#8: Cybercrime – What's new?

Cybercrime metamorphoses with each passing technological milestone

While hacking, email spoofing and phishing continue to be the most common modus operandi, mobile devices are now at the top of the list of devices that enable financial theft due to ease of physical access as compared with data on a cloud or information residing on physical servers at data centers.

Cybercriminals are also jumping on the internet of things (IoT) bandwagon by exploiting poor password practices to take control of IoT devices for malicious or criminal purposes.

Further, many cybercriminals are turning to social media to not only carry out phishing attacks but also scope out potential "marks". Using social media allows them to vastly extend their reach to more people and decide who to attack.

With more than half the world's population using the internet and internet enabled devices, fraud prevention approaches now require solutions that can extend to mobile and cloud environments, make greater use of behavioral analytics, take advantage of integrated threat intelligence capabilities, and most importantly, be designed with customer experience in mind.

Organisations are therefore now turning to behavior analytics technologies to ensure that authenticated users and anonymous guests are interacting with their websites or public interfaces (such as apps etc.) in expected ways.

While it is impossible to stop every fraud attack, it is possible to change how organisations detect and respond to them in order to minimise the potential loss or damage.

Creating a cyber-perimeter is the need of the hour

Click here, to download the complete survey report