





# HOME NETWORK ATTACK




 **John and his family** live in a nice home on a leafy road in the Home Counties.

Give a hacker an inch and they'll rob you blind...

John's broadband router is **clearly visible in a window.** 


 Mark, the hacker, needs to **get a closer look...** 

He waits for an empty driveway and **approaches the house under the guise of a food delivery driver.** 

  
**Access to everything**


With the router type and password **Mark can easily join it.**   

Many of the popular routers have vulnerabilities and the hacker is able **to access all Wi-Fi run devices in the home and monitor their web traffic.**

  
When John checks his online bank account he sees that his money has been **transferred to an unknown source!**


**It's all gone!** 

## HOW TO MANAGE THE RISK

 Check with your broadband provider that the core software or firmware on the router is **the latest version.**

**Ask how to disable WPS** (Wi-Fi Protected Setup), it was supposed to be an easy way to get devices connected to a router. But the push-a-button-to-connect system came with flaws and some routers use the same default digits.

If you use Wi-Fi signal boosters, **check how they connect to your network.**

 **Remove password** from back of router.

 **Change any factory passwords** on your smart home devices.

Keep your broadband router **out of sight** so the password or device is not visible.

Consider smart doorbells to **capture who visits your home** when you are not in (but don't announce that you are not in). 