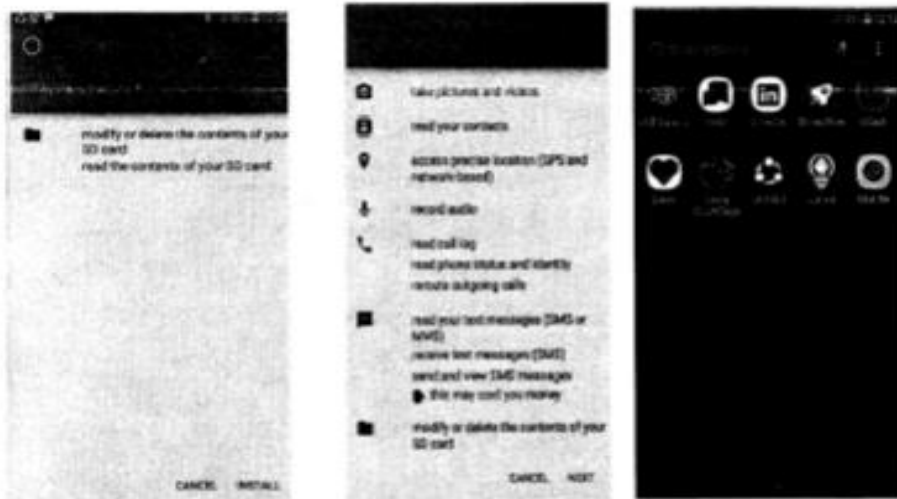


COVID-19 പ്രതിരോധിക്കുന്നതിനും, രോഗലക്ഷണമുള്ള ആളുകളെ കണ്ടെത്തുന്നതിനുമായി കേന്ദ്ര സർക്കാർ വികസിപ്പിച്ച് പുറത്തിറക്കിയ മൊബൈൽ അപ്ലിക്കേഷനായ 'Arogya sethu' മൊബൈൽ അപ്ലിക്കേഷന്റെ വ്യാജ ലിംഗുകൾ ഇന്ത്യയിൽ ഉപയോഗിച്ച് വരുന്ന സ്റ്റാർട്ടപ്പോണുകളെ ലക്ഷ്യം വെച്ച് വിദേശരാജ്യങ്ങളിൽ പ്രവർത്തിക്കുന്ന തീവ്രവാദസംഘടനകൾ നിർമ്മിച്ച് അയച്ച് സ്വകാര്യ വ്യക്തി വിവരങ്ങളും, രാജ്യരക്ഷ വിവരങ്ങളും ചോർത്തുവാൻ ശ്രമിക്കുന്നതായി അറിയാൻ സാധിച്ചിട്ടുണ്ട്. വ്യാജ 'Arogya sethu' അപ്ലിക്കേഷന്റെ ലിംഗുകളിൽ ക്ലിക്ക് ചെയ്യുന്നവരിൽ malicious അപ്ലിക്കേഷനായ Chat me appലേക്ക് direct ചെയ്യുകയും. ആയത് മെബൈൽ ഫോണുകളിൽ download ചെയ്യുന്നതിലൂടെ പ്രസ്തുത മൊബൈലിന്റെ access ഡീറ്റേൽസും, ഡാറ്റ പുറന്തള്ളുവാനുള്ള പവറും ഹാക്കേർസിന് ലഭിക്കുന്നു.

Malicious app ആയ Chat Me appന്റെ Screen shotകൾ



ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

1. SMS or Whatsapp or message എന്നിവയിലൂടെ വരുന്ന Arogya Sethu app ന്റെ ലിംഗുകൾ ഉടൻ തന്നെ delete ചെയ്തു കളയുക.
2. അബദ്ധവശാൽ malicious ലിംഗുകളിൽ ക്ലിക്ക് ചെയ്തവർ
  - a. മൊബൈൽ device ഫാക്ടറി റീസെറ്റ് ചെയ്യുക.
  - b. Internet serviceലൂടെ ഉപയോഗിച്ച് വരുന്ന എല്ലാ പാസവേർഡുകളും മാറ്റംവരുത്തുക.
  - c. Operating System, Security apps എന്നിവ update ചെയ്യുക.
3. പൊതുജനങ്ങൾ ഗൂഗിൾ പ്ലേ സ്റ്റോർ. ആപ്പിൾ സ്റ്റോർ. എന്നിവയിലൂടെ ലഭിക്കുന്ന official Arogya sethu അപ്ലിക്കേഷനുകൾ മാത്രം മൊബൈലുകളിൽ ഡൗൺലോഡ് ചെയ്യുവാൻ ശ്രദ്ധിക്കുക. ആയതിന്റെ ലിംഗുകൾ

For iPhone users

<https://apps.apple.com/in/app/aarogyasetu/id1505825357>

For Android based smartphones users

<https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu>