Solution spotlight | **Data - the oil of the digital economy**

Kingdom of Bahrain | 6 February 2022

keypoint

We have just had international data privacy week – but data privacy should always be top of mind so our data experts have explored what it means at an individual level.

What is data privacy?

Data privacy focuses on how data is handled, collected and used. It means the ability of a person to determine when, how, and to what extent personal information - names, locations, contact information, or online or real-world behaviour - is shared with or communicated to others.

Are data privacy and data security the same?

Short answer - no! Data security is much broader than data privacy and is focused on protecting data from unauthorised users through different forms of encryption, key management, and authentication.

Social networking sites

Social networks - like Facebook - update their privacy policies fairly often, prompting users with a pop up to accept or reject the new policy. As privacy policies are often incredibly long, users tend to simply accept new policies without checking them. As a result, social networks can legitimately - and often do - share user information with third parties.

To avoid this, visit your social media application to ensure that the privacy settings you have selected haven't changed. If they have changed due to the company's 'updated privacy policy', either reselect – or consider if you want to continue with the application if it is so keen to violate your privacy!

Another point on social networking - share as little personal information about yourself and your family on social networks as possible. Do not, for instance, post a picture of your new car with your registration visible, or a photo of your house with the street number in plain sight. On Facebook, unfriend anyone you do not personally know.

What about apps on mobile phones?

Permissions on mobile phones are an important part of access control. When installed for the very first time, apps require the user's permission to access certain areas of your phone. Try not to give permissions when the permission doesn't relate directly to the app as you might find your personal data, contacts, account passwords and bank passwords are harvested. If you give permission for a specific, one-time use, go back to the app's permission setting afterwards and edit it.

Installing apps

Before downloading an app, check reviews and ratings, try to relate its functions to the permissions it is asking for and don't install it if you smell something fishy – or just don't feel comfortable with the level of permissions.

App permissions

Allowing an application such as Google Voice to make phone calls or send texts can be legitimate – but you could be allowing your phone to automatically contact premium-rate numbers and text services! This is a good one to look out for when deciding whether a request is reasonable.

Network communications

We are quite often asked for full internet access, to view network or wi-fi status or create a Bluetooth connection so an app can retrieve widgets or update a web browser or social networking software. However, this is also an essential permission for malware designed to transfer data off a phone, so be careful! Apps requesting Bluetooth connections are less common but allow data to be transferred to someone (or so ask yourself exactly why this is being asked for.

keypoint

Your location

If an app asks for permission to find a GPS or network-based location, it could be trying to remotely activate your phone's GPS functionality and use it to track your handset. While this sounds worrying, it's usually fairly easy to determine whether a request is legitimate. Mapping apps, location finders and GPS software will commonly ask for this access, which is integral to the smooth running of the software.

Storage

Requests to modify or delete SD card contents give apps full access to read and delete data and create files on attached SD cards. While any malware designed to gather data from a phone or install additional files will need this form of access, many legitimate applications require it at as well. Judge each case on its individual merits and exercise caution if you believe the request to be unusual.

Your personal information

While requests to read contact data or read or write calendar data are potentially dangerous (because malware could be used to access that contact and calendar information), it's usually fairly easy to spot unusual requests. Replacement calendars, phone books and social networking software all commonly request this access, but unless it's obvious exactly why an app needs this information, you are probably better off saying 'no'.

Data takeaway

Your data is **yours** - so it is your **right** and your **responsibility** to know how, when and where it is used. Before sharing any personal data, think how it might be used to harm you, your family, your colleagues or your business!

Contact us:

Srikant Ranganathan
Senior Director
srikant.ranganathan@keypoint.com
+973 1720 6827

Sagar Rao
Manager
sagar.rao@keypoint.com
+973 1720 6802

Prakash D'mello
Data SME
prakash.dmello@keypoint.com
+973 1720 6806