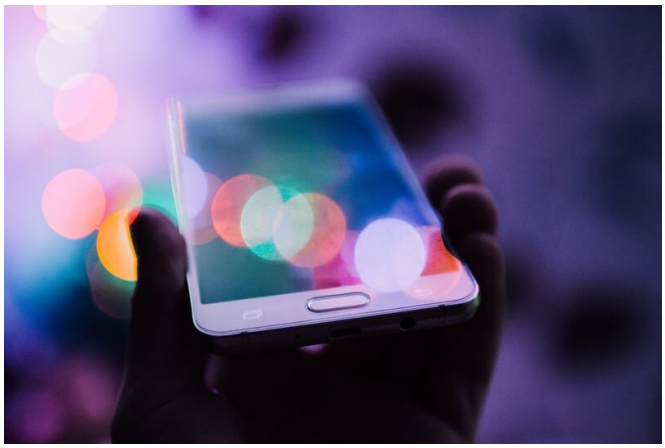
Your old mobile phone number could compromise your cybersecurity

10 May 2021, by Sarah Katz



Mobile phone. Credit: Unsplash

The Department of Computer Science and Center for Information Technology Policy at Princeton University has conducted a study and released a paper assessing the security and privacy risks of phone number recycling by mobile characters in the United States.

Such a risk could pose a threat to many users, as every time you change your mobile phone number, your carrier will recycle your previous number. They 'recycle' the number by assigning it to a new phone and corresponding customer. The carriers report doing this in order to avoid 'number exhaustion,' or a situation where all possible numbers have already been used for each mobile phone.

The problem arises, however, when these recycled phone numbers actually end up granting new customers access to the private information of previous phone users. This means that, in the hands of a new customer who decides to hack into a phone, a recycled number could pose untellable security risks for many users.

For example, the Princeton study cites one instance wherein a new user of a phone received multiple text updates regarding a previous user's medical information and upcoming spa appointments. While not necessarily dangerous in the hands of a non-malicious user, this information still constitutes personal user information not intended for the phone's current customer.

Indeed, although many users implement two-factor authentication for their mobile phones, recycled phone numbers don't always clear or entirely update data. This means that a phone with a recycled number might still allow a user access to a previous customer's email and social media accounts.

Moreover, because many people often use phone numbers as login credentials to personal platforms, any cross-reference of phone numbers with people search database websites such as BeenVerified or Intelius as well as passwords from largescale data breaches could yield access to a plethora of additional private information.

In fact, the researchers discovered that 66 percent of recycled numbers sampled still had connections to the online accounts of previous customers. Furthermore, out of 259 surveyed phone numbers, 215 had been recycled and remained vulnerable to at least three types of attacks. They further report that of 200 recycled numbers assessed over one week, 19 of them still received private messages and sensitive calls intended for previous owners.

Additionally, the researchers at Princeton stated that while mobile carriers such as T-Mobile and Verizon released documentation notifying users of this security risk, neither company appears to have taken any steps on the backend to make prevent attacks going forward.

More information: Lee, K., and Narayanan, A. "Security and Privacy Risks of Number Recycling at

Mobile Carriers in the United States." Department of Computer Science and Center for Information Technology Policy Princeton University, Princeton University, 3 May 2021, recyclednumbers.cs.princeton.e … d-numbers-latest.pdf