Social Cybersecurity and the Help Desk: New Ideas for IT Professionals to Foster Secure Workgroup Behaviors

Cori Faklaris

Human-Computer Interaction Institute, School of Computer Science, Carnegie Mellon University
5000 Forbes Ave., Pittsburgh, PA 15213, USA
cfaklaris@cs.cmu.edu

ABSTRACT

Among the underappreciated roles of information technology professionals is that of "sales and marketing" for end-user security compliance. In this workshop paper, I offer ideas drawn from social psychology for communication strategies and micro-interventions that could help specialists in end-user support as well as information security analysts and computer and information systems managers to improve compliance with mandated security tools and best practices. I briefly describe our team's work to develop playful security interventions that leverage social factors and to document and analyze workgroup resource sharing through questionnaires on Amazon Mechanical Turk and interviews with local IT professionals. We hope our work can help identify and lead to effective methods to address pain points in end-user security support.

1. INTRODUCTION

The more than 800,000 computer support specialists in the U.S. [11] have a deceptively simple job: to provide help and advice to end users and their organizations. In practice, this means they must make use of technical skills in troubleshooting information technologies such as devices and user accounts; critical judgment and decision-making in how to escalate tickets and transfer calls; elicitation techniques such as open-ended questions to effectively draw out details of computing problems from their clients; and other so-called "soft" or "baseline" skills [9,10] to better connect with their user base. Such skills are needed also by the 100,000 information security analysts [12] and more than 350,000 computer and information systems managers [13] who develop standards and strategies that support specialists will help to carry out. Their security challenges have worsened as boundaries blur between personal and work use of technologies, lessening the ability of an IT staff to directly control the system environment; and employment becomes more collaborative and ad-hoc, making it more difficult to directly manage users – who have been long considered the weakest link in any security scheme.

Against this backdrop, I believe my research team's work could help improve the effectiveness of security compliance "sales and marketing" for front-line IT professionals as well as the analysts and managers around them. Specifically, we have been analyzing and testing how to apply Cialdini's *Social Influence Theory* [1] to improve end users' awareness, motivation and knowledge of cybersecurity tools and best practices. Previous work has found that social factors were responsible for many reported changes in security behaviors, such as using a smartphone PIN or enabling a Facebook security feature [3–5]. We now are extending this research to a workplace context.

My contributions in this paper are the following:

- An overview of Cialdini's "Weapons of Influence," commonly used by sales and marketing professionals to influence consumer behavior as well as in social engineering attacks such as spearphishing;
- Ideas for how IT professionals can turn these "weapons" to good use by fostering secure workgroup behaviors using social influence techniques;
- A summary of our work to develop playful end-user interventions and to collect data on how workgroups share accounts and devices, some of which are not owned or managed by their employers, with the ultimate goal of creating new security tools and techniques for these contexts.

2. SOCIAL INFLUENCE THEORY

Much cybersecurity research has focused on users as isolated actors. By contrast, our Social Cybersecurity research group has investigated how to leverage findings in social psychology to encourage safer cybersecurity behaviors. In this view, individuals' information processing and decision making about technology [8] is partly driven by their relationships with others and their need to accurately gauge their situation or context and present a consistent self-concept to themselves and others [2].

Cialdini's *Social Influence Theory* is among the most prominent theories of how people are persuaded to change their behaviors. Using techniques of interviewing and participant observation among "compliance professionals" such as door-to-door salespeople, Cialdini found evidence for six categories of persuasion techniques he termed "Weapons of Influence" [1] for their potency and chance of success. These are (1) *reciprocity*, our seemingly hardwired desire to repay in kind what someone else does for us and to share resources in a network of obligation; (2) *commitment and consistency*, our drive to live up to a commitment once we have made a choice or taken a stand publicly; (3) *social proof*, our tendency to see a behavior as correct in a given situation to the degree that we can observe others performing it; (4) *liking*, our basic drive to cooperate and comply with those we share personal affinities with; (5) *authority*, our instinct (varying by culture) to obey people who are presented as authority figures or

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018. August 12 -- 14, 2018, Baltimore, MD, USA.

experts; and (6) *scarcity,* our greater desire for those resources to which we perceive our access being limited.

These concepts from Cialdini's work and those of others studying social influence show up frequently in sales and marketing campaigns, such as when charities ask for a small donation after a "big ask" of a large amount or time commitment (*reciprocity*) and make donors' names publicly available (*social proof)*, then repeat their donor solicitation (*commitment and consistency*). Cialdini and collaborators demonstrated that these "Weapons of Influence" can be used to design and experimentally validate interventions to spur behavior change. One notable research study showed that placing cards in hotel rooms to notify guests that the previous room occupants had reused towels, rather than have the staff change them out, led to greater towel reuse by the new guests [6].

Das et al. found support for the application of social influence theory to problems in usable privacy and security [5], notably in a large-scale study of Facebook's implementation of the "social proof" concept for the Trusted Contacts user authentication feature [4]. We now are turning our focus to the workplace as a context in which social factors can be leveraged to spur the adoption of security tools and best practices.

3. SOCIAL INFLUENCE APPLICATIONS

Those who work with computer and information systems have long known that technology is usually only a means to an end for their clients to accomplish their goals. Helping to maintain good cybersecurity practices is a secondary motivation of their user base, at best. IT professionals' challenges have worsened in the "Bring Your Own Device" era, also known as "Bring Your Own Technology," in which they may need to help troubleshoot and head off problems with the connection to the enterprise network of employees' personal devices such as smartphones and third-party computing accounts, such as Gmail and Facebook. Employees may frequently switch projects or work teams and collaborate often with short-term contractors or freelancers. They also may need to share devices such as an on-call pager or tower workstation or accounts such as a customer email inbox, company website or branded social media accounts, which complicates the one-user-one-account model of user authentication, authorization and resource management.

Because end users may be the only humans in the loop who truly are aware of all the devices and accounts being used to get their jobs done, IT professionals are in more need than ever of new ways to motivate these users to help keep the network secure. The following ideas are a jumping-off point for discussion of how social influence techniques can be adapted for IT professionals to nudge voluntary compliance among employees and contractors with mandated security tools and practices. Some ideas could be directly implemented by the Help Desk, but many may require the approval or the involvement of the security analysts and managers who plan and direct their work.

3.1 Reciprocity

Cialdini's *reciprocity* principle recognizes our desire to repay in kind what someone else does for us and our seeming hardwiring to share resources in a network of obligation.

One method to invoke this principle is to give a gift that subtly obliges its use. One such "gift" might be a company-branded USB drive, which would encourage its use vs. employee-provided drives that might be help spread malware to the enterprise network. The drive could also include a package of approved apps or software for users to run on their personal computers for work use. Another "gift" idea to invoke the reciprocity principle is a thank-you card to end users for helping to keep the system free of viruses, malware and data breaches – obliging the recipients to keep up this good work.

Another method for applying reciprocity involves how to frame a request for a user concession to security protocols. Rather than present the request outright, Cialdini's work suggests first making a "big ask" of a more extreme version of the request that the user is likely to object to. The user will be more likely to agree to the more modest request (which is the real goal) either out of a feeling that they should reciprocate a concession or that they have scored a "win" by not being held to the initial request.

3.2 Commitment and Consistency

Under the *commitment and consistency* principle, once people make a choice and take a stand, they feel pressure to live up to that commitment.

One simple way to invoke this principle would be to ask system users to "please watch out for" mistakes in security protocol, such as leaving passwords exposed to public view. If they politely agree to this request, they now may feel internal pressure to, indeed, keep a watchful eye for mistakes among their coworkers that could lead to a security breach.

Another idea is to ask users to make a list of -- and sign their names to -- the security practices and tools that they intend to take advantage of in the next three months. These might be most effective if the user is first primed in a training session with an overview of desired practices and tools that they are unlikely to think of on their own, such as creating different passwords for each account and downloading and installing updates within one hour of being notified of its availability.

3.3 Social Proof

The *social proof* principle says that we view a behavior as correct in a given situation to the degree that we can observe others performing it.

The key to this principle is making security behaviors observable by others [5]. Our team is investigating whether statistics about the relative uptake of security practices by workgroup members (such as the relative strength of everyone's chosen passwords or frequency of accepting software updates) can be displayed to users via a web browser plugin or use of spare display real estate such as a lock screen.

A nontechnical way of leveraging this principle could be to "crowdsource" the work group's best security tips and then publicize these and the contributor credits via a newsletter, public meeting or group email as the social catalyst for driving use of the security tips.

3.4 Liking

Cialdini's *liking* principle recognizes the degree to which our personal affinities are bound up in cooperation and compliance – and vice versa.

One way to leverage this principle along with social proof would be to set a group goal and reward for improving the use of security tools and best practices, such as gift cards for 100% team use of an approved password manager.

Another way to apply this principle is to recruit a popular member of the workgroup as a helper and ally for the IT department. Similar to a system "super user," this worker would receive training and encouragement to model the desired security behaviors while helping to implement security protocols and generally lightening the support load for the specialists.

3.5 Authority

The *authority* principle recognizes our instinct, varying by culture, to obey people who are presented to us as authority figures or experts.

One way to apply this principle to encourage better adoption of security tools and practices is to cite security experts or academic research to back up claims of why a certain policy or protocol is being required. It may be sufficient, too, to cite the IT department's own research into why a certain antivirus package or authentication scheme was decided upon, because the IT staff themselves might be seen as relevant authorities.

Conversely, it can pay large dividends to train end users to avoid being tricked by social engineering tactics that also invoke the authority principle. It is a best security practice to educate users to question out-of-the-blue emails or social media messages that ask for their network credentials or for the user to install, modify or remove software or computing devices. Users should also know to watch out for and question strangers dressed similarly to IT staff, because they may actually on the premises to steal computers, passwords or intellectual property.

3.6 Scarcity

The final principle, *scarcity,* refers to the phenomenon that limiting access to a resource makes it more desirable.

One aspect of scarcity is that people are more likely to fixate on losses rather than gains [7]. This suggests it is better to frame conversations about security tools and best practices according to what end users might *lose* if secure behaviors are not employed ("70% of employees who didn't enable two-factor authentication had their passwords hacked"), instead of how they will *benefit* from such behaviors ("70% of employees with two-factor authentication enabled reported no security issues").

Another aspect of scarcity that Cialdini remarked upon [1] is that when a resource is first freely accessible and then limited, it becomes even *more* desirable than if the access was limited to begin with. The implication of this is that IT departments should strive to consistently apply and enforce security protocols and policies. Erratic enforcement or granting of exceptions may, counterintuitively, inspire rebellions among end users who become attached to the periods of relative freedom of choice.

4. WORKS IN PROGRESS

Our research team is working on several mini-games and everyday interventions that utilize the above social influence concepts. One idea, as noted above, is to create web browser plug-ins and screen displays that can help make team members' security practices visible to each other by providing statistics or even a leaderboard of how well individual team members are complying with security best practices, such as creating strong passwords and installing needed software updates. Another design being implemented is for a mobile game app that would foster social competition, likely through simulations of how players' in-game "workgroup" scores against others, while teaching a rubric for how to distinguish notifications of legitimate software updates from likely hoaxes or attacks. Such playful interventions could be deployed in an enterprise network as well as in homes or other consumer contexts to help end users consider the impact of security practices on their social ties.

We have now turned our attention to the workplace as a specific social context for usable privacy and security. An initial questionnaire of workers on Amazon Mechanical Turk has given us some insights into the difficulties people encounter when sharing work accounts and devices, such as losing track of account passwords after employees leave a business. We are planning an interview study with local IT professionals to get a more in-depth picture of why and how issues and challenges arise in workplace resource sharing. Through collection and analysis of this data and consideration of the above suggestions for adapting social influence techniques, we hope to develop effective interventions to improve IT support and workgroup social cybersecurity.

5. CONCLUSION

Prior work has shown the usefulness of applying Cialdini's *Social Influence Theory* [1] to improve end users' awareness, motivation and knowledge of cybersecurity tools and best practices. In this paper, I have provided an overview of Cialdini's six "Weapons of Influence": *reciprocity*, *commitment and consistency*, *social proof, liking*, *authority*, and *scarcity.* I then provided ideas for how to adapt these "weapons" to help IT professionals to encourage their clients' voluntary compliance with security tools and best practices. I concluded with a summary of our research group's work in progress to extend our prior findings in the social factors of cybersecurity to mini-games and everyday interventions and to collect and analyze data about workplace sharing behaviors. We hope our work can help identify and lead to effective interventions for pain points in end-user security for IT support specialists in the current era.

6. ACKNOWLEDGMENTS

My thanks go to my advisors, Laura Dabbish and Jason Hong, of the Human-Computer Interaction Institute, and to CMU visiting student Yunpeng Song, with whom I am collaborating on this research. My work is supported by the National Science Foundation under award no. SaTC-1704087.

7. REFERENCES

[1] Robert B. Cialdini. 2001. *Influence: science and practice* (4th ed ed.). Allyn and Bacon, Boston, MA.

[2] Robert B. Cialdini and Noah J. Goldstein. 2004. Social Influence: Compliance and Conformity. *Annu. Rev. Psychol.* 55, 1 (January 2004), 591–621. DOI:https://doi.org/10.1146/annurev.psych.55.090902.142015

[3] Sauvik Das. 2017. Social Cybersecurity: Reshaping Security Through An Empirical Understanding of Human Social Behavior. *Dissertations* (May 2017). Retrieved from http://repository.cmu.edu/dissertations/982

[4] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (CCS '14), 739–749. DOI:https://doi.org/10.1145/2660267.2660271

[5] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1416–1426. DOI:https://doi.org/10.1145/2675133.2675225

[6] Noah J. Goldstein, Robert B. Cialdini, and Vladas Griskevicius. 2008. A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels. *J. Consum. Res.* 35, 3 (October 2008), 472–482. DOI:https://doi.org/10.1086/586910

[7] Daniel Kahneman and Amos Tversky. 2000. *Choices, Values, and Frames*. Cambridge University Press.

[8] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *Manag. Inf. Syst. Q.* 27, 3 (2003), 5.

[9] 2015. *The Human Factor: The Hard Time Employers Have Finding Soft Skills*. Burning Glass Technologies. Retrieved June 19, 2018 from https://www.burning-glass.com/wp-content/uploads/Human_Factor_Baseline_Skills_FINAL.pdf. Last accessed June 19, 2018.

[10] 2016. 10 Soft Skills Every IT Professional Should Develop. *Harvard Extension School*. Retrieved June 19, 2018 from https://www.extension.harvard.edu/inside-extension/10-soft-skills-every-it-professional-should-develop. Last accessed June 19, 2018.

[11] Computer Support Specialists : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics. Retrieved May 25, 2018 from https://www.bls.gov/ooh/computer-and-information-technology/computer-support-specialists.htm. Last accessed June 19, 2018.

[12] Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics. Retrieved June 19, 2018 from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. Last accessed June 19, 2018.

[13] Computer and Information Systems Managers : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics. Retrieved June 19, 2018 from https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm. Last accessed June 19, 2018.