What can hackers do with your mobile number?

May 3 2021, by Edward Apeh

Credit: Pixabay/CC0 Public Domain

Boris Johnson's personal phone number has been publicly available on the internet for 15 years, it has been revealed. Listed at the bottom of a 2006 press release, the number has reportedly been accessible online

from the time the prime minister was shadow higher education minister through to his rise to Number 10.

That such a high-value mobile number has been publicly available for so long has raised cybersecurity concerns. If hostile states had access to the number, it's possible they could have used it to spy on the prime minister. That would pose a serious security risk to the UK.

Hackers and cybercriminals place a high premium on our mobile phone numbers—with which they can do a lot of damage with very little effort. While there is currently no evidence that Boris Johnson's data and communications have been compromised, having your mobile phone number being freely available significantly increases your vulnerability to cyber-attacks.

Impersonation

One such cyber-attack is the "SIM swap"—a very common technique that's difficult to stop. It's usually used by hackers to exploit a high-value individual's exposed phone number.

SIM swaps see hackers call up the victim's mobile phone provider, impersonating them and requesting to "port-out" the phone number to a different carrier or a new SIM card. They can use other publicly available information—such as the victim's date of birth and their address—to make a more convincing case.

On completion of the port-out, the phone number activates on the attacker's SIM card, and the hacker can send and receive messages and make calls as if they were the victim.

Phone companies have been aware of this problem for years, but the only routine solution they've come up with is offering PIN codes that a

phone owner must provide in order to switch devices. Even this measure has proved ineffective. Hackers can get the codes by bribing phone company employees, for instance.

Access

Once hackers gain control of a phone number, they can then access their online profiles—on Facebook, Twitter, Gmail and WhatsApp—which are all usually linked to the mobile number. All they need to do is ask the social media companies to send a temporary login code, via text message, to the victim's phone.

This was reported to be the case for Twitter CEO Jack Dorsey, whose mobile phone SIM swap resulted in hackers posting offensive messages to millions of his followers. Other high-value individuals have also fallen victim to these kinds of attacks, including the actress Jessica Alba, and online personalities like Shane Dawson and Amanda Cerny.

Aside from posting offensive messages, hackers have been reported to use the accounts to spam, steal identities, access private communications, steal cryptocurrency, and maliciously delete mobile phone data.

Surveillance

Hackers can also use another even simpler method to attack a phone—though some advanced spyware is needed to make the attack stick. Hackers armed with someone's phone number can send them a text message with a hyperlink within it. If clicked, the link allows spyware to infiltrate the phone, compromising much of its data.

It appears this method was used to infiltrate and spy on Jeff Bezos'

phone in 2020, after reports found it to be "highly probable" that a text sent from Mohammed bin Salman, the crown prince of Saudi Arabia, delivered the spyware to Bezos' phone. Similar spyware has been used to monitor the phones of journalists and human rights activists.

It is possible that Boris Johnson's mobile phone has never been hacked, in spite of the 15 years that his number was freely available online. However, seeing as the exposed phone numbers of high-value individuals can be taken advantage of by criminals or hackers from hostile states, tight new security measures should be put in place to avoid such an oversight happening again.

Provided by The Conversation