KCS Group Europe

Apps for everything: where we should draw a line

We have entered an era characterized by digital addiction. Our lives are now tied to technology; everything can be controlled by apps on a phone. Since technology has acquired such a dominant role today, ranging from the use of social media to communicate to asking Alexa to turn on the lights, we should think more carefully about the implications that comes with it and learn where to draw a line.

Nowadays there are apps for every need. They are not limited just to checking the weather or reading the news, they go further than that. Social media has become the prominent means of communication, almost replacing our day-to-day physical interactions.

Mobile banking is another tool offered by apps that facilitates the way we experience dealing with financial matters. Through the app it is possible to access your current bank statement and even make payments and transfers. Apps like Apple Pay allow you to complete transactions without even needing you card in the shop, but just using your phone instead. On one side they make our life easier, but on the other, they expose us to threats from bad actors.

Facebook is even exploring the possibility of combining social media and financial services on the same platform to allow customers to chat with their bank through Messenger, to avoid the waiting time on the phone.

Shopping is another activity that deeply relies on apps. Moving from the physical shop, users now prefer either to shop on websites or, even easier, directly through their phones. Studies have demonstrated that customers not only spend more time shopping when using their mobile but are even more likely to purchase. But again, the downside: shopping apps have access to credit card details plus personal information and preferences. A lot is put at stake.

Apps have also taken over the transport sector. Their services range from calling a taxi to renting a car, all at your fingertips. Uber is the leader in the sector, but a long list follows. Other apps instead will calculate your journey and give the best options available on public transport. Moreover, it is now possible to rent vehicles just with an app: for example, Car2go and Zipcar for cars and Yugo, Scoot or Bird for any sort of scooter sharing option. Not only do these apps collect financial data, but they also track your movements in real time and are capable of detecting information about your daily commute (ie. Citymapper).

Technology is evolving, and it can record human functions such as blood pressure or sleep cycles, like the new generation of Apple watches do. Even the NHS website has a list of about 40 apps that it recommends for health purposes, the topics are varied: reducing stress and anxiety, first aid, healthy eating, exercise tracker, stop smoking, and many others - even one that plays music for the specific amount of time that you should brush your teeth.

Apps for everything: where we should draw a line

These apps can be very helpful but at the same we should reflect and think about the amount of personal, very intimate, information we unknowingly allow them to record and share with third parties every day.

Finally, the most intrusive: smart homes. In fact, all the appliances connected with the central command, most commonly known as Siri or Alexa, are constantly recording data and sending it back to their manufacturers. It is possible to connect any sort of device, from coffee machines, to beds and curtains, as well as lights and thermostats: they are all discreetly 'spying' on you and your habits.

As the number of people utilizing a smartphone is increasing with the rise of the Internet of Things so do the security threats related to its use. The more the devices/appliances connected the more the chances of being hacked as the available entry points for malicious actors multiply. Protecting the mobile device should be a priority as cybercriminals evolve and learn to adapt to new technologies.

A first step should be to be extremely cautious when downloading apps, especially if from third party sources as those could be corrupted or malicious. Another important trick is to keep the apps updated as new security features are constantly being released by the suppliers. Finally, it would be desirable to avoid making transactions when using public Wi-Fi as it would ease the theft of credit card credentials.

Smartphones and their apps are now an integral part of our lives, as we resort to them for every need. Although they can be very helpful at times, we should learn when and how to draw the line between us and technology. Lots of information, too much, is constantly shared increasing the chances of falling the victim of hacks.

We have survived hundreds of years without Alexa turning on the light we can survive many more?

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

To find out more or to arrange a meeting to discuss your business needs, please…
email the team at info@kcsgroup.com or call (00 44) 2072451191