

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University,
Senior Lecturer

Monday 9th November 2020



Another Chrome zero-day, this time on Android – check your version!

Google is warning users that a Chrome 0-day is being actively exploited. Users are strongly encouraged to update to a safe version. Android users may not have the necessary patch immediately available, in which case an alternative browser should be used (the default browser can be changed but Chrome cannot be uninstalled from Android). [Read here>](#)

NHS data: Can web creator Sir Tim Berners-Lee fix it?

Tim Berners-Lee (founder of the World Wide Web) is working on a solution to problem of storing and managing health records. The prototype web platform, Solid, attempts to walk the fine line between preserving patient privacy and allowing access to healthcare workers that need it. Sir Tim, working with a company called Inrupt, is running a pilot project in Greater Manchester looking to help improve the lives of people suffering from dementia. [Read here>](#)

Covid: Romance fraudsters ‘target lonely’ in lockdown

Romance fraud is on the risk. With people increasingly isolated in lockdown, fraudsters are targeting the lonely trying to extract saving and exploit them as mules in money laundering. Over the summer 600 reports of fraud were made each month to the Action Fraud hotline, up from 400. The average victim lost £10,000. The public have been urged to look for warning signs, such as “too perfect” profile pictures, and to stick to reputable apps and websites. [Read here>](#)

Black Friday – stay safe before, during and after peak retail season

There are going to be a lot of legitimate bargains on offer in the run up to “Black Friday”, both in the USA and around the world. However, there are also going to be many scams trying to entice victims into risky behaviour. Sophos have released some tips to stay vigilant and safe. [Read here>](#)

HMRC smishing tax scam targets UK banking customers

A sophisticated smishing campaign is operating this week, posing as HM Revenue and Customs (HMRC) tax rebate notice. SMS messages are being sent telling recipients that they are eligible for a tax rebate. Anyone clicking on the link is taken to a multi-page form that gathers extensive personal information formatted to convincingly replicate the Gov.UK template. There are also internet bank phishing pages for anyone who enters valid a bank account number and sort code. The article lists the known phishing URLs, but more are being continually deployed as fast as they get taken down. [Read here>](#)