Beware mobile carriers, the media's watching you...

By Leigh Andrews

13 Nov 2014

Headlines about mobile malware dominate the media. If you were to believe all of them, you'd never turn on your phone. But whose responsibility it is really to educate digital and mobile citizens of fraud risks? Read on to find out more...

Mobile brings with it great promise and possibility but also the risk of data and personal information breaches, especially in the Snowden era, said moderator Brendan Smith, VP of professional services at Vital Wave, in the second panel discussion on the final day of the Mobile360 event. The panel unpacking these issues comprised Ciaran Bradley, SVP solutions and innovation of Adaptive Mobile, Ibrahim Dikko, director of regulatory affairs at Etisalat Nigeria, Alvin Rajoo, business development director of 4C Group and Jacqueline Fick, executive of forensic services for Cell C.

Bradley kicked off the session and ensured attendees were paying attention by asking questions about loss of privacy and mobile malware as well as national security concerns as risks to enhancing digital citizenship. On the topic of mobile malware, he said there are a number of premium 'Trojans' that you don't realise you've installed on your handset, which is why two-factor authorisation codes to access mobile banking are on the rise.

Should you believe everything the media says about mobile safety threats? Not necessarily...

But Bradley says not to let media sensationalism get to you, as a Google study on the annual Virus Bulletin of 2013 showed only a minor amount of installations actually threaten your personal data. So yes, there's no denying that privacy as a concern, but privacy from whom?

> *Is the case for mobile malware overhyped? The question posed discussing the biggest risks to citizens in the mobile age @GSMA #mobile360- Brendon Petersen (@Bren_Peter) November 7, 2014*

Bradley points out that we're already sharing too much online due to lack of member understanding. He added that Facebook reports its requests for information from legal agencies was up by 24% in the start of 2014 over the year previous. But Bradley says not to take a negative stance as it's not all doom and gloom. That said, he feels mobile network operators definitely have key role to play in educating the next two billion subscribers to come online, which will be one of the most difficult tasks.

Dikko then echoed Bradley that it is a huge concern to educate those who are not yet online and those who have already started using mobile banking platforms, saying there's already a raging debate over whose responsibility it is to educate these people. He asked, "If people drive while using their handset, should the mobile operator be blamed?"

Next was Rajoo, who said that in a few years, as the networks evolve, all information that can be digitised will be digitised. There's already proof of this with consumers showing a preference to communicate via typing than voice, evidenced by the popularity of WhatsApp.

Mobile banking... here's why you *should* worry

Rajoo said the mobile device is therefore not just for communication but also for transacting, and that's where the biggest risks lie. An example of this is if your handset suddenly embarks on a download while roaming, as this is pricey if you don't notice it happening.

Parental control also is important, and Rajoo feels certain mobi-sites should be blacklisted so that they can't be accessed by children.

Fick spoke next, saying she can't count how many times she's been asked what a mobile operator is doing with a forensic services division.

> *"SA ranked by the FBI as the 6th most active cyber country in the world" @CellC's Jacqueline Fick - Head Forensic Services #mobile360- Brendon Petersen (@Bren_Peter) November 7, 2014*

Fick adds that we focus so much on having good computer IQ and being 'PC literate' but we forget that having 'mobile IQ' is just as important, if not more so. "Unfortunately many still see the mobile phone as a 'tring tring' to call people on, we forget just how much information we share on it," cautions Fick. That's why it's important to get people to rethink saving passwords on their handsets in order to mitigate the risk and get people to be more responsible mobile citizens.

Sex sells - be careful you don't fall for phishing links and lose your money in the process!

Next, Bradley spoke about the possibility of posting short videos on mobi-sites in order to educate mobile consumers of the risks of following shortened phishing links. He says, "Sex sells, so we don't think about clicking on a link from a non-verified Twitter contact... But before you know it, all your banking info has been stolen if you didn't take care to protect your mobile banking."

Dikko added that certain very popular sex sites were blocked in Nigeria in light of mobile banking safety, as education is not just responsibility of mobile network operators. Rajoo interjected that it's human nature for us to simply react to a crisis and not prepare ahead. That's why a lack of passwords - or rather, a lack of clever passwords - is leading to fraud. He suggests launching a simple SMS campaign if the SIM card in a handset switched, that would lock the device in case it had been stolen. He calls this an example of doing simple things people can understand. For example, when consumers open the box of a new handset, most don't read the handset instruction manual first - you simply want to turn on the device and get started.

Password education as a vital aspect of protecting personal information in the mobile space

To get around this problem, Rajoo suggests adding a sticker to the handset's screen asking users to replace the default password before starting. He pointed out again that it's about going down to the lowest common denominator of non-sophisticated customers. Fick agreed that awareness is a shared responsibility of government, mobile network operators, law enforcement and more, all of which are experts in different fields.

She feels the basic message is most effective and that mobile consumers need to be taught the basic skills of changing password and not clicking on foreign links will go a long way. She adds that TV is a great medium to reach the masses, as well as SMS, newspapers as well as internal staff communications, as successful change starts small, then creates a ripple effect.

© James Thew – 123RF.com

In closing, Smith asked the panel how identity theft can be stopped. Fick spoke of the need for mobile network operators to seek better co-operation with role players, adding that successful strategies against identity theft leading to financial loss are on the cards due to public-private partnerships between police and banks. Dikko says biometrics can help too, where different levels of enforcement regarding SIM registration rules are implemented like using someone's photograph as well as getting them to fill out a form and check it against biometrics. He says this is a stringent process in Nigeria, where many citizens don't have a set address.

This led to a discussion of privacy vs national security and how societies find a balance. While privacy is definitely top-of-mind post-Snowden era, we're only now realising power of digital surveillance. Most people don't even realise just how much data is out there, but security companies do. Luckily, they need the right to publish certain information. That's why Bradley says it's reassuring that Facebook statistics in South Africa show there were just two requests based on national security in the past year, with around 15,000 in the US over the same timeframe. Dikko said it is already built into the mobile network operators' licenses that they will cooperate with national security requests, but says this brings into question how to still protect citizens while complying.

L to R: Alvin Rajoo, business development director of 4C Group; Ciaran Bradley, SVP solutions and innovation of Adaptive Mobile; Ibrahim Dikko, director of regulatory affairs at Etisalat Nigeria; Jacqueline Fick, executive of forensic services for Cell C; and Brendan Smith, VP of professional services at Vital Wave.

Verizon's very relevant supercookie example

Rajoo spoke next about cookies, which are always a controversial subject. He said there are cases where storing

information on users is acceptable such as if the intent is good, such as if it's used to localise browser content or time zones or to optimise specific handset screen information, but you should still ask for users' permission and not just take it without consent.

What caught people out in the Verizon case that it's been active for two years and adds a unique identifier to the user's http header, so adding the power of analytics could make this very dangerous. He says many say it's there for marketing purposes, but others have been caught out for not making it obvious and not handling the fallout well. Click here for *Time magazine*'s online overview of the Verizon supercookie case.

Lastly, the panel implored the audience to not just think of it as the mobile network operator's responsibility to get the information out there. You need to think from the start how any information will be portrayed if the media gets hold of it. There's also the role if third parties like advocacy groups or government, as well as the consumer protection council. Dikko feels civil society groups should be encouraged to do more and collaborate with mobile network operators. Fittingly, he pointed out that a handful of mobile operators signed a code of conduct for mobile money providers operating across 51 countries on Thursday at the spectrum-based GSMA event - click here for more.

Click here to read up on the first panel discussion of the day.

ABOUT LEIGH ANDREWS

Leigh Andrews AKA the #MilkshakeQueen, is former Editor-in-Chief: Marketing & Media at Bizcommunity.com, with a passion for issues of diversity, inclusion and equality, and of course, gourmet food and drinks! She can be reached on Twitter at @Leigh_Andrews.

- Sign of the future? The creativity of April Fool's Day pranking in the retail industry - 2 Apr 2019
- #ECO19: Why brands need to create emotional experiences for Generation CX - 19 Mar 2019
- The business of curating a Loveable online and pop-up store - 15 Nov 2017
- #CGFSummit: Reap the rewards of doing business sustainably - 17 Jun 2016
- #CGFSummit: Digitisation of everything - 17 Jun 2016

View my profile and articles...