TECHNOLOGY

How to Protect Your Data in a Connected World

NewsUSA

(NU) - The phrase 'six degrees of separation,' suggests that only a minuscule measurement is what divides one person from another. Today, the Internet of Things (IoT) has decreased those degrees dramatically, connecting us not only to each other, but to everything from our fitness trackers to our coffee makers.

Consider this: according to a recent report by the Federal Trade Commission, the number of Internet-connected devices tops 25 billion worldwide. And that number is expected to double in the next five years, according to experts cited in the report.

In a world where everyone and everything is connected, digital security is a must-have, just as important as the lock on your front door or the keys to your house.

"Technology is revolutionizing the way consumers use cars, homes, work spaces and everyday items," Rep. Darrell Issa, R- Calif., told USA Today in a recent interview. "These devices raise both opportunities and questions about regulatory policy, spectrum space, privacy and more."

Underscoring Issa's concerns are high-profile hacks, including one that took remote control of a Jeep on a busy highway. Experts warn who consumers need to understand that, although convenient, the IoT is an interconnected system, and security is needed to prevent a weakness in one device (like a SmartWatch) from becoming an open door to attack in another device (such as a connected car).

Protecting your privacy has never been more important.

The good news is that sensitive industries such as banking, government, and healthcare have worked with companies like Gemalto, a global leader in digital security, to solve difficult security challenges. While most may not recognize the name "Gemalto," experts say that almost everyone uses at least one or two of the company's solutions, which are embedded in a wide variety of connected devices, credit cards, passports, and ID badges.

So, to ensure that your data is protected from hackers, Gemalto recommends the following tips:

- **Secure the device.** Sensitive devices need an added layer of protection, such as a SIM card or a tamper-resistant Secure Element that stores data in a safe place.
- **Control the access.** Implement two-factor authentication to ensure that only authorized people are granted access to the data.
- **Secure the data.** Ensure that sensitive data is encrypted and that encryption keys are stored in a separate and safe place.