Letter to the Editor

Security Concerns to Be Considered When Downloading Human Immunodeficiency Virus/Sexually Transmitted Disease Related Smartphone Applications

Savita Lorreta Brito-Mutunayagam, BmedSci, MBChB; Imali Fernando, Dip HIV, MRCP, MB ChB

Chalmers Sexual Health Centre, Edinburgh, United Kingdom

Corresponding Author:
Savita Lorreta Brito-Mutunayagam, BmedSci, MBChB
Chalmers Sexual Health Centre
2a Chalmers Street
Edinburgh, EH3 9ES
United Kingdom
Phone: 44 447833497767
Fax: 44 0131 5361609
Email: savita.brito.mutunayagam@gmail.com

(J Med Internet Res 2013;15(10):e222) doi: 10.2196/jmir.2650

KEYWORDS

HIV/STD; smartphone applications; security

"Mobile Phone Applications for the Care and Prevention of HIV and Other Sexually Transmitted Diseases: A Review" by Muessig et al is an excellent review that succinctly summarizes currently available mobile phone applications (apps) related to the prevention and care of human immunodeficiency virus (HIV) and other human immunodeficiency virus/sexually transmitted disease (STDs) [1]. The authors have comprehensively reviewed apps related to HIV/STDs and identified the need for health care professionals to work closely with app developers to provide accurate evidence based advice, and design effective risk reduction interventions.

While Muessig et al rightly raised concerns regarding the accuracy and reliability of the content of these apps, an important area not discussed in their review is the security of the apps. When downloading an app, the user is asked to authorize the "permissions" requested by the application. These "permissions" enable the optimum performance of the app on a smartphone [2]. There are over 100 different " permissions" requested by smartphone applications. While some of the "permissions" requested are harmless, many raise serious concerns regarding the confidentiality and security of the apps requesting them [2]. These include permissions that request;

The above mentioned permissions that an app may require for optimum functioning involve access to and control of sensitive personal data. Applications often have legitimate reasons for accessing this sensitive and private data. Permission to obtain the exact GPS location of the app user is necessary if the app is designed to provide information on the nearest HIV/ STD testing center. If the app is designed as a personal assistant for those living with HIV, access to the user's calendar is important to remind them of their next hospital appointment.

However, the concern arises when the app is not developed by a named professional health care body/organization and there is no assurance of confidentiality. Today's smartphone applications often fail to provide users with visibility into where their private data is being stored and how it is being used. There are often significant social implications associated with a diagnosis of HIV and the secure storage of their personal information is of immense importance to those living with the condition. Even individuals simply looking for information on the topic, or calculating their risk of contracting a STD after unprotected sexual intercourse, may be concerned if an unverified smartphone application had access to their personal information including precise location.

Muessig et al reviewed HIV and STD related apps that matched their search criteria in the Apple iTunes Store and the Android Google Play Store, as combined these two companies account for over 86% of the global app market [1]. In the android store this information is readily available within the app details. Apple does not explicitly specify permissions required in the app details, but this information is available on download. Apple states that all their apps are pre-screened prior to making them available for download. However, the recent controversy surrounding Apple, for enabling the download of malicious apps that stole their users' address books, show that this screening process is not infallible [3].

Providing HIV and STD prevention and care services via smartphone applications is an area of rapid and immense growth. If provided by trusted and professional organizations which guarantee the security of their users' personal information, they can be a powerful and rapidly accessible resource. However, it is essential that users are aware of the potential confidentiality

and security breaches when downloading these apps. They must be encouraged to pay attention to the app developer in order to ascertain if it is a reputed body Furthermore, they should note the permissions requested by the apps and only proceed with the download if they are comfortable with these requests. Whilst more vigilance amongst app users is essential, it is also the responsibility of the companies that offer these apps to ensure their products are not malicious and employ the highest levels of data protection software.

Conflicts of Interest

None declared.

References

1. Muessig KE, Pike EC, Legrand S, Hightow-Weidman LB. Mobile phone applications for the care and prevention of HIV and other sexually transmitted diseases: a review. J Med Internet Res 2013;15(1):e1 [FREE Full text] [doi: 10.2196/jmir.2301] [Medline: 23291245]
2. Chia HP, Yamamoto Y, Asokan N. International World Wide Web Conference. 2012 Apr. Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals URL: http://www2012.wwwconference.org/proceedings/proceedings/p311.pdf [accessed 2013-04-04] [WebCite Cache ID 6Fd53y4iK]
3. Gilbert J. The Huffington Post. 2012 Feb. iPhone App Privacy: Path, Facebook, Twitter and Apple Under Scrutiny for Address Book Controversy URL: http://www.huffingtonpost.com/2012/02/15/iphone-privacy-app-path-facebook-twitter-apple_n_1279497.html [accessed 2013-04-04] [WebCite Cache ID 6Fd6eINX7]

Edited by G Eysenbach; this is a non–peer-reviewed article. Submitted 04.04.13; accepted 01.10.13; published 07.10.13.

Please cite as:
Brito-Mutunayagam SL, Fernando I
Security Concerns to Be Considered When Downloading Human Immunodeficiency Virus/Sexually Transmitted Disease Related Smartphone Applications
J Med Internet Res 2013;15(10):e222
URL: http://www.jmir.org/2013/10/e222/
doi: 10.2196/jmir.2650
PMID: 24100134