through a short setup process with Gmail and Facebook. For both apps she used the Authenticator application to take a picture of a QR code. As soon as the phone snaps the QR code, it adds a random number generator for the application that changes every minute. Now when Kim wants to log into her account from a new computer, she has to type her password and the currently displayed random number. Thus, even if her password were stolen, the attacker would still not have the random number required to log into the account.

Kim had learned a lot in the past hour about her online security and was getting a little tired, but as long as Jenn was teaching, Kim was going to keep learning. "Next up is LastPass. It is a browser add-on that allows you to manage all of the passwords you use in your online life. LastPass not only manages your passwords, but even enters them for you!" explained Jenn.

"So LastPass just saves all of my passwords and logs in for me? Why not just remember four or five passwords?" asked Kim.
"Well," said Jenn, "it's a bit more complicated. When you sign up for new websites or change existing passwords, you can have LastPass create a complex password and remember it for you. For example, this is a password I just had LastPass generate: **7XacK9V4eWtvbzQV88Fc**. While two-step authentication is the best approach to security, not all sites have that capability. Ideally, all of the sites you login to should be protected by separate and individual passwords like the one I just generated. Since there is no way we can remember numerous complex passwords, we need a tool such as LastPass to do it for us. The

really good news is that even if someone hacks into a service you use frequently such as Twitter and steals your password, it won't be a big problem for you because that password is only used on Twitter and can't be used to login to any of your other accounts." Having satisfied most of Kim's questions, Jenn helped Kim install the LastPass application and configure it for use.

"That's about everything I can teach you right now," said Jenn. "There's a lot more you could do to increase your security, but without extra research they would sound like a bunch of random acronyms to you. VPN, YubiKey, Whole Disk Encryption, Tor, VMWare and BSD Virtual Machines, HTTPS Everywhere: these all don't make any sense to you, do they? asked Jen.

"Not really," replied Kim.

"Well, don't worry about it. The few steps we have taken in the last hour have increased your security beyond what the vast majority of technology users employ and, more importantly, you have the essentials down. If you want to learn more about some of the things I just listed off we can meet up later and I can show you," said Jenn with a smile. Jenn continued hurriedly, "But finals are just around the corner, and I need to get to the library to study," and then she headed out the door.

With her roommate gone and her online life recovered, Kim sat and reflected on how vulnerable she had been and how little she knew about basic areas of security. What is more surprising is that she had grown up with technology and been using it since her earliest days in school. It stunned her to think that no one had ever talked with her about the importance of securing her online life. On the other hand, what troubled her the most was a simple question that would never be definitely answered, "Why me?" There were at least forty other students in the same coffee shop and all early indications are that she was the only one that was attacked. "It just doesn't make any sense," she muttered. Then it slowly dawned on her as she thought of people who might have a vendetta against her. "Ryan Scott's impeachment didn't seem to sit well with him. And I know he's never forgiven me for my article. It MUST be...That rotten...!"

3. CONCLUSION

Kim's senior year was shaping up to be everything she had hoped. She was chosen as the editor for the university's paper, which almost guaranteed her a job with a major news organization after graduation. Her new position went into effect at the end of the spring semester. She had all summer to get ready for the fall semester and the publishing of the first edition under her leadership. She spent most of her summer learning about the operational details of running the paper. She also spent a lot of time talking with the paper's IT staff, which is something she never would have done prior to her hacking experience. In fact, she put into place a new set of policies for securing technology at the student-run paper. She insisted that two-step verification be turned on for all paper staff and asked the IT staff to put on a training session prior to the start of the fall semester on how to use LastPass. In the same predicament that she was once in, the vast majority of her friends on the paper had never heard of two-step verification or LastPass.

One of the perks of Kim's new position was the weekly editor's column that allowed her to sound off on a topic of her choice. She had spent a good part of the summer thinking about her first column and was thrilled when it appeared in print. It was titled "A Digital Native is Hacked: My Story." It began, "In the span of 24 hours my digital life was turned upside-down. This is the story of how I was hacked and I am telling it publicly so it doesn't happen to you."

4. Questions and Student Lab

1) What steps are you taking to protect your digital life? Could you fall victim to a similar attack?
2) If someone were to get access to your email address and password, how many different sites could they log into?
3) How many different sites do you log into regularly? Do you use the same login information for any of these sites?
4) Setup Google two-factor authentication
    4a) If you have a smartphone, install and configure the Google Authenticator App
5) Setup Facebook two-step verification
    5a) If you have a smartphone, configure the Facebook Code Generator
6) Create a LastPass account and generate secure passwords.
7) What is your email recovery password? Is it an email account you still use?
8) Is someone had access to your email, what other online services could they compromise through password resets?
Bonus:

1) Pick one of the services listed by Jenn and research how it could provide additional security: VPN, YubiKey, Whole Disk Encryption, Tor, VMWare and BSD Virtual Machines, HTTPS Everywhere, Bitcoin.
2) Create a walkthrough for your fellow students on how to implement a technology listed in question one.
3) Create an online tutorial demonstrating the technologies featured in the case.

5. REFERENCES

ARP spoofing. (2013, June 14). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=ARP_spoofing&oldid=558983438

Eder, S., & Valentino-DeVries, J. (n.d.). A Spy-Gear Arms Race Transforms Modern Divorce. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10000872396390443995604578002751421246848.html?mod=WSJ_WhatTheyKnowPrivacy_LeftTopNews

Farhi, P. (2013, June 14). CBS confirms reporter Sharyl Attkisson's computer breached. *Washington Post*. Retrieved from http://articles.washingtonpost.com/2013-06-14/lifestyle/39967790_1_cbs-news-computer-intruder

Fowler, G. A. (2012, October 13). When the Most Personal Secrets Get Outed on Facebook. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html

Green, T. (2013, June 15). CBS News Confirms Investigative Reporter Sharyl Attkisson's Computer Was Hacked. *International Business Times*. Retrieved from http://www.ibtimes.com/cbs-news-confirms-investigative-reporter-sharyl-attkissons-computer-was-hacked-1308429

Honan, M. (2012a, August 6). How Apple and Amazon Security Flaws Led to My Epic Hacking | Gadget Lab | Wired.com. *Wired Magazine*, (20.08). Retrieved from http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

Honan, M. (2012b, August 6). How I Got My Digital Life Back Again After An Epic Hacking | Gadget Lab | Wired.com. *Wired Magazine*. Retrieved from http://www.wired.com/gadgetlab/2012/08/mat-honan-data-recovery/

Johnson, D. (2013, June 7). Turn on 2-step verification to enhance security. *CBS News*. Retrieved from http://www.cbsnews.com/8301-505143_162-57587955/turn-on-2-step-verification-to-enhance-security/

Nicole Perlroth, & Bilton, N. (n.d.). Facebook Says Hackers Breached Its Computers. *New York Times*. Retrieved from http://bits.blogs.nytimes.com/2013/02/15/facebook-admits-it-was-hacked/

Perlroth, N. (2013, February 20). Some Victims of Online Hacking Edge Into the Light. *The New York Times*. Retrieved from http://www.nytimes.com/2013/02/21/technology/hacking-victims-edge-into-light.html

Reputation.com Reviews: Associated Press's Response to Getting Hacked. (n.d.). *Reputation.com*. Retrieved 7/5/2013 http://www.reputation.com/reputationwatch/reputationcom-reviews-associated-presss-response-getting-hacked

Segal, D. (2012, June 9). Hacked on Facebook and Seeking Help - the Haggler. *The New York Times*. Retrieved from http://www.nytimes.com/2012/06/10/your-money/hacked-on-facebook-and-seeking-help-the-haggler.html

Smith, H. A., & McKeen, J. (2011). The Identity Management Challenge. *Communications of the Association for Information Systems*, *28*(1). Retrieved from http://aisel.aisnet.org/cais/vol28/iss1/11

Zetter, K. (2013, January 1). New York Times Hacked Again, This Time Allegedly by Chinese | Threat Level | Wired.com. *Wired*, (21.01). Retrieved from http://www.wired.com/threatlevel/2013/01/new-york-times-hacked/

Editor's Note: *This paper was selected for inclusion in the journal as the ISECON 2013 Best Teaching Case*