Are our pets leaking information about us?

February 27 2023

Credit: Pixabay/CC0 Public Domain

Pet and animal-related apps are creating cybersecurity risks to their owners, new research has shown.

While being able to trace your cat and dog may be an attractive benefit to many pet owners as it can provide peace of mind, allowing a third

party to track your movements may be much less attractive.

Computer scientists at Newcastle University and Royal Holloway, University of London have exposed multiple security and [privacy issues](#) by evaluating 40 popular Android apps for pets and other [companion animals](#) as well as farm animals. The results show that several of these apps are putting their users at risk by exposing their login or location details.

Password vulnerability was one of the areas exposed by the team. They identified three applications that had the user's login details visible in plain text within non-secure HTTP traffic. This means that anyone is able to observe the [internet traffic](#) of someone using one of these apps and will be able to find out their login information. In addition to login information, two of the apps also showed user details, such as their location, that may enable someone to gain access to their devices and risk a cyber-attack.

Another area of concern identified in the study was the use of trackers. All but four of the applications were found to feature some form of tracking software. A tracker gathers information on the person using the application, on how they use it, or on the smartphone being used.

The scientists also warn that the apps perform very poorly in terms of notifying the user of their privacy policy. Their analysis shows that 21 of the apps are tracking the user in some way before the user even has a chance to consent to this, violating current data protection regulations.

The study was led by Newcastle University and the Royal Holloway, University of London and presented at the 2022 *IEEE European Symposium on Security and Privacy Workshops* conference and published as part of the proceedings.

Scott Harper is a Ph.D. student at Newcastle University's School of Computing and the lead author of the study. He said, "Pet tech such as smart collars and GPS trackers for your cat or dog, is a rapidly growing industry and it brings with it new security, privacy, and safety risks to the pet owners.

"While owners might use these apps for peace of mind about the health of their dog or where their cat is, they may not be happy to find out about the risks the apps hold for their own cybersecurity. We would urge anyone using these apps to take the time to ensure they are using a unique password, check the settings and ensure that they consider how much data they are sharing or willing to share," Harper explained.

Pet tech, the technology in the pet care industry to improve the health, well-being, and overall quality of life of pets, is growing rapidly and includes a wide range of products, including GPS trackers, automatic feeders and pet cameras.

Examples of pet tech include wearable devices that monitor a pet's activity levels, heart rate, and sleep patterns, as well as smart feeding systems that dispense food on a set schedule or in response to the animal's behavior. There are also apps and platforms that allow owners to track and manage their pets' health records and connect with veterinary professionals.

Co-author Dr. Maryam Mehrnezhad, from the Department of Information Security at Royal Holloway, University of London, added, "We are using modern technologies to improve several aspects of our lives. However, some of these (often) cheap technologies come at the price of our privacy, security, and safety. Animal technologies can create complex risks and harms that are not easy to recognize and address. In this interdisciplinary project, we are working on solutions to mitigate such risks an allow the animal owners to use such technologies without

risk or fear."

A second study by the research team included a survey of almost 600 participants from the UK, U.S. and Germany. The researchers asked questions about the technologies used, incidents that have occurred or participants believe may occur, and the methods used by participants to protect their online security and privacy and whether they apply these to their pet tech.

Published in the journal *Proceedings of the 12th International Conference on the Internet of Things*, the findings show that participants do believe that a range of attacks may occur targeting their pet tech. Despite this, they take few precautions to protect themselves and their pets from the possible risks and harms of these technologies.

Co-author, Dr. Matt Leach, Director of Comparative Biology Centre, Newcastle University, added, "We would urge those developing these technologies to increase the security of these devices and applications to reduce risk of their personal information or location being shared."

The researchers urge those who are using pet tech, to ensure they are using a unique password only for that app, check the settings and consider what data they are sharing. Users should be cautious about any new IoT devices they bring into their home. They should download apps associated with animal tech from known app stores and constantly check the permissions of such apps and revoke any unnecessary permission from them. Guides such as [Mozilla's *Privacy Not Included project](#) are available to help inform consumers on the potential [security](#) and privacy risks.