

Security, is there an App for That?

BRUSSELS and HERAKLION, Greece, /PRNewswire/ -- A new ENISA report identifies the top security risks and opportunities of smartphone use and gives practical security advice for businesses, consumers and governments. Top risks include spyware, poor data cleansing when recycling phones, accidental data leakage, and unauthorized premium-rate phonecalls and SMSs.

Worldwide smartphone sales doubled last year (Gartner) and 80 million were sold worldwide in Q3 2010 alone - ENISA's new report on smartphone security risks and opportunities is timely. If you are one of the hundreds of millions of smartphone users worldwide, you probably spend more time with your phone than your spouse. With its array of applications and sensors, it may even know more about you. These new life-partners are now an essential tool across all sections of society, from top government officials to businesses and consumers. They are famous for their diversity of functions; a smartphone can be a contactless wallet, a camera/videophone, a barcode reader, an email client, or a way of accessing social networks.

"Given the growing importance of smartphones for EU businesses, governments and citizens, we consider it essential to assess their security and privacy implications," says Prof. Dr.Udo Helmbrecht, Executive Director of ENISA.

In its new report, ENISA analyses the key security opportunities and risks. Some of the key risks are:

- * Accidental leakage of sensitive data -e.g. through GPS data attached to images.
- * Data theft by malicious apps and from stolen, lost or decommissioned phones.
- * "Diallerware" - malicious software which steals money through unauthorised phone calls.
- * Overload of network infrastructure by smartphone applications.

In terms of opportunities, backup is often very well integrated into smartphone platforms, making it easy to recover data if the phone is lost or stolen. Another opportunity lies in the use of app-stores: "Most smartphone users only install 3rd party software through controlled software distribution channels," says Dr. Marnix Dekker, co-author of the report.

The most important result of the report is a comprehensive set of strategies for securing smartphones. "Smartphones are a goldmine of sensitive and personal information - it's vital to understand how to maintain our control over this data. We've designed our recommendations to plug into a typical security policy," says Dr. Giles Hogben, co-author of the report. The report has recommendations for

Security, is there an App for That?

Published on Wireless Design & Development (<http://www.wirelessdesignmag.com>)

businesses, top officials and consumers - and for dealing with the security risks of mixing these roles.

Read the full report at: <http://enisa.europa.eu/smartphonesecurity/> [1]

Source URL (retrieved on 07/31/2014 - 12:04am):

<http://www.wirelessdesignmag.com/news/2010/12/security-there-app>

Links:

[1] <http://enisa.europa.eu/smartphonesecurity/>