Cyber 2025 Position Paper
Social Influence and Trust in Cyberspace

Melanie C. Green
University of North Carolina at Chapel Hill

Some security challenges rely on individuals' judgments and behaviors. Online and cyber environments evoke some of the same kinds of social influence processes that occur offline, but these environments also pose some unique challenges, including the speed with which information can spread and possibilities for deception and anonymity.

Several areas of online behavior pose challenges and opportunities for cybersecurity research:

- **Online Persuasion and Trust**

Some types of cyber threats rely on user behavior: for example, individuals opening attachments or clicking on links to malicious sites. Although most individuals have some level of wariness or suspicion in online contexts, individuals are not often good at identifying deceptive sites or scams. Rather than increasing overall levels of suspicion, interventions could be developed to help users understand which cues to attend to, and ways to protect themselves and their systems against threats. (Additionally, technological solutions can be developed to help caution users or protect them against their own errors.)

Furthermore, existing networks of trust can be used for malicious purposes (e.g., hacked Facebook or email accounts that are then used for viruses or spam); research is needed to help users recognize these events.

- **Spread of Misinformation**

The difficulty of correcting misinformation has been demonstrated by social and cognitive psychologists, and has had substantial consequences in health and social domains (e.g., vaccination controversies). The problems of misinformation are amplified by the speed with which messages spread in cyberspace. Messages which go viral often have strong emotional content: they evoke surprise, anger, or amusement. They are also often narrative in form (telling a story). These features make the information more likely to be accepted by users, and this persuasion may be persistent over time and resistant to corrective information. A greater understanding of how to slow or stop the spread of incorrect information and how to correct this information can be an important direction for cybersecurity research.

- **Influence of Social Groups/Social Networks**

Bond and colleagues (2012) showed that banner messages presented on Facebook increased voter turnout; in particular, banner messages showing that one's friends had voted were particularly effective in encouraging users to click the "I voted" button and to actually vote. This Facebook experiment had a socially-beneficial purpose, but similar influence strategies could be used for more dangerous purposes. In particular, there is substantial evidence (from studies by Cialdini and others) that individuals conform to the behavior of others, but without necessarily recognizing this influence. A greater understanding of online social influence and ways that individuals might recognize and resist this influence can contribute to cybersecurity, particularly given the ease with which social consensus can be manipulated (e.g., through "bots" on Twitter, manipulations of Facebook message presentation, etc).

On the positive side, online social networks can also be a source of social capital, which contributes to stronger communities. Understanding how to build strong online communities and how such communities can help defend against cyberthreats can be an important future direction.