Securing Self-Love through fitness

Office of Information Technology
Division of Information Security
FEBRUARY 2023

February is commonly known as the month of love and on February 14th many Americans celebrate love. The best form of love is self-love and a popular way that most people achieve self-love is through health and fitness.

As many embark on their fitness journey, they will use a fitness watch, tracker, or app to track their goals. These wearable fitness devices are designed to monitor a person's physical ability, sleep quality, and heart rate and to improve athletic performance.

They can not only track our health, but are also connected to other mobile devices and smart homes. They can also be used to make payments. There are many types of wearable devices on the market; the most popular brands are Fitbit, Apple, Samsung Galaxy, and Garmin.

These devices are extremely useful for assisting people to monitor their health and track their fitness goals, but they can pose many security vulnerabilities, risking privacy and exposing personal data.

How are fitness trackers unsafe?

There are multiple ways that your wearable fitness tracker can be compromised, including:

Bluetooth vulnerability: Most wearable fitness devices sync via Bluetooth to smartphones, tablets, and other devices. If a cybercriminal is in close proximity, they can potentially intercept the device using Bluetooth and gain access to sensitive information such as emails, text messages, passwords, or bank information. The cybercriminal can potentially sell this personal and financial data on the black market for a profit.

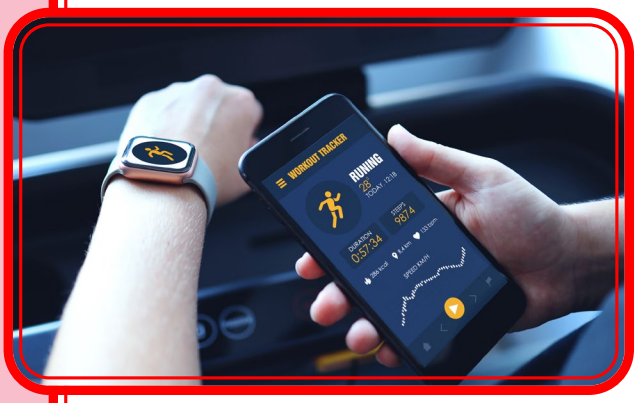
Unsecure app or website: Many wearable fitness devices have a complementary fitness app or link to a website that data is transmitted through. If the website is unsecure, cybercriminals can easily steal the user's personal information. Imposter apps, which mimic legitimate companies like Apple or Amazon, and fake apps can compromise fitness devices with malware to steal the user's confidential information.

Third-party companies: Most wearable fitness devices collect and store user data, and rely on third-party apps to provide additional features. Relying on a third-party app can pose an additional security threat because these apps can experience their own data breaches, exposing users' personal and financial data.

No authentication: Most wearable fitness devices lack any form of authentication, such as a password or pin, which can make it easier for a cybercriminal to access them.

Lack of firmware updates: Some wearable fitness devices are more vulnerable to cybersecurity and malware attacks because they do not have a strong firmware update process. Weak firmware updates call allow criminals to compromise the device and the user's information.

Location: Many wearable fitness devices have an integrated GPS that can track the user's real-time location, including their home address or place of employment. The wearable device could also include detailed maps of saved workout routes, which could be easily accessible to other users and cybercriminals. With this information, cybercriminals can locate the user to either physically attack them or gain access to their home/car to physically steal items while they are away.



Shoulder surfing: The vast majority of users wear fitness devices at the gym, on public transit, or in public places, which creates an additional risk due to shoulder surfers.

How to secure your wearable fitness device

Do your research before purchasing a wearable fitness device. Search the internet for the device or app to obtain a better understanding of what other users have experienced using the device and if there have been any data breaches. Also, read the privacy policies of the device and app before purchasing.

Here are a few tips to ensure your fitness device is secure:

- Always do your research.
- Avoid using unsecure public Wi-Fi for device connections.
- Always opt out of any unauthorized pairing.
- Always opt out of sharing personal information with third-party apps.
- Avoid viewing sensitive messages on your device in public.
- Download apps only from legitimate app stores.
- Always purchase from reputable brands.
- Always create strong passwords and use multi-factor authentication when available.
- Always keep the firmware updated.
- Turn on automatic updates and always keep software updated.

During your self-love journey, make sure you are not only securing your heart, but you are also securing your device. Wearable fitness devices can be extremely helpful on your fitness journey, but remember that they also come with risks. By being aware of the risks that wearable fitness devices pose, you can limit your vulnerability to cybercrime.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.