

"Getting In Bed with Robin Sage."

By Thomas Ryan

Co-Founder & Managing Partner Provide Security, LLC.



www.providesecurity.com

Contents

Abstract	2
Creating the Persona	3
Analysis Details	4
Looking Ahead	6
References	7
Project Contributors	7

Abstract

Given the vast number of security breaches via the internet, The Robin Sage Experiment seeks to exploit the fundamental levels of information leakage—the outflow of information as a result of people's haphazard and unquestioned trust. The experiment was conducted by creating a blatantly false identity and enrolling on various social networking websites. By joining networks, registering on mailing lists, and listing false credentials, the conditions were then set to research people's decisions to trust and share information with the false identity. The main factors observed were: the ability to exploit other individuals' level of trust based on gender, occupation, education/credentials, and friends (connections).

By the end of this experiment, Robin finished the month having accumulated hundreds of connections through various social networking sites. Contacts included executives at government entities such as the NSA, DOD and Military Intelligence groups. Other friends came from Global 500 corporations. Throughout the experiment Robin was offered gifts, government and corporate jobs, and options to speak at a variety of security conferences.

Through this 28-day experiment, it became evident that the propagation of a false identity via social networking websites can be rampant and viral. Much of the information revealed to Robin Sage violated OPSEC and PERSEC procedures. The deliberate choice of an attractive young female appears to have exposed the role that sex and appearance plays in trust and people's eagerness to connect with someone. In conjunction with her look, Robin Sage's credentials listed on her profile resulted in selection perception; people's tendency to draw unwarranted conclusions in their attempt to make a quick decision. By acquiring a large number of connections, Robin had the ability to identify the individual who was positioned to provide the most intelligence based on their involvement in multiple government agencies. The false identity combined with carefully chosen false credentials led to a false trust that could have resulted in the breach of multiple security protocols.

Creating the Persona

The success of the Robin Sage Experiment relied heavily on the calculated creation of Robin's gender, occupation, education, credentials, and friends (connections). Determining the false identity's characteristics directly led to the wide variety of reasons people chose to connect. Moreover, as Robin's network grew, so did the potential gain for her new connections?

Gender

Choosing a young, attractive, and edgy female was a deliberate decision on the part of the Today, the vast majority of the creator. security industry is comprised of males. The heavily male dominated sector allows women to be a commodity in more ways than one. For example, just as women have proven to offer fresh new perspectives in the fields of marketing, journalism, and business, they are also able to assess security matters with a different outlook.

Some of Robin's male connections took a more assertive approach by offering her tickets to security conferences, complimenting and presenting available iob pictures, opportunities. Whether these same reactions would have been elicited towards another male is questionable. It can be put forth that Robin's appearance and gender played a key role in many people's comfort level. Furthermore, flirtatious gestures' regarding her picture reveals that her attractiveness led to the success of her propagation. One connection commented, "Greeeat pics," while another charmed her with, "You have to forgive me but I never forget a face (esp. one as pretty as yours)." These overt compliments develop the initial sense of trust that Robin established with her newly formed "friends."

Occupation

Robin Sage's present job was listed as "Cyber Threat Analyst" at Naval Network Warfare Command. This position suggested that she not only had seasoned expertise, but she also had passed the trusted background checks of the government. Many security professionals made these quick, yet inaccurate assumptions when considering Sage's occupation. This green light in terms of trust led her "friends" to offer further advancements in her career.

With no experience at all, Robin was asked to review papers written by professionals with over 10 years experience. For example, a fellow lecturer at the NASA Ames Research Center sought out Sage's knowledge and opinions pertaining to some of his papers and presentations. One professional introduces himself on LinkedIn with. "[am Senior Business а Development/Marketing/Sales Executive Consultant with 20 years+ in the Federal Government Homeland Security/Civilian/DoD Security Marketplace." While his introduction may suggest he is well acquainted with the security world, his fall for Robin Sage proved otherwise. Though he claims to have "expertise in the Cyber-Security [field]," he not only trusted Robin enough to connect with her, but he also privately messaged her with the hopes of a phone conversation to discuss her cyber intelligence background. Open requests such as these have the serious potential of opening a means of communication for private and/or information to be exchanged.

Education & Credentials

The power of one's network is only as strong as the people within it. Robin's first class education combined with her certifications proved her worthy of any security professional's web of connections. Because her experience demonstrated an expansive knowledge of the security field, the benefits of with Robin included connecting possible job opportunities, knowledge growth, and helpful contacts.

Throughout the experiment, various professionals approached Robin regarding job opportunities. Again, it can be surmised that these invitations were a result of her false education and credentials. The methodical creation of the identity's background played a pivotal role in the confidence people had in her actual existence.

Fellow alumni from her high school network, St. Paul's School, and her college network, Massachusetts Institute of Technology (MIT), chose to link to her on the basis of common educational ties. With no actual verification of her attendance, people entered into another level of trust based on no facts whatsoever.

"Friends", "Connections", and "Followers"

Robin Sage's friends served as her largest basis garnering trust from her targeted professionals. After acquiring just a few respected friends, Robin had what she needed to propagate the security field. The creator carefully chose security experts such as Jeremiah Grossman (Co-Founder and CTO of WhiteHat Security), Dan Kaminsky (Director of Penetration Testing at IOActive), and Marc Maffrett (Chief Security Architect at FireEye). By successfully fooling some of the most respected specialists in the security sector, Robin's credibility rapidly soared.

The success of a network is directly tied to the people and connections that one forms. Effectively targeting a person can be done in various indirect ways. For example, one connection messaged Robin, "I've never met you, but I saw you had Marty on your Facebook list, so that was good enough for me." This message encompasses the dangers of social networking when people fail to do their own research and instead, rely on other's judgment.

Analysis Details

A closer look at the creation of Robin's profile reveals that there were many opportunities for people to realize that this was a false identity. This section will first explore the oversights on behalf of the people that chose to connect to Robin Sage. It will then delve into the implications that develop when the initial trust is granted to a cyber predator.

Gender Implications

Drawing conclusions based on Robin Sage's appearance and gender is the initial mistake on the part of the target. Using advanced facial recognition software, the victim could have traced the profile picture to its origin-a pornographic website, and determined that the identity undoubtedly did not match. While getting your hands on software like this is not always so simple, there are other ways the target could have examined these pictures to conclude that the profile was counterfeit.

Robin Sage, on first glance, fit the profile of a young professional; fashionable in style, and flirtatious in personality. However, red flags should have been raised in assessing her number of pictures. Why would someone who appeared so social, have such few pictures? And, why would someone who touted their professional background on each social networking forum, use such unprofessional photographs?

It can certainly be argued that social networking websites stand as platforms for more relaxed professional networking. Robin's identity, had it been real, may have just posted her casual pictures because this type of connecting resembles nothing of a cocktail party. However, the profile viewer should have asked these questions and perhaps after assessing her other characteristics, he or she would have rendered a more accurate answer towards the question of her actual existence.

Occupation Implications

Careful attention to Robin's work experience and a few searches in Google, would have revealed that her occupational title does not This should have immediately even exist. raised skepticism on the part of the profile viewer. Moreover, her LinkedIn introduction speaks to her ten years of cyber security experience. However, this time frame would have put the young professional into the security field at the age of fifteen. Though there are anomalies of young teenagers mastering computer hacking skills at exceptionally young ages, the likelihood of these cases are small and incredibly rare.

As people sought Robin's professional advice, they placed themselves in an extremely vulnerable position. If the creator behind Robin had intentions other than to perform a social experiment, he would have had means to mislead experts in their studies and even steal their research. As noted in the previous section, the fellow lecturer at the NASA Ames Research Center offered to share his paper with Sage. Had his paper not yet been published, Robin would have gathered information and statistical data that she could have turned around and claimed to be her Furthermore, if Robin wanted to misguide the expert, she could have pointed the lecturer in an entirely different direction, and because he had already made the decision to trust her, he may have fallen prey to her tactics.

Professionals can also waste a considerable amount of their time pursuing false identities such as Robin's in order to fill positions. For example, Sage received messages from one job recruiter with the hopes of placing her in a Senior Research Analyst Position in Atlanta, Georgia. Not only did the recruiter spend time explaining the position, but she also requested Robin's resume for review. Opening up this

type of communication would allow someone to learn more about the company's goals, security, and salaries. Had Robin submitted a false resume and been offered a phone screening interview, the person behind the false identity would have had the opportunity to inquire more about the company. Though simple questions about a company may not initially appear threatening, the emergence of social engineering suggests otherwise. Pointed and carefully worded questions can often reveal far more information than what may appear on the surface. The only solution to avoiding these types of situations is to not befriend a false identity in the first place.

Education/Credentials Implications

Robin's education and credentials complimented her false occupation and helped grow her number of connections. Often times, peripheral information like this plays a critical role in developing trust. While a picture or an occupation may initially appear unconvincing, an identity's education and training background may all one need's to be swayed.

It is important to note that some security experts properly vetted Robin Sage's background. Perhaps by practicing these techniques, other professionals may avoid making the same mistake in the future. One security specialist, who goes by the name Simple Nomad, reached out to a friend who was an MIT alumnus. By asking a trusted friend to review his MIT alumni network, Simple Nomad was able to conclude that Robin Sage was neither an MIT alumnus, nor an actual person. University networks are significantly more reliable than networks such as LinkedIn, Facebook, and Twitter. Their alumni offices keep official records of current and previous students. By consulting a trusted friend and fact checking with a reliable network, Robin Sage's identity was proven false.

John Tierney, a security professional based out of New York, called Robin Sage's bluff by researching her NSA IAM (INFOSEC Assessment Methodology) credentials. By reviewing public information, Tierney managed to

deduce that the identity was false. Public information includes a rating program and provides a list of every individual that passed the NSA IAM courses. The absence of Robin Sage's name or any name similar to Sage's confirmed that she did not exist. More often than not, public information that is readily available is all that is needed to prove a false identity.

The risk in trusting qualifications to voluntarily seems obvious. Sage's multiple security credentials combined with her occupation would lead one to believe that she had TS/SCI (Top Secret/Sensitive Compartment Information) Clearance with Polygraph. People's trust in this identity could have very easily led to the sharing of information under the false premise that Robin Sage had expertise in the field.

Friends, "Connections," and Followers **Implications**

Many social networking websites have a section to show users who their mutual friends are with another person. LinkedIn uses numbers to show the degrees of separation between connections. These strategies encourage people to grow their network by establishing trust based on mutual friends. For example, though someone may not have known Robin Sage, their decision to link to them may have been based on the fact that five of their other respectable friends chose to do the same. As discussed in a previous example, one professional (Senior Attack Pattern Analyst for CAPEC at MITRE) accepted Robin's friendship request because his peer had done so.

Cyber predators are aware of this "mutual friends" oversight that social networking users frequently make. To exploit the weakness, lurkers pinpoint the person they are pursuing and indirectly track them. By connecting with a

number of the target's friends, the predator is building a line of trust with his target without the victim even knowing. Therefore, when it comes time to connect with the targeted individual, mutual friends stand as a comfort factor for the target. Because his or her friends trusted this false identity, it is more likely that the request to connect will be accepted.

To avoid being fooled by a fictitious individual on account of the "mutual friend" tactic, it is important to take a closer at the identity's profile. In the case of Robin Sage, users should have noticed that all of her friends/connections were formed in a very small time span. In the duration of one week, the identity formed a Twitter, LinkedIn, and Facebook and was rapidly making connections with people. Furthermore, mutual friends often sprout from a single common tie that two users have. However, if the mutual friends seem disconnected and unrelated, it is imperative that the user investigates further. The best-suited defense is to reach out to the mutual friends and ask about their relationship with the questioned identity. A simple inquiry regarding the profile may confirm or deny the individual's authenticity.

Looking Ahead

Before moving into the future, it is essential that appropriate lessons be derived from mistakes in the past. The Robin Sage experiment was created with the intentions of bringing awareness to the risks that social networking can pose when proper vetting is not performed.

In the past, Facebook required users to provide emails that verified their attendance to universities and institutions. However, since Facebook opened its gates to the greater public on September 26, 2006, it drastically increased the ways in which predators can create false identities. In the future, it is imperative that social networking sites explore sounder and more effective ways to prohibit the creation of fictitious profiles. As these websites continue to grow, they must take responsibility for the safety of their millions of users. While Facebook, LinkedIn, and Twitter may impose better inspection practices, the only person who can entirely insure their own safety is you.

This paper has adequately outlined various ways to properly examine profiles prior to accepting connection requests. Careful reviews of small details such as pictures, work experience, and credentials may provide just enough insight to refrain from linking to harmful individuals. Take the extra time to consult mutual friends or quickly perform your own research through the use of any common search engine. More often than not, false identities, just like Robin Sage, intentionally and unintentionally, leave simple clues for you along the way.

References

Perez, Richard, and Timm, Carl . Seven Deadliest Social Network Attacks. Syngress, May 2010.

Brenner, Bill. "Seven Deadly Sins of Social Networking Security". CSO Online. June 30, 2009

(http://www.csoonline.com/article/496314/seven -deadly-sins-of-social-networking-security).

Schneier, Bruce. "CIA Invests in Social-Network Datamining". Schneier on Security. October 26, 2009

(http://www.schneier.com/blog/archives/2009/1 0/cia invests in.html).

Nathan Hamiel, Shawn Moyer. "Fail 2.0: Further Musings on Attacking Social Networks". Shmoocon. February, 2009 (http://www.shmoocon.org/2009/presentations-all.html).

Strano, M. M. . "User descriptions and interpretations of self-presentation through Facebook profile images". Cyberpsychology: Journal of Psychosocial Research on Cyberspace. http://www.cyberpsychology.eu/view.php?cisloclan ku=2008110402&article=(search%20in%20Issues) . February 20, 2009.

Lenhart, Amanda . "Adults and Social Network Websites by Amanda Lenhart". PEW Internet and American Life Project, January 14, 2009 (http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx)

Project Contributors

Authors: Thomas Ryan & Gabriella Mauch

<u>Contributors:</u> Guy Fawkes, Pete Herzog, Omachonu Ogali, Jon Miller, Simple Nomad, Timothy "Thor" Mullen, John Tierney, Jacqueline Singh, Chris Nickerson, Tom Brennan, Dr. Kevin Schatzle PROVIDE SECURITY® CONSULTANTS ARE HANDPICKED BASED UPON THEIR EXTENSIVE TRAINING AND VAST HANDS-ON EXPERIENCE IN CYBER SECURITY, PHYSICAL SECURITY, EXECUTIVE PROTECTION AND INVESTIGATIONS. OUR PROFESSIONALS ARE UNIQUELY SKILLED AND WELL VERSED IN THE LATEST CONCEPTS OF CONVERGENCE IN THE SECURITY FIELD.





www.blackhat.com

Provide Security | Getting In Bed With Robin Sage

BlackHat USA | 8