



Issued 4/14/17

The Way You Hold Your Phone Could Get You Hacked

Hackers are able to steal PINs and passwords just from the way a mobile phone tilts while being held, new research suggests. Cyber-security experts at Newcastle University have revealed the ease with which malicious websites and apps can spy on us using the motion sensors in our smartphones and tablets. Analyzing the movement of a device as the keyboard was used, they were able to crack four-digit PINs with 70 percent accuracy on the first guess and 100 percent by the fifth guess.

But despite the big players in the industry being aware of the problem, a solution has yet to be found. Lead author Maryam Mehrnezhad, a research fellow in the School of Computing Science, said: "Most smartphones, tablets, and other wearables are now equipped with a multitude of sensors, from the well-known GPS, camera and microphone to instruments such as the gyroscope, rotation sensors and accelerometer. "But because mobile apps and websites don't need to ask permission to access most of them, malicious programs can covertly 'listen in' on your sensor data and use it to discover a wide range of sensitive information about you such as phone call timing, physical activities and even your touch actions, PINs and passwords."

Because there is no uniform way of managing sensors across the industry, the research points toward there being a real threat to personal security.

Mehrnezhad said: “More worryingly, on some browsers we found that if you open a page on your phone or tablet which hosts one of these malicious codes and then open, for example, your online banking account without closing the previous tab, then they can spy on every personal detail you enter. “And worse still, in some cases, unless you close them down completely, they can even spy on you when your phone is locked. “Despite the very real risks, when we asked people which sensors they were most concerned about, we found a direct correlation between perceived risk and understanding. “So people were far more concerned about the camera and GPS than they were about the silent sensors.” The team was able to identify 25 different sensors that came standard on most smart devices and were used to give different information about the device and its user.

The researchers found that each user touch action — clicking, scrolling, holding and tapping — induced a unique orientation and motion trace and so on a known webpage, the team was able to determine what part of the page the user was clicking on and what they were typing.