Online Privacy vs. Security

Are consumers who more freely share their personal information online at a higher risk for becoming a fraud victim?

Does Less Privacy Increase Risk?

Again and again, surveys tell us that U.S. consumers say they worry about security and value their privacy, yet they continue to freely give up personal and private information for more convenient services. This disparity in what consumers say compared to what they actually do has been highlighted in a number of recently conducted experiments showing that individuals are often willing to give up private or sensitive personal information for small rewards. One famous example of this phenomenon came from a study conducted in New York, where consumers overwhelmingly gave up sensitive personal information, including the last four digits of their social security numbers in exchange for a cookie. With the amount of personal data already exposed in today's world through cameras, microphones, sensors, online interactions and data breaches, does continuing to expose personal information really put an individual at greater risk of having their identity stolen? If we assume that consumers will continue to choose convenience over privacy and security, are they and the organizations they seek credit and services from likely to come under increasing attack in the coming years? To answer these questions, ID Analytics conducted a study to determine whether a person’s online exposure — the degree to which they share personal information online — is a predictive measure of whether they are at risk of becoming a victim of identity theft.

Study Methodology

ID Analytics collected data from an online people search engine, which aggregates exposed information on individuals from hundreds of websites, in order to gather information about individuals’ online presence. The collected data was used to produce variables that would identify an individual’s degree of online exposure by looking at the relationship between the combinations of exposed information, number of sources found, the accuracy of the information, the channels provided, among many other factors. Finally, these variables were used to build a supervised model, referred to as the “Exposure-Fraud Score”, aimed at using an individual’s online exposure to predict the likelihood of a consumer becoming a victim of identity theft. The Exposure-Fraud Score was tested by comparing two populations — the general population of people seen that had not been associated with identity theft, as well as a target population of consumers who were known to have been victims of identity theft. The theory behind the test was fairly simple; if the model could predict whether a consumer was likely to become a victim of identity theft using only online exposure data, a reasonable conclusion is that there is a direct relationship between sharing information online and becoming a fraud victim.

Results

The Exposure-Fraud Score was indeed able to have some success in predicting which consumers were likely to become victims of identity theft, which suggests a correlation between the degree of privacy an individual uses online and their likelihood of being a victim of identity theft.

Figure 1 looks at the distribution of the score, where a higher score indicates a higher likelihood of the individual becoming an identity theft victim, on both the general population (blue line) and the population that were seen as victims of identity theft (orange line). The chart clearly shows that the individuals in the identity theft population have a higher-risk score distribution than the general population, accurately reflecting their increased risk. This separation is especially powerful amongst highest score bands, there is a lift of over 500% for individuals seen over 650 and 800% for those over 900. The separation between the two lines shows that a model that is built solely using variables identifying an individual’s online exposure is able to differentiate identity theft victims from the overall

---

EXECUTIVE SUMMARY

population, confirming a troubling relationship between a consumer’s online exposure and their risk of becoming a victim of identity theft.

Why it matters

As consumers’ demand for customized services and interactions increases, they will be asked to share personal information with an increasingly diverse group of organizations and individuals. Despite fraudsters already existing access to a large volume of information on U.S. consumers — either through legitimate or illegitimate means — this study suggests that consumers who continue to forfeit their privacy in favor of convenience will be at a higher risk for identity theft than the general population.

While in many ways these results are concerning, as they point to a potential rise in the level of fraud in the U.S. marketplace in the coming years, it also suggests that consumers have some degree of control over their risk level for identity theft, based on the amount and level of personal information they are willing to share. The most predictive variable in the online exposure model is the number of social profiles that were able to be identified suggesting that consumers who limit their online exposure are making it more difficult for fraudsters to find personal information and lessening their risk of identity theft.

For organizations, this study highlights the likelihood that, as consumers continue to eschew privacy for convenience, fraudsters will be increasingly well-armed to perpetrate identity theft. There will be an ever increasing need for fraud tools to combat the growing sophistication of threats. It’s a trend that ID Analytics will continue to explore in the coming months and years — working to better understand how fraudsters are leveraging the increased availability of personal consumer information, and innovating new and improved solutions to keep them at bay.

ID Analytics’ solutions protect you and your clients
Partner with an experienced, trusted firm. Since 2002, ID Analytics has been delivering a unique perspective of risk based on proprietary Advanced Analytics and the ID Network®, one of the nation’s largest networks of cross-industry consumer behavioral data, not available in consumer credit reports. For more information about ID Analytics contact us at marketinginfo@idanalytics.com or 866-248-7344 or visit www.idanalytics.com.

ID Analytics is a registered trademark of ID Analytics, LLC. All other trademarks and registered trademarks are the property of their respective holders.