CASE STUDY

MENTAL HEALTH APPS: Privacy Risks

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

PROJECT SNAPSHOT

Thousands of mental health apps are now on the market, offering cost-effective and easily accessible support services. However, while these apps serve an important purpose, many are also putting the privacy of users at risk and could be improved.

WHO'S INVOLVED

This project was funded by the Cyber Security Cooperative Research Centre (CSCRC), with research carried out by the University of Adelaide in collaboration with Bristol University.

WHAT'S THE ISSUE?

The growing pressures of daily life are driving more people to use mental health apps when seeking psychological support. This trend has accelerated significantly in the past year due to social distancing demands that have been imposed as a result of the COVID-19 pandemic. While digital mental health services are increasingly being endorsed by governments and health professionals as a low-cost alternative to therapy, there are potential downsides. While these apps might offer help in addressing problems connected to our changed lifestyles, new research has revealed they can be risky when it comes to privacy. Analysis of mental health apps on the market has revealed the personal privacy of app users is often at risk. The risk comes either through security breaches or by common data sharing practices between app developers and third parties which are not cyber secure. Considering the sensitivity of personal health data, loss of privacy can prove harmful to an individual's reputation or health, which in turn, can hinder trust in such solutions.

Our research has found most apps pose linkability, identifiability and detectability threats. These are potential violations, since users of mental health apps are generally unaware of the privacy impacts from targeted advertising and re-identification, and the disclosure of a mental health condition. The majority of apps tested were identified to have critical security issues, including transmission of sensitive information over the internet and logging sensitive information, while some were found to leak sensitive data to third parties.

WHAT WERE THE OBJECTIVES?

- Examine privacy risks in mental health apps;
- Determine solutions to reduce the threats;
- Raise awareness of the privacy risks and concerns to allow app developers to improve their products and offer greater protection for users

TECHNOLOGY DESCRIPTION

Our team of researchers carried out security assessments and privacy analysis on 27 publicly-available mental health apps. The criteria for the apps included having at least 100,000 users and a minimum four-star rating on Google.

Penetration testing was used to effectively 'reverse engineer' the app and retrieve the source code. This static analysis allowed researchers to analyse the source code and permissions used and investigate the websites the app is communicating to. Dynamic analysis was also carried out, and involved our researchers using the app to capture what was going on in the background in terms of data sharing etc.

Researchers determined it was relatively simple to carry out privacy checks and monitor network traffic to determine whether the apps put users at risk. Highlighting potential problems allows developers an opportunity to improve their product and offer greater privacy protection.

Despite the apps scoring highly on Google, researchers determined they should be considered 'high risk', and it is recommended developers carry out data protection assessments. Researchers found 'start-up' apps often had small teams and did not have the resources to carry out assessments. There was also a lack of awareness of what developers should be doing to protect user privacy.

APPLICATION

Developers of the 27 mental health apps studied by our team, were all contacted and offered the report findings and feedback from the responsible disclosure process. Responses received to date to the findings have been relatively positive, indicating appreciation to ethical research, intended to help build more secure and privacy-preserving apps. Of the companies that have reported back, companies reported back, feedback has indicated that the issues raised were or are being fixed for the subsequent releases of the apps. This analysis could be beneficial to help developers improve current and future apps in this space.