

ONLINE DATA SHARING

Jeremy, a local businessman, and his family home are **featured in a national magazine article.**

Mark the hacker saw the article. With some research he learnt Jeremy was married with three children and their **social media accounts had limited privacy settings.**

Mark focused on the son's social media posts, he was able to find university information and other facts.

His Instagram told Mark that the family went **skiing to the same place every winter.**

This information allowed him to know **when the house would be empty.**

Posts about sports day told Mark which school the children attend **He was able to confirm patterns and wealth levels.**

A wealth of information

Routines

Posts about horse riding lessons and other leisure activities **showed when the house was empty during the week.**

Using open source data, Mark was able to find **photographs and the floor plan of the family home.**

Planning

In a matter of minutes, Mark has external imagery of the property **he can see all security features present.**

Mark wants to visit in person... **so he pretends to be a delivery driver,** as the homeowner will open the door every time to one.

After checking the response times of the local police, **Mark picks a time** when Jeremy and his family are away **and breaks in.**

HOW TO MANAGE THE RISK

Educate all family members on the risks of oversharing online. Information such as full names, birth dates, locations, and family connections can be harvested for targeted spearphishing or identity fraud.

Establish a family "safe word" or verification protocol to confirm identities in the event of unexpected urgent calls or messages requesting money.

Ensure that you and your family have the appropriate privacy settings enabled on your social media accounts. Different social media channels might require **different levels of privacy. Do you know who is following you online?**

Think twice about posts and photos you're sharing. Make sure none of your sensitive information is in them – driving licences, passports, letters and other documents. Or posts that show you are on holiday, signalling that your home is empty.

When you enter your details to a website or app, **always check the terms and conditions,** and even then, be careful what you're agreeing to others knowing about you or your account.

Consider the amount of information you give Companies House, **don't use your personal address.**

Turn off location tags (geotagging) on apps, cameras and social media uploads on your and your children's mobile devices: anything that might reveal the location. This isn't just about privacy, but also **you and your family's personal safety**.