Symantec Corporation has released the Norton Cybercrime Report 2012. The report recognises India as one of the fastest growing internet and mobile market globally. According to the report, with over 137 million internet users in India, 7 out of 10 users access internet through mobile. Additionally, the country's social media user base increased from 38 million in 2011 to 60 million in 2012.

As per the report findings, both mobile and social media platforms emerged as the preferred site for cybercrime attacks. The report states that cybercriminals are constantly changing their tactics to target both these fast-growing platforms where consumers are less aware of security risks. The individuals have faced loss of data, identities and finances.

Moreover, the report estimates that in India, more than 42 million people were affected by cybercrime over the last 12 months. People affected by cybercrime suffered direct financial losses of about $8 billion.

David Hall, marketing manager, regional consumer product, Asia Pacific, Norton by Symantec, says, "Cyber terrorism will get highly personal as attacks focus on individuals or minority groups and there is a higher possibility that new electronic payment methods could be vulnerable to hacks and breaches."

A few of the key emerging trends in cybercrime in 2013 are:

Cyber conflict becomes the norm - Conflicts between nations, organisations, and individuals will play a key role in the cyber world. Espionage can be successful and also easily deniable when conducted online. Nations or organised groups of individuals will continue to use cyber crime in an attempt to damage or destroy the secure information or funds of its targets. The year 2013 will see more targeted attacks on individuals and non-government organisations, such as supporters of political issues and members of minority groups in conflict.

Ransomware is the new scareware - Ransomware is a malicious software that disables the

functionality of a computer and demands a ransom in order to restore the computer to its original state. Cybercriminals have taken to cheating people by using online payment methods. In 2013, attackers will use more professional ransom screens, up the emotional stakes to motivate their victims, and use methods that make it harder to recover the lost money.

Madware catching-up - Mobile adware, or “madware,” disrupts the user experience and can potentially expose location details, contact information, and device identifiers to cybercriminals. Madware, which sneaks onto a user device when they download an application often sends pop-up alerts to the notification bar address icons, changes browser settings, and gathers personal information. Over the last nine months the number of applications including the most aggressive forms of madware has increased by 210 per cent. Since, location and device information can be legitimately collected by advertising networks, it helps cybercriminals target users with appropriate advertising. There will be increase in madware as increasing number of companies seek to drive revenue growth through mobile advertising.

Monetisation of social networks bringing in new risks - As consumers, people place a high level of trust in social media - from sharing personal details, to spending money on game credits, to gifting items to friends. While e-payments have so far been adopted slowly by consumers but with the addition of payment methods in social media, e-payments will increase significantly. With this there would also be increase in the incidents of cybercrime, wherein malware will spread socially. It takes over the user's account, re-sets passwords and uses the encrypted but stored credit card information to make real world purchases for the cybercriminals. Cybercriminals will sell and trade financial information with one another to gain greater access to people’s accounts.

As users shift to mobile and cloud, so will cybercriminals - Cybercriminals will follow users to new mobile devices such as smartphones and cloud. There have been significant increase in presence of Android-based malware in 2012. As users add new applications to their mobile phones they will pick up malware. Some mobile malware duplicates old threats, like stealing information from devices. Today mobile malware sends premium text messages to accounts that cybercriminals can profit from.

According to Norton Cybercrime Report 2012, in India 31 per cent of mobile users have received unsolicited SMS text asking them to call back on an unknown number or click on an embedded link. What makes people more prone to cyber attacks is the fact that the majority of the mobile internet usage is being handled by unsecure mobile applications.

About Us We are Hiring Contact Us

Subscribe Privacy Policy Advertise Terms & Conditions

Copyright © 2010, tele.net.in All Rights Reserved