The Rise of Mobile Cybercrime

The Rise of Mobile Cybercrime: Be Aware. Be Secure.

Digital connections now play a central role in global socio-economic development, and mobile is the clear growth driver. These days, practically everything digital you want to do can be done on a mobile device. The mobile-centric world of consumer convenience, seamless interactions, and real-time services have brought with it trillions in revenue - and where there is money, fraud will surely follow. The threats are operating on a global scale so it's no surprise that by 2019 cybercrime will be a $2.1 trillion problem.[1]

The Shocking Truth

News of the vulnerabilities to the central nervous system of a mobile network, Signaling System No. 7 (SS7), went mainstream this year when US current affairs show, 60 Minutes, revealed just how simple it was to hack into a Congressman's phone, listening to and recording calls, tracking his movements and viewing his contacts. This wasn't just another news story about the perils of mobile spam or fraud scams but exposed how every mobile operator in the world has weaknesses in their network, which can be exploited by fraudsters and hackers and put anyone at risk. As fraudsters become increasingly sophisticated, they will continue to abuse holes in technology for their own financial gain.

Be Aware, Be Secure

As the old adage goes, "knowledge is power". The vulnerabilities are real and abuse is happening, but while operators have a responsibility to protect their customers, it is everyone's responsibility to be cyber aware and cyber conscious in order to protect themselves accordingly. But how aware mobile subscribers are of mobile network weaknesses and indeed all mobile cybercrime threats, in reality, is a question that remained unanswered.

We carried out a survey to explore consumer awareness across the US, UK, and Australia to see what the general consensus was. What concerns subscribers the most? Are they being cybersecurity savvy? What if they experienced an attack? What role do they feel their operator plays as part of this?

The Bottom Line

Mobile subscribers are very afraid of the different types of mobile cybercrime threats but a high number are unaware of the extent that these pose. While at the same time, a good proportion of mobile subscribers (32%) never check their balance or their bill to verify that they have been correctly charged or to detect possible suspicious activity on their account. Sometimes, the only evidence of an attack would be the discrepancies on a bill.

But irrespective of this, there is a level of trust and a strong assumption that their operators will protect them from these threats - and, if they found out they were attacked, almost 1/3 would change their provider and half would seek compensation.

Securing the network is the best approach for operators to secure customer loyalty, and ultimately protect their bottom line. However, as our infographic shows, consumers can take a few simple steps to protect themselves too by being more cyber aware, and cyber-savvy.

MAVENIR BLOG POST

The Rise of Mobile Cybercrime: Be Aware. Be Secure.

[1] Juniper Research The Future of Cybercrime & Security Report 2015 - 2020