MYTHS AND PERCEIVED RISKS OF SOCIAL MEDIA SURVEY
FACT SHEET

Purpose: To uncover the biggest myths and perceived risks associated with active social media use, which has become the latest gateway for savvy identity thieves. In the United States, people fall victim to identity theft every two seconds, and active social media users are twice as likely to become victims of cybercrimes, according to Javelin Strategy & Research.

Methodology: InfoArmor conducted an online survey among social media users in the United States between April 7-13, 2015. The survey yielded 405 responses and carries a margin of error of +/- 5 percent.

Survey Sample: Data have been analyzed in total, as well as by gender, age and level of social media activity.

Survey respondents include:
- Men (209) and women (196)
- Social media users under age 30 (100), between the ages of 30-49 (101), and 50 and older (204)
- Active social media users (who post a minimum of three times per week: 149) and less active users (who post fewer than three times per week: 256)

Key Findings:

Facebook, it is. Facebook remains the dominant social media channel. Twice as many social media users have a Facebook account as have a LinkedIn profile – the next most popular social channel. There are demographic skews to social media: LinkedIn users are older and male, while Pinterest and Instagram users are younger and female.

More than half of Americans use social media to keep in touch with family and friends, but connecting with friends is contradictory. That’s because nearly four out of five survey respondents reported that half of those in their networks are not true friends. This is consistent across genders, ages and activity levels. Few (10 percent) social media users will friend someone they neither know or with whom they have a connection in common, but 41 percent are happy to friend someone with a mutual connection. This number jumps to 53 percent among those under age 30. These users assume that if they share a mutual connection, the individuals they friend “must be OK.”

Social media users know the risks of posting too much, but in many cases they do it anyway, opening their lives to cybercriminals who can readily access their personal information. Photos are the most commonly shared information. Especially worrisome is that regular use of social media does not make people any wiser. In fact, the more active posters share the most personal information, photos, vacation information, check-ins from around town, etc. – opening themselves up to potential wrong-doers. In the end, it’s not just themselves they are putting at risk: By regularly tagging others in their posts, they are giving ID thieves access to their friends, too.

-more-
At least one in five posters will share their work history, post information from vacation and check in on social while they are out and about. Those age 50 and older exercise more caution in posting such information.

**Social media privacy settings provide a false sense of security.** Although there is a high familiarity (73 percent) with sharing and privacy settings (67 percent), 40 percent of social media users rarely or never check their privacy settings. More active social media users check their privacy settings more frequently inasmuch as they are more likely to check them *occasionally.* What’s more, nearly half of social media users never clean out their social channels, and even the most frequent posters are not much more likely to do so.

**Despite these findings, what scares social media users most?** The majority of survey respondents agreed that using social media could open them up to crime or some other harmful offense. They are also fearful of giving up their privacy by oversharing information.

**Implications:** While social media will continue to grow, the effects of sharing information in social channels remain to be seen. As such, social media users should exercise caution by living online like a biography, not a diary.

In particular, users should:

- Censor themselves by posting information that would not be damaging to them in any way in the future;

- Be cognizant of the consequences of posting highly personal or too much information, since information shared online can never truly be erased;

- Be vigilant in checking their privacy settings on their social channels; and

- Lead by example to teach children and teens not to overshare and take ownership of their personal information online.