Lessons from BigBasket security breach

Hacking of BigBasket's servers is not just one firm's problem to solve, it is up to all of us to take active measures in protecting ourselves, and those we interact with, through the technology we use.

By Rahul De', Kriti Nagori, and Divyansh Bengani

Cyber crime is growing in India at a rapid pace. In 2019, the official records showed a 64% increase in cyber crime cases, as compared to the previous year. In 2020, owing to the surge in digital activities following from the lockdowns driven by the Covid-19 pandemic, the crime rate increased further, with some estimates at 80% higher than previous years.

Both private firms and government departments have moved to shore up security, however, there is no respite from crime. On 9th November 2020, one of the premier e-commerce sites in India, BigBasket, reported the theft of 20 million records of customers from their servers.
Cyber crime is affecting individual citizens also. There is widespread fraud and theft through digital means, and the victims are both rural citizens with low cyber literacy, as well as highly trained, urban IT professionals. Victims are tricked into revealing one-time passwords or into scanning quick-response (QR) codes in response to seemingly innocent requests.

We set out to investigate why is it that people are so vulnerable to cyber crime and cyber attacks. One hypothesis we formed is that most people are aware of the threats posed by their IT usage, but don't take them seriously enough. We set out to test this hypothesis by some simple experiments: ask people questions about security, present to them a possible scenario, then ask again about their threat perception. Our findings are revealing.

Our respondents belonged to two categories - the Digital Natives, who were under 35 years of age, and the Digital Migrants, who were above 35 years. All respondents were urban, educated up to college level, and of both genders. Digital Natives were savvy with computing and online activities, whereas Migrants were less familiar.

Awareness

71% of the Digital Migrants believed their online transactions were safe, until they were introduced to expert recommendations about safe behaviour, after which this figure became 30%. However, this new information had little effect on the Digital Natives, as they were generally aware of these guidelines.

Social Media

We observed a similar response to the security threats of social media. Users were asked to classify how safe they thought their social media accounts were. Next, a hard-hitting statistic was presented, and the same question was asked towards the end of the survey to ensure that the effect of recency bias was reduced. We wanted to gauge if a user's perception of their safety level changes. Initially, 53% of the Digital Migrants classified their social media accounts as safe. However, after seeing a few statistics highlighting the vulnerability of these accounts to criminal activity, the number reduced to 18%. The effect was not very pronounced on Digital Natives, since they were already aware of these facts.

Trust in the Product

Research has shown that people trust the product to keep them secure. They focus on the actual task while expecting the product to handle the secondary tasks of security. We asked users if they felt safe online, and among the respondents who said yes, 58% believed that the platform protected them. Thus, respondents put the onus of safety on the products and platforms.

Framing Effects

When security threats are framed as a loss, versus being framed as gains from being secure, the responses are different. Both sets of users were first presented with a scenario of data loss, because they did not have anti-virus software. Then they were presented with a scenario of benefits gained from following security practices. The response to losses was much sharper than for benefits.

Further, when security threats were framed as a personal loss, as opposed to a loss incurred by a third person, the response of both groups was sharper to the former. Around 74% of the respondents wanted to learn more about cyber risk when the survey question was framed with the former as opposed to 59% with the latter.

Financial Loss

Financial losses grab greater attention than other losses. To test this, we asked users if they would adopt a cyber security measure. The next question put users in a hypothetical situation where they incurred a financial loss. Their willingness to adopt the preventive measure was then assessed.

Initially, only 14% of Digital Migrants and 36% of Digital Natives were willing to adopt measures to counter the cyber-security risks. However, when presented with a financial loss situation, this number jumped to 83% and 73% respectively. We concluded that the fight-or-flight response was thus triggered by something as tangible as one's hard-earned money being lost.

Conclusions

Our study and analysis have implications for the design of products and of policy measures to control cyber crime. One, product designers and government should distinguish between the two groups of users, Natives and Migrants, and their understanding and perception of technology. One group is clearly more risk-averse than the other. Two, provide hard statistics and facts to both groups while presenting any product or policy. Three, highlight losses and threats in framing messages, over benefits.

Particularly, financial loss has a greater attention-grabbing effect than other things. For instance, mentioning the loss of money from hacking of accounts has a far greater effect than mentioning the number of accounts hacked.

Cyber crime will continue to grow unless we counter it with both well-designed products and well-thought through consumer awareness policies and measures. Hacking of BigBasket's servers is not just one firm's problem to solve, it is up to all of us to take active measures in protecting ourselves, and those we interact with, through the technology we use.

Rahul De' is a Professor of Information Systems, Kriti Nagori and Divyansh Bengani are MBA students, at IIM Bangalore