KRACK (Key Re-installation Attacks)

The latest hacking headline

No need to panic.

The attack exploits a flaw in how the WPA2 Wi-Fi encryption system is typically implemented. It essentially tricks devices into reusing what are meant to be onetime encryption settings across multiple messages, making it possible for attackers to decode them.

How to help protect your devices against KRACK

- Wi-Fi users should immediately update their Wi-Fi-enabled devices as soon as a software update is made available. Wi-Fi enabled devices are anything that connects to the Internet — from laptops, tablets, and smartphones to other smart devices such as wearables and home appliances.
- Only browse secure websites whose URL begins with HTTPS. HTTPS-enabled websites provides an extra layer of security by using encryption.
- Consider using a secure Virtual Private Network (VPN), to help protect your data against this new threat.

Note: Changing your Wi-Fi password **will not** prevent attacks

"For most people, just making sure you patch your devices when you can is probably the right answer," says Nikita Borisov, a professor at the University of Illinois at Urbana-Champaign known for his role in finding security flaws

Temporarily switching away from Wi-Fi to wired Ethernet or cellular connections is probably overkill for most users, he says.

Some exceptions for consumers might include internet of things devices in the home—things like music servers and Wi-Fi-enabled lightbulbs—which can lag behind other equipment in deploying encryption, he says.

Of course, those would generally involve less sensitive data than websites or apps.