LAI Leading Authorities, Inc.

Graham Cluley

Award-Winning Tech Security Analyst

Targeted Attacks. The glory days of mass-mailed malware, tricking users into believing they were opening a love letter or a photograph of Anna Kournikova are behind us. Today your company is at risk of being hit by carefully-crafted targeted attack, designed with your business in mind to maximise its potential for success.

Drawing upon examples like Sony, TalkTalk, and Ashley Madison, Graham Cluley describes the damage that can be done to corporations—not just through the theft of customer data and intellectual property, but also to a company's brand image. Looking to the future, Graham Cluley discusses how all companies have to be aware that they are potentially fighting a new enemy online—the state-sponsored attacker.

The Rise Of Malware. From back bedrooms to boardrooms, Graham Cluley describes how viruses and trojan horses turned from a schoolboy prank into a threat which could steal secrets from governments, disrupt nuclear facilities in Iran, and even help secret agents assassinate their opponents. Graham Cluley draws on his 25 year history in the anti-virus industry to explain who the malware authors are, how the nature of the attacks are changing, and the steps that organisations need to take to prevent themselves from becoming the next victim.

The Internet Of Insecure Things. More and more household items are being connected to the internet, often with little thought regarding security. If not taken seriously, the threat could even be deadly. In the last few months, we have all read headlines of how Jeeps have been remotely hacked while driving at 70 mph down the motorway, giving attackers the potential ability to kill the brakes, or interfere with the steering. Meanwhile millions of vehicles have been recalled because vehicles are becoming the ultimate mobile device—computers that we sit in.

We wouldn't dream of attaching a desktop computer to the internet without having security in place, so how come everything from internet-connected toothbrushes to smartphone-controlled washing machines and remote control thermostats are fine to plug in?

The truth is that "smart" devices have the potential to be very dumb when it comes to security. Unlike PC and software vendors who have decades of computer security experience, the manufacturers of these new devices often have little in the way of expertise and yet could still be exposing us and our personal data to the threat of hackers. Graham Cluley describes the threat, and calls upon the manufacturers and developers to take the security of these devices more seriously.