Protect your Wi-Fi devices from KRACK attacks

A newly discovered security vulnerability found in the Wi-Fi protocol named **KRACK** (**K**ey **R**einstallation **A**tta**ck**s) was recently announced. Anyone who uses a Wi-Fi enabled device could face a risk for sharing unencrypted traffic with potential attackers who bypass WPA2 network security. KRACK targets the third step in a four-way authentication "handshake" performed when your Wi-Fi client device attempts to connect to a protected Wi-Fi network. Attackers who exploit this weakness could steal sensitive data passing through your network including emails, photos, passwords, credit card numbers, chat messages and so on.

Here are some steps you can take to protect yourself from the next KRACK attack:

EXTRA ENCRYPTION

Use a VPN service that you trust to protect your information and data with layers of encryption

HTTPS EXTENSIONS

Stick to websites that uses HTTPS encryption even when surfing from a password protected public Wi-Fi hotspot

UPDATE YOUR DEVICES

Update all your routers and Wi-Fi devices (laptops, phones ...) with the latest security patches

CONSIDER CELLULAR

Disable Wi-Fi on your device and use cellular data to avoid anyone watching your browsing traffic

USE ETHERNET WHEN AVAILABLE

Disable Wi-Fi connection and switch to Ethernet for your essential devices until all your devices are patched

INTERNET-OF-THINGS DEVICES

Disconnect IoT devices such as Google Home from your network until they have been updated by their makers

Safeguard your important data. Always stay vigilant.

A-Speed Infotech Pte Ltd

3 Ang Mo Kio Street 62 #01-46 LINK@AMK (Terrace Building) Singapore 569139

Telephone: +65 6634 1000 Email: sales@aspeed.com.sg

aspeed-infotech-pte-ltd aspeed.infotech

SPEED a-speed infotech pte ltd