HOME NETWORK ATTACK



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

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

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

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.**

It's all gone!

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

HOW TO MANAGE THE RISK

Keep all device operating systems, browsers, and mobile apps **updated** with automated security patches.

Create a **separate guest Wi-Fi** network dedicated specifically to Internet of Things and smart home devices to isolate your main computers and personal data.

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.**

Change default administrator passwords on home routers and access points immediately upon setup.

Remove password from back of router.

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).