# Gaming and Social Media

***Slide 1***

## ഗെയിമിംഗ്

ഇനി നിങ്ങളിൽ പലവർക്കും ഇഷ്ടമുള്ള ഒരു Topic-നെ കുറിച്ച് സംസാരിക്കാം, ഗെയിമിംഗ്. നിങ്ങളിൽ മിക്കവരും കമ്പ്യൂട്ടർ ഗെയിംസ് കളിക്കുന്നുണ്ടാകും അല്ലെ? നിങ്ങൾ അത് നന്നായി ആസ്വദിക്കുന്നുണ്ടാകും അല്ലെ? നിങ്ങളിൽ എത്രപേർക്കു അറിയാം ഗെയിം കളിക്കുന്നത് നമ്മുടെ പലതരം കഴിവുകളെ ഉദ്ബോധിപ്പിക്കും എന്നത്. കമ്പ്യൂട്ടർ ഗെയിംസ്ന്റെ കുറച്ചു ഗുണങ്ങൾ നമുക്ക് പരിശോധിക്കാം.

## ഗെയിമിംഗ്ൻറെ നല്ല വശങ്ങൾ

***Slide 2, 3***

- പ്രശ്നങ്ങൾ പരിഹരിക്കാനുള്ള കഴിവ്
- നിങ്ങളുടെ ബുദ്ധിവികാസത്തിനും നിങ്ങളിലെ ഭാവന വർധിപ്പിക്കാനും ഒരു പരിധി വരെ കമ്പ്യൂട്ടർ ഗെയിംസ് സഹായിക്കുന്നതാണ്.
- കണ്ണുകളും കൈകളും  തമ്മിലുള്ള ആശയവിനിമയം വർധിപ്പിക്കുന്നു

  നിലവിൽ ലഭ്യമായ പല ഗെയിംകളും കളിക്കുക വഴി കുട്ടികൾക്ക് hand - eye co-ordination വർധിപ്പിക്കുവാൻ കഴിയുന്നതാണ്.
- കമ്പ്യൂട്ടർ ഗെയിംസ് കളിക്കുന്നവരിൽ സൂക്ഷ്മ നിരീക്ഷണവും ചിന്താശകതിയും മുൻപത്തെ തലമുറയെക്കാളും കൂടുതലാണെന്നു പഠനം തെളിയിക്കുന്നു.
- ആസൂത്രണം, വിഭവ ക്രമീകരണം

ഒരു ഗെയിം കളിക്കുമ്പോൾ പരിമിതമായ മാർഗങ്ങൾ ഉപയോഗിച്ച് ആസൂത്രണം ചെയ്തു വിജയിക്കാൻ ശ്രമിക്കുമ്പോൾ നമ്മളിലെ ബുദ്ധിസാമർഥ്യം വർധിപ്പിക്കുവാൻ സഹായിക്കുന്നു. ശരിയായ തീരുമാനങ്ങൾ പെട്ടെന്നു എടുക്കുവാനുള്ള കഴിവ് ഗെയിംസ് കളിക്കുന്നവരിൽ കൂടുതലായി കാണപ്പെടുന്നു

***Slide 4***

ഗുണങ്ങൾ ഉണ്ടെങ്കിലും തുടർച്ചയായും അനിയന്ത്രിതമായും ഗെയിംസ് കളിക്കുന്ന പല കുട്ടികളിലും ഉറക്കക്കുറച്ചിലും, ക്ഷീണവും തളർച്ചയും കണ്ടു വരുന്നു. അവർ സമൂഹത്തിൽ നിന്നും പിന്തിരിയാനുള്ള പ്രണവത കൂടിവരുന്നു.
കമ്പ്യൂട്ടർ ഗെയിംസ് കളിക്കുന്നവരുടെ തലച്ചോറിൽ റെസ്പോൺസ് റീവാർഡ് എന്നിവ കൂട്ടിയിണക്കുന്ന stratium എന്ന ഭാഗം വളരെ പ്രവർത്തനക്ഷമമായി കാണപ്പെടുന്നു. എന്നാൽ അവരുടെ hippocampus, വളരെ ദുർബലമായിരിക്കും. ഈ ഭാഗമാണ് ബന്ധങ്ങളെ കുറിച്ചുള്ള ഓർമ്മകൾ ഉണ്ടാക്കുന്നത്. ഇത് തലചോറിൻറെ പൊതുവായ പ്രവർത്തനത്തെ വിപരീതമായി ബാധിക്കുകയും പിൽക്കാലത്തു alzheimer's schizophrenia പോലുള്ള രോഗങ്ങൾക്ക് കാരണമാകുകയും ചെയ്യുന്നു

## ഗെയ്മിങ്ങിന്റെ ദൂഷ്യ വശങ്ങൾ

***Slide - 5***

ഇപ്പോൾ സുലഭമായ 90 % ഗെയിംസ്കളും അക്രമാസക്തമാണ്. ഇത് കുട്ടികളിലെ ചിന്താശകതിയെ തെറ്റായ രീതിയിൽ വളർത്തും, കൂടാതെ കുട്ടികളിൽ പലരും ഗെയിംസിൽ കാണുകയും ചെയ്യുകയും ചെയ്യുന്ന കാര്യങ്ങൾ യഥാർത്ഥ ജീവിതത്തിലും ചെയ്യാൻ ശ്രമിക്കുന്നു

അമിതമായ ഗെയിമിംഗ് ശീലം പല ശാരീരിക ബുദ്ധിമുട്ടുകൾക്ക് കാരണമായേക്കും
ഇനി നമുക്കു അമിതമായ ഗെയിമിംഗ്ൻറെ ദൂഷ്യങ്ങൾ നോക്കാം

- കഴുത്തുവേദന, നടുവേദന, തോൾ സംബദ്ധമായ പ്രശനങ്ങൾ.
- മറ്റു കളികളിൽ ഏർപെടാതിരിക്കുന്നതു കുട്ടികളുടെ ശരിയായ വളർച്ച കുറക്കുന്നതും, ബുദ്ധിവികാസത്തിന് തടസമായേക്കും, പെരുമാറ്റ സംബന്ധിച്ച പ്രശ്നങ്ങൾ വർധിക്കും.
- ഇതിനെല്ലാം പുറമെ അമിത വണ്ണത്തിനും അനിയന്ത്രിതമായ ഗെയിമിംഗ് കാരണമാകുന്നു

വീഡിയോ ഗെയിമിംഗ് യിലുള്ള ലഹരി കുട്ടികളിലെ പാഠ്യേതരമായ വാസനകളെയും മറ്റു കളികളിലുള്ള താല്പര്യം കുറക്കുന്നു

മണിക്കൂറുകളോളം ഗെയിം കളിക്കുന്നത് കുട്ടികളിലെ അമിതവണ്ണത്തിന് കാരണമാകുന്നു, കാരണം മറ്റു കളികളിൽ ഏർപ്പെടുന്നില്ല.

കണ്ണ് സംബദ്ധമായ രോഗങ്ങളും, കൈ കുഴകുള്ള വേദന, കൈകാലുകൾക്കുള്ള വേദന ഇവയെല്ലാം ഗെയിം യിലുള്ള അമിതമായ ആസക്തി ഉള്ള കുട്ടികളിൽ കണ്ടുവരുന്നു.

Carperl-Tunnel Syndrome, കൈക്കുഴയിൽ അനുഭവപ്പെടുന്ന വേദനയും മരവിപ്പും ആവശ്യത്തിലധികം നേരം കമ്പ്യൂട്ടർ ഉപയോഗിക്കുന്നതിന്റെ പാർശ്വഫലം ആണ്.

ഗെയിംനു വേണ്ടി കുറയെ സമയം ചിലവഴിക്കുമ്പോൾ നമ്മുടെ കുട്ടികൾ കുടുംബബന്ധങ്ങളും സുഹൃത്ത്ബന്ധങ്ങളും മനസിലാകാതെ പോകുന്നു. അവർക്ക് പലപ്പോഴും ബന്ധുക്കളുടെ കൂടെയും സുഹൃത്തുക്കളുടെ കൂടെയും സമയം ചിലവഴിക്കുന്നത് ഇഷ്ടമില്ലാതെ വരുന്നു.

അക്രമവാസനയുള്ള ഗെയിംകൾ നമ്മുടെ കുട്ടികളെ തെറ്റായ ദിശയിൽ വളരാൻ പ്രേരിപ്പിക്കുന്നുണ്ടെന്ന് പഠനങ്ങൾ പറയുന്നു.

മണിക്കൂറുകളോളം ഗെയിം കളിക്കുന്നത് നമ്മുടെ കുട്ടികളുടെ കഴിവുകൾ ശോഷിപ്പിക്കുന്നതാണ്, ഏകാഗ്രത കുറവും ആവശ്യത്തിനുള്ള ഉറക്കമില്ലാതിരിക്കുന്നതും ഒടുവിൽ പരിക്ഷകളിലെ മോശം പ്രകടനത്തിന് വഴി തെളിക്കുന്നു.

ഇതുകൊണ്ടെല്ലാം നമ്മുക്ക് നമ്മളെ ബാധിക്കാതെ ആസ്വദിക്കുന്ന രീതിയിൽ ഗെയിം കളിക്കുന്നതാണ് ഉചിതം.

## ഗെയ്മ്സിന്റെ സ്രോതസ്സുകൾ

***Slide - 6***

ഇനി എങ്ങനെയെല്ലാം ഗെയിംസ് നമുക്ക് കിട്ടുന്നു എന്ന് നോക്കാം

### *Boxed Games*

ഓൺലൈൻ വഴിയോ അല്ലെങ്കിൽ സ്റ്റോറുകൾ വഴിയോ ഗെയിം സിഡികൾ വാങ്ങി നമുക്ക് നമ്മുടെ കംപ്യൂട്ടറുകളിലോ ഗെയിം കൺസോളികളിലോ കളിക്കാവുന്നതാണ്.

### *Digital Download*

നമ്മുക്ക് ഗെയിമുകൾ നേരിട്ട് ഇന്റർനെറ്റ് ൻറെ സഹായത്തോടു കൂടി ഡൌൺലോഡ് ചെയ്തു നമ്മുടെ കംപ്യൂട്ടറുകളിലോ ഗെയിം കൺസോളികളിലോ കളിക്കാവുന്നതാണ്.

### *Mobile storefronts*

മൊബൈലോ ടാബ്ലെറ്റോ ഉപയോഗിക്കുന്നവർക്ക് അതാതു മൊബൈൽ store place -ൽ നിന്ന് ഗെയിം ഡൌൺലോഡ് ചെയ്യാവുന്നതാണ്.

### *Subscription*

ഒരു സൈറ്റിൽ അക്കൗണ്ട് ക്രിയേറ്റ് ചെയ്തു പണമടച്ചു അല്ലെങ്കിൽ ഒരു സമയപരിധി വരെ ഫ്രീ ആയിട്ടോ സബ്സ്ക്രൈബ് ചെയ്തുകൊണ്ട് ഗെയിമുകൾ കളിക്കാവുന്നതാണ്.

### *Freemium*

ഇങ്ങനെ ഉള്ള ഗെയിംകളിൽ പരസ്യങ്ങൾ ഉണ്ടാകും; അല്ലെങ്കിൽ ഗെയിംൻറെ ഒരു ഭാഗം മാത്രമേ ഫ്രീ ആയിട്ട് കളിക്കാൻ പറ്റൂ. ഗയിം മുഴുവനായി കളിക്കാൻ നമുക്ക് പണമടക്കേണ്ടി വരും.

### *സോഷ്യൽ networking ഗെയിംസ്*

ഇവ ഫേസ്ബുക്കിൽ അല്ലെങ്കിൽ മറ്റെന്തെങ്കിലും സോഷ്യൽ networking-ന്റെ സഹായത്തിൽ കളിക്കാൻ പറ്റുന്നതാണ്. ഇവയിൽ നമ്മുടെ ഗെയിമിന്റെ സ്റ്റാറ്റസുകൾ നമ്മുടെ ഫ്രണ്ട്സ്നു കാണാൻ പറ്റുകയും നമുക്കു ഫ്രണ്ട്- നെ കളിക്കാൻ ക്ഷണിക്കാൻ പറ്റുകയും ചെയ്യും.

## ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

### ***Slide - 7***

ഇനി ഗെയിംസ് കളിക്കുമ്പോൾ ശ്രദ്ധിക്കേണ്ട കുറച്ചു കാര്യങ്ങൾ

### ***Slide – 8***

ഗെയിമിംഗ് മെഷീൻ Updated ആക്കി വെക്കുക: കമ്പ്യൂട്ടറുകളെ തകരാറിലാക്കുന്ന പ്രോഗ്രാമുകളും വൈറസുകളും നിന്നും സുരക്ഷണം നൽകുക, ആന്റി വൈറസ് സോഫ്റ്റ് വെയർ ഇൻസ്റ്റാൾ ചെയ്തു സമയാസമയം അപ്ഡേറ്റ് ചെയ്യുക.

Password വാക്യങ്ങളിൽ നിന്ന് ഉണ്ടാക്കുക: ശക്തമായ പാസ്സ്വേർഡ് നു 12 അക്ഷരമെങ്കിലും ഉണ്ടാകും. നിങ്ങൾക്കു ഓർത്തുഎടുക്കാൻ പറ്റുന്ന ഒരു വാക്യത്തിൽ നിന്ന് Password ഉണ്ടാക്കാൻ ശ്രമിക്കുക.

തുറന്നു പറയുക: ഗെയിമിങ് ഗ്രൂപ്പിൽ നിങ്ങൾക്കു എന്തെങ്കിലും ബുദ്ധിമുട്ടു ഉണ്ടെകിൽ, ആരെങ്കിലും നിങ്ങളെ ബുദ്ധിമുട്ടിക്കുന്നുണ്ടെങ്കിൽ മുതിർന്നവരോട് പ്രയാസങ്ങൾ തുറന്നു പറയുക.

*Cyber Bullying*

ഭീഷണികളും തരം താഴ്ത്തലുകളും റിപ്പോർട്ട് ചെയ്യുക: നിങ്ങളെ ശല്യപെടുത്തുന്നവരെ എങ്ങനെ ബ്ലോക്ക് ചെയ്യാമെന്നും അവർക്കു എതിരെ എങ്ങനെ റിപ്പോർട്ട് ചെയ്യാമെന്നും പഠിച്ചു വയ്ക്കുക.

സ്വകാര്യ വിവരങ്ങൾ സംരക്ഷിക്കുക: നിങ്ങളുടെ യഥാർത്ഥ പേരോ, വിലാസമോ, ഫോട്ടോകളോ അപരിചിതരുമായി കൈമാറാൻ പാടില്ല. നിങ്ങളുടെ യഥാർത്ഥ പേരുപയോഗിക്കാതെ മറ്റൊരു പേര് ഉപയോഗിക്കുക. യഥാർത്ഥ ഫോട്ടോക്ക് പകരം അവതാർ ഉപയോഗിക്കാവുന്നതാണ്

വ്യക്തിത്വം സംരക്ഷിക്കുക: നിങ്ങൾ കളിച്ചുകൊണ്ടിരിക്കുമ്പോൾ വോയിസ് ചാറ്റ്, വീഡിയോ ചാറ്റ് എന്നിവ ഉപയോഗിക്കാതെ ഇരിക്കുക.

സമയ നിയന്ത്രണം: ഗെയിം കളിക്കാനായി ഒരു സമയ ക്രമം നിശ്ചയിക്കുക.

അപരിചിതർ നൽകുന്ന ഡൌൺലോഡ് ലിങ്ക് തുറക്കാതെ ഇരിക്കുക: ഇതുവഴി അവർ നമ്മുടെ കംപ്യൂട്ടറുകളിൽ വൈറസുകൾ വ്യാപിപ്പിക്കുവാൻ കഴിയും.

ഗെയിമിംഗ് ലോകത്തിൽ വച്ച് പരിചയപ്പെടുന്നവരുമായി നേരിട്ട് കാണാനുള്ള സാഹചര്യങ്ങൾ ഒഴിവാക്കുക.

Be a good digital citizen

റിസ്ക് കളെ കുറിച്ചുള്ള അവബോധം, കാര്യങ്ങൾ നല്ലതായി നിർണയിക്കാനുള്ള കഴിവ്, എന്നിവ ഇപ്പോഴും ഉണ്ടായിരിക്കണം

Entertainment റേറ്റിംഗ് സോഫ്റ്റ്വെയർ ബോർഡ് ൻറെ നല്ല റേറ്റിംഗ് ഉള്ള ഗെയിമുകൾ തിരഞ്ഞെടുക്കണം.

വീടുകളിൽ കംപ്യൂട്ടറുകൾ പരമാവധി Open ആയുള്ള സ്ഥലങ്ങളിൽ വയ്ക്കുക.

ശരിയായ രീതിയിൽ സമയ നിക്ഷിപ്തമായി ഉപയോഗിച്ചാൽ ഗെയിമിംഗ് നല്ലതു തന്നെ. പക്ഷെ അത് നമ്മുടെ ജീവിതത്തെയും ആരോഗ്യത്തെയും ബാധിക്കാതിരിക്കാൻ ശ്രദ്ധിക്കുക

# Social Media

## ***Slide – 9, 10***

ഇനി നിങ്ങൾക്കു താല്പര്യം ഉള്ള മറ്റൊരു വിഷയം, Social Media. നിങ്ങൾക്കു facebook, whatsapp എല്ലാം സുപരിചിതം അല്ലെ? ഇതൊക്കെ ഉപയോഗിക്കാറുണ്ടോ? സോഷ്യൽ മീഡിയയെ പറ്റി വേറെ എന്തൊക്കെ നിങ്ങൾ കേട്ടിട്ടുണ്ട്?

എന്താണ് സോഷ്യൽ മീഡിയ എന്ന് നിങ്ങൾക്കു അറിയാമോ?

ഇന്റർനെറ്റ് ഉപയോഗിച്ചു ആശയവിനിമയം നടത്തുവാനും, ചർച്ചകൾ നടത്തുവാനും ഉള്ള ഒരു മാധ്യമം ആണ് സോഷ്യൽ മീഡിയ അഥവാ സാമൂഹ്യമാധ്യമം.

നമുക്ക് Information പങ്കുവയ്ക്കാനും കൈമാറാനും ആശയങ്ങളും ജോലിസാധ്യതകളും പങ്കുവയ്ക്കാനും ചിത്രങ്ങൾ വിഡിയോകൾ എന്നിവ കൈമാറാനും പങ്കുവയ്ക്കാനും social media സഹായിക്കും.

## ***Slide 11***

സോഷ്യൽ മീഡിയയുടെ നേട്ടങ്ങൾ എന്തൊക്കെ ആണെന്ന് നിങ്ങൾക്കു അറിയാമോ?

ഫേസ്ബുക്ക് അടക്കമുള്ള സോഷ്യൽ നെറ്റ്വർക്കിംഗ് വെബ്സൈറ്റുകൾ വ്യക്തികളുടെ സാമൂഹികജീവിതത്തെ പല രീതിയിലും സ്വാധീനിച്ചിട്ടുണ്ട്. മുറിഞ്ഞു പോയ സൗഹൃദങ്ങളെയും ബന്ധങ്ങളെയും കൂട്ടി യോജിപ്പിക്കുവാൻ ഫേസ്ബുക്കിന് സാധിക്കാറുണ്ട്. ഉദാഹരണത്തിന്, ജോൺ വാട്സൺ എന്ന വ്യക്തിക്ക് 20 വർഷം മുൻപ് നഷ്ടപ്പെട്ട തന്റെ മകളെ അവളുടെ ഫേസ്ബുക്ക് പ്രൊഫൈൽ വഴി കണ്ടെത്തുവാൻ സാധിച്ചത് അത്തരത്തിലുള്ള ഒരു സംഭവമാണ്.

1. Worldwide connectivity: ലോകത്തിലെ ഏതു കോണിലുള്ള സുഹൃത്തുക്കളെ കാണുവാനും, അവരുമായി ആശയവിനിമയം നടത്തുവാനും സഹായിക്കുന്നു

2. commanality of interest (പൊതുവായ താല്പര്യങ്ങൾ): സോഷ്യൽ മീഡിയ ഉപയോഗിക്കുന്നതിലൂടെ നിങ്ങളുടെ അഭിരുചികൾക്കു അനുസ്യൂതമായ ഒരു സൗഹൃദ കൂട്ടായ്മ രൂപപ്പെടുത്താൻ നിങ്ങൾക്ക് സാധിക്കും.

3.തത്സമയ വാർത്താ വിനിമയം: സോഷ്യൽ നെവർകിങ് സൈറ്റുകളിലൂടെ തത്സമയം ഈ ലോകത്തിലെ ഏതു കോണിൽ നടക്കുന്ന സംഭവ വികാസങ്ങളും ഞൊടിയിടയിൽ അറിയാൻ നിങ്ങൾക്കു സാധിക്കും.

4. ബിസിനസ് വിപുലീകരണം:നമ്മുടെ ബിസിനസ്സിന്റെ വിപുലീകരണത്തിനും വേണ്ടി സോഷ്യൽ മീഡിയ ഉപയോഗിക്കാം.

## ***Slide 12***

പക്ഷെ സോഷ്യൽ മീഡിയ ഉപയോഗിക്കുമ്പോൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ പലതുമുണ്ട്:

- സോഷ്യൽ മീഡിയയിൽ നിന്നും കിട്ടുന്ന വിവരങ്ങളെ നിങ്ങൾ അന്തമായി ഒരിക്കലും വിശ്വസിക്കരുത്, അത് എപ്പോഴും സത്യം ആകണം എന്നില്ല.

- നമ്മുടെ ഡയറിയിൽ എഴുതുന്നത് പോലെ വ്യക്തിപരമായ കാര്യങ്ങൾ സോഷ്യൽ മീഡിയയിൽ എഴുതുന്നത് പ്രോത്സാഹനീയം അല്ല

- ആവശ്യമില്ലാത്ത കാര്യങ്ങൾ forward ചെയ്യാൻ ശ്രമിക്കാതിരിക്കുക

- നിങ്ങൾ ചെയ്യുന്ന എല്ലാ കാര്യങ്ങളും സോഷ്യൽ മീഡിയയിൽ പോസ്റ്റ് ചെയ്യേണ്ട ആവശ്യം ഇല്ല

### Types of Social Media

## ***Slide 13***

സോഷ്യൽ മീഡിയയെ പല വിധത്തിൽ തരംതിരിക്കാം.

*Social News Site and book marking Sites*- ഇതിൽ user നു അവരെഴുതിയ ലേഖനങ്ങൾ പോസ്റ്റ് ചെയ്യുകയും മറ്റുള്ളവർക്ക് അത് വായിച്ച ശേഷം rate ചെയ്യുകയും ചെയ്യാം .ഉദാഹരണത്തിന്: digg, reddit

*ബ്ലോഗ്,മൈക്രോബ്ലോഗ്*- ഇതിൽ user നു വളരെ ചെറിയ കുറിപ്പുകൾ കൈമാറാം Ex:Twitter ,tumbler

*സോഷ്യൽ നെറ്റ്വർക്കിംഗ് സൈറ്റ്* - ഒരേ പോലെ ചിന്തിക്കുന്നവർക്ക് അവരുടെ ആശയങ്ങൾ പറയാനും ചർച്ചചെയ്യാനും പറ്റുന്ന സൈറ്റ് ആണ് ഇവ. Ex Facebook, google+

*മീഡിയ sharing സൈറ്റ്* - നമ്മൾ എടുക്കുന്ന ചിത്രങ്ങളും വീഡിയോസും മറ്റുള്ളവരുമായി ഷെയർ ചെയ്യാൻ പറ്റുന്ന സൈറ്റ് ex: youtube, Instagram.

*Virtual World*: ഇതിൽ user നു ഒരു സാങ്കല്പിക ലോകം തന്നെ ലഭിക്കും. അവർക്കു അവരുടേതായ identity ഉണ്ടാക്കാനും ജീവിക്കാനും സാധിക്കും.

## ***Slide 14***

സോഷ്യൽ മീഡിയ ഉപയോഗിക്കുമ്പോൾ നമ്മൾ ഉറപ്പുവരുത്തേണ്ട കാര്യങ്ങൾ

ഇനി പറയുന്ന കാര്യങ്ങൾ ഒരിക്കലും പങ്കുവെക്കാതിരിക്കാൻ ശ്രദ്ധിക്കുക,

- നിങ്ങളുടെ contact Information.
- എല്ലാവരുമായി പങ്കുവെക്കാൻ നിങ്ങൾ ആഗ്രഹിക്കാത്ത ചിത്രങ്ങൾ
- നിങ്ങളുടെ വിദ്യാലയത്തെകുറിച്ചോ ജോലിയെക്കുറിച്ചോ ഉള്ള വിവരങ്ങൾ
- നിങ്ങളുടെ യാത്ര പ്ലാനുകൾ.
- നിങ്ങളുടെ സ്വത്തുവിവരങ്ങൾ.
- സുഹൃത്തുക്കളുടെ മോശമായ ചിത്രങ്ങൾ.
- ചെയിൻ സ്റ്റാറ്റസ് updates.

എപ്പോളും ഓർക്കുക Social media-യിൽ,

1) നമ്മുടെ സംഭാഷണങ്ങൾ ഒന്നും സ്വകാര്യമല്ല.
2) അപരിചിതരെ ഒരിക്കലും ആഡ് ചെയ്യരുത്.
3) നിങ്ങളുടെ അക്കൗണ്ടൻറെ privacy setting public ആക്കരുത്.
4) എല്ലാ പോസ്റ്റുകളിലും കമന്റ് ചെയ്യരുത്.
5) അപ്രസക്തമായ പോസ്റ്റുകളിൽ സുഹൃത്തുക്കളെ ടാഗ് ചെയ്യരുത്.
6) ഗെയിം ഇൻവിറ്റേഷനുകളോ അപ്പ്ലിക്കേഷനുകളോ ആവശ്യമില്ലാതെ അയക്കരുത്.

## ***Slide 15***

എന്തെല്ലാമാണ് social media വരുത്തി വെക്കുന്ന ഹാനികൾ

- *വൈകാരികതയുടെ അഭാവം*: സോഷ്യൽ മീഡിയ വഴിയുള്ള സംഭാഷണങ്ങളിൽ മറ്റൊരാളുടെ യഥാർത്ഥ വികാരങ്ങൾ മനസിലാക്കാൻ സാധിക്കുകയില്ല.
- *വേദനിപ്പിക്കാനുള്ള അനുവാദം*: മുഖാമുഖമുള്ള സംസാരം അല്ലാത്തതിനാൽ ഒരു വ്യക്തിയെ വേദനിപ്പിച്ചിട്ടു എളുപ്പം രക്ഷപ്പെടാൻ സാധിക്കും.
- *മുഖാമുഖ സംഭാഷണങ്ങളുടെ കുറവ്*: കംപ്യൂട്ടറിനോടുള്ള അമിതമായ ആശ്രയം face-2-face സംഭാഷണത്തിനുള്ള ഒരു വ്യക്തിയുടെ കഴിവിനെ സാരമായി ബാധിക്കും.

എന്തെങ്കിലും കേട്ടുകഴിഞ്ഞാൽ അതിനു മറുപടി കൊടുക്കുന്നത് അയാൾക്കു വളരെ അസാധാരണമായി അനുഭവപ്പെടും.

- *തെറ്റായ പ്രതിച്ഛായ*: നമ്മളുടെ പെർഫെക്റ്റ് ആയിട്ടുള്ള ചിത്രങ്ങളും, നല്ല വാർത്തകളും മാത്രം നമ്മൾ പോസ്റ്റ് ചെയുന്നു. നമ്മുടെ ജീവിതത്തിലെ പരാജയങ്ങളും ദുഖങ്ങളും എപ്പോളും മറച്ചുവെക്കാൻ ശ്രമിക്കുന്നു. ഇതിലൂടെ നാം എപ്പോഴും പെർഫെക്റ്റ് ആണെന്ന് വരുത്തി തീർക്കാൻ നമ്മൾ ശ്രമിക്കുന്നു
- *കുടുംബബന്ധങ്ങളുടെ തകർച്ച:* Facebook, ടിറ്റെർ, ജിമെയിൽ തുടങ്ങിയ അപ്പ്ലിക്കേഷനിലൂടെയുള്ള ആശയവിനിമയം വഴി നമ്മൾ കുടുംബബന്ധങ്ങളിൽ നിന്നും ഊഹിക്കുന്നതിനേക്കാൾ കൂടുതൽ അകലുന്നു.

## ***Slide 16***

ഇനി വളരെ പ്രചാരത്തിൽ ഇരിക്കുന്ന 2 സോഷ്യൽ മീഡിയ അപ്പ്ലികേഷണിനെ പറ്റി പറയാം, അവയുടെ സെക്യൂരിറ്റി സെറ്റിങ്സിനെ പറ്റിയും.

### Facebook

facebook ,whatsapp എന്നീ അപ്പ്ലിക്കേഷൻസ് നിങ്ങളുടെ സ്വകാര്യതയും സുരക്ഷിതത്വവും ഉറപ്പുവരുത്താനുള്ള ഒരുപാട് സംവിധാനങ്ങൾ നൽകിയിട്ടുണ്ട്. അതിൽ ചിലത് താഴെ കൊടുക്കുന്നു:

- നിങ്ങളുടെ പോസ്റ്റ് ആരെല്ലാം കാണുന്നു
- നിങ്ങളുടെ ഫോൺ നമ്പർ ഉപയോഗിച്ചു ആർക്കെല്ലാം നിങ്ങളെ കണ്ടെത്താം?
- ആർക്കെല്ലാം നിങ്ങൾക്ക് frends Request അയക്കാം?
- നിങ്ങളുടെ ടൈംലൈനിയിൽ പൊതുവായി കാണാവുന്നത് എന്തെല്ലാം?
- മറ്റുള്ളവർ Tag ചെയ്യുന്നത്

പക്ഷെ കുട്ടികൾ പ്രത്യേകിച്ചും Teenagers facebookലും whatsapp ലും പലതും പോസ്റ്റ് ചെയ്യുന്നതിന് മുന്നേ ഒരു വട്ടം പോലും ആലോചിച്ചു ആലോചിക്കുന്നില്ല, അവർ ചെയ്യുന്നത് എത്രത്തോളം അപകടകരമാണ് എന്ന്. പല കുട്ടികളും അവരുടെ contact ഡീറ്റൈൽസും, അഡ്രസ്സും മറ്റു വ്യക്തിപരമായ കാര്യങ്ങൾ ഷെയർ ചെയ്യുന്നു എന്നാണ് പഠനങ്ങൾ തെളിയിക്കുന്നത്. ഇത് മറ്റുള്ളവർക്കു അവരെ പറ്റി കൂടുതൽ അറിയാൻ അവസരം കൊടുക്കുകയും അത് മറ്റു അപകടങ്ങളിലേക്കു നയിക്കുകയും ചെയ്യുന്നു

## ***Slide -17***

### WhatsApp

നിങ്ങൾക്കു എല്ലാവര്ക്കും അറിയാവുന്നതു പോലെ Whatsapp നിങ്ങളുടെ ഫോൺ നമ്പർ ഉപയോഗിച്ചുള്ള സോഷ്യൽ മീഡിയ ആണ്. whatsapp-ന്റെ അശ്രദ്ധാപൂർണമായ ഉപയോഗം പല അപകടങ്ങൾക്കും വഴി തെളിക്കും

- അപരിചിതർക്ക് വാതിൽ തുറന്നുകൊടുക്കുന്നു - ഒരാൾക്ക് നിങ്ങളുടെ നമ്പർ കിട്ടിയാൽ നിങ്ങളുമായി ബന്ധപ്പെടാൻ എളുപ്പമാണ്.
- അശ്ളീലസംഭാഷണങ്ങൾക്കുള്ള (Sexting) സാധ്യത വർധിക്കുന്നു.
- Cybebullying- നുള്ള സാധ്യത കൂടുന്നു.
- നിങ്ങൾ നിൽക്കുന്ന സ്ഥലം സംബന്ധിച്ച വിവരങ്ങൾ എളുപ്പത്തിൽ അറിയാൻ പറ്റുന്നു.

***WhatsApp** ഉപയോഗിക്കുമ്പോൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ*

- നിങ്ങളുടെ സ്വകാര്യവും വിലപ്പെട്ടതുമായ വിവരങ്ങൾ പങ്കുവെയ്ക്കാതിരിക്കുക. അത് server-ൽ സേവ് ചെയ്യപ്പെടുകയോ ഹാക്ക് ചെയ്യപ്പെടുകയോ ചെയ്യാം.
- പരിചയമില്ലാത്തവർക്ക് മറുപടി കൊടുക്കാതിരിക്കുക, അവരെ ബ്ലോക്ക് ചെയ്യുക.
- എന്താണെന്നറിയാതെ ലിങ്കുകളിലോ ചിത്രങ്ങളിലോ ക്ലിക്ക് ചെയ്യാതിരിക്കുക. ഇത് നിങ്ങളുടെ വിവരങ്ങൾ ചോരാൻ ഇടയാക്കും.
- ക്ഷണം കിട്ടി എന്നുള്ളതുകൊണ്ട് എല്ലാ ഗ്രൂപ്പിലും ചേരരുത്.
- Share settings: നിങ്ങളുടെ contact പട്ടികയിൽ ഉള്ളവർക്ക് മാത്രമായി ചിട്ടപ്പെടുത്തുക.
- ഗ്രൂപ്പിൽ ചേരുമ്പോൾ സൂക്ഷിക്കുക. എല്ലാവരും നിങ്ങൾക്കു അറിയാവുന്നവരാണോ എന്ന് ഉറപ്പുവരുത്തുക.
- വിവരങ്ങൾ പങ്കുവയ്ക്കുമ്പോൾ ജാഗരൂകരാകുക.

ആവർത്തിച്ചുള്ള ഓർമ്മപെടുത്തലുകൾക്കു ശേഷവും കുട്ടികൾ അവരുടെ സ്വകാര്യവിവരങ്ങൾ പരസ്യപ്പെടുത്തുന്നവരുണ്ട്. ഇത്തരം സമൂഹമാധ്യമങ്ങളെല്ലാം ഇരകളെ തേടിക്കൊണ്ടിരിക്കുന്ന ആളുകളെകൊണ്ട് നിറഞ്ഞിരിക്കുകയാണ് എന്ന് കുട്ടികൾ മനസിലാക്കണം. നേരത്തെ സൂചിപ്പിച്ചതുപോലെ ഒരിക്കലും നിങ്ങളുടെ വിവരങ്ങൾ പരസ്യപ്പെടുത്താതിരിക്കുക. സമൂഹമാധ്യമങ്ങളിൽ അപരിചിതരുമായി ഇടപെടാതിരിക്കുക. ഇവയെല്ലാമാണ് നിങ്ങളെ അപകടത്തിൽപ്പെടുത്താനായി മറ്റുള്ളവർ ഉപയോഗിക്കുന്ന മാർഗ്ഗങ്ങൾ.

സൂക്ഷിക്കുക Social media നല്ല രീതിയിൽ ഉപയോഗിക്കുക.

## മൊബൈലും ശരിയായ ഉപയോഗങ്ങളും

### ***Slide 1***

ഇന്ന് മൊബൈൽ ഫോൺ ഉപയോഗിക്കാത്ത അധികം ആളുകൾ ഇല്ല. സുഹൃത്തുക്കളും, കുടുംബാംഗങ്ങളും സഹപ്രവർത്തകരുമായി നല്ല രീതിയിൽ ആശയ വിനിമയം നടത്താൻ അത് സഹായിക്കുന്നു. പക്ഷേ മൊബൈലുകളുടെ അമിതമായ ഉപയോഗം നിങ്ങൾക്ക് ആരോഗ്യ പ്രശ്നങ്ങൾ ഉണ്ടാക്കും.

മൊബൈൽ ഫോൺ നിങ്ങളിൽ എന്തൊക്കെ സ്വാധീനം ചെലുത്തുന്നു എന്ന് നിങ്ങൾക്കു അറിയാമോ?? സാമൂഹികവും മാനസികവും ശാരീരികവും ആയ ഒരുപാട് ദുഷ്ഫലങ്ങൾ അതിനുണ്ട്.

### ***Slide 2***

- സാമൂഹിക ജീവിതത്തെ ബാധിക്കുന്നു

കുടുംബാംഗങ്ങളെപ്പോലും പരിഗണിക്കാൻ സമയമില്ലാത്ത വിധം എല്ലാവരും അവരവരുടെ ഫോണുകളിൽ ശ്രദ്ധ കേന്ദ്രീകരിക്കുന്നു. ഭക്ഷണ ശാലകളിൽ ആണെങ്കിൽ പോലും വീട്ടുകാർ അവരവരുടെ ഫോണുകളിൽ മുഴുകി ഇരിക്കുന്നത് കാണാം.

- വർധിച്ചു വരുന്ന മാനസിക പിരിമുറുക്കം

തുടർച്ചയായ മൊബൈൽ ഫോൺ ഉപയോഗം നിങ്ങളിൽ വിപരീത ഫലങ്ങൾ ഉണ്ടാക്കാം.

- വേദനകൾ

സെൽ ഫോൺ പ്രവർത്തിപ്പിക്കാൻ തുടർച്ചയായി കൈ ഉപയോഗിക്കണം, ഇത് നിങ്ങളുടെ സന്ധികളിൽ വേദന ഉണ്ടാക്കുന്നു. പുറം വേദനയും ഇതിന്റെ അനന്തര ഫലമാണ്.

- കാഴ്ച ശക്തിക്ക് കോട്ടം തട്ടുന്നു

മൊബൈൽ ഫോണിൽ കുറേ നേരം നോക്കി ഇരിക്കുന്നത് ഭാവിയിൽ നിങ്ങളുടെ കാഴ്ച ശക്തിക്ക് കുറവു വരുത്താം. ചെറിയ screen-ലെ അക്ഷരങ്ങൾ വായിക്കുക വഴി കണ്ണുകൾക്കു ആയാസം അനുഭവപ്പെടാം.

- റേഡിയേഷൻ (വികിരണങ്ങൾ)

മനുഷ്യനിൽ മൊബൈൽ ഉപകരണങ്ങളുടെ വികിരണങ്ങൾ ഉണ്ടാക്കുന്ന ആഘാതത്തെ പറ്റി ഇപ്പോഴും പഠനങ്ങൾ നടന്നു വരികയാണ്. ഇപ്പോഴത്തെ അറിവുപ്രകാരം ഇത്തരം വികിരങ്ങൾ വഴി കാൻസർ ഉണ്ടാകാനുള്ള സാധ്യത 40% വരെ കൂടുതലാണ്.

- സെൽഫി മൂലം ഉണ്ടാകുന്ന അപകടങ്ങൾ

അപകടകരമായ സാഹചര്യത്തിൽ സെൽഫികൾ എടുക്കാൻ ശ്രമിക്കുകവഴി നിരവധി അപകടങ്ങളാണ് ഇന്ന് ഉണ്ടായി കൊണ്ടിരിക്കുന്നത്.

***Slide 3***

# Text Neck

അമിതമായ മൊബൈൽ ഫോൺ ഉപയോഗത്തിന്റെ മറ്റൊരു ഫലമാണിത്.

നമ്മുടെ തല ശരിയായ രീതിയിൽ വെയ്ക്കുമ്പോൾ നട്ടെല്ലിൽ അനുഭവപ്പെടുന്ന ഭാരം 4.5-5.5kg വരെ ആണ്. ഈ രീതിയിൽ നിന്നും തുടർച്ചയായ മാറ്റം എല്ലാത്തരത്തിലുള്ള കഴുത്തുസംബന്ധമായ രോഗങ്ങൾക്കു കാരണമാകുന്നു. പലപ്പോഴും ഒരു ശാസ്ത്രക്രിയക്കു തന്നെ ഇത് വഴിവെച്ചേക്കാം.

എല്ലാദിവസവും എന്നെയും നിങ്ങളെയും പോലെ എല്ലാവരും ഏകദേശം 2-4 മണിക്കൂർ വരെ വായനക്കും മെസ്സേജുകൾ അയക്കുന്നതിനുമായി കഴുത്തു തിരിച്ചു ഫോണിൽ നോക്കി ഇരിക്കാറുണ്ട്. വർഷത്തിൽ ഇത് ഏതാണ്ട് 700 മുതൽ 1400 മണിക്കൂർ അധിക സമ്മർദ്ദമാണ് നട്ടെല്ലിനു നൽകുന്നത്. ഇതിന്റെ തീവ്രത കൂട്ടാനായി, ഹൈസ്കൂൾ വിദ്യാർത്ഥികൾ ഏതാണ്ട് 5000 മണിക്കൂറുകൾ പഠനത്തിനും, ടൈപ്പ് ചെയ്യാനും അവരുടെ ഉപകരണങ്ങളിൽ ചിലവിടുന്നു. നിങ്ങൾക്കു നിങ്ങളുടെ കഴുത്തിനെ സംരക്ഷിക്കണമെങ്കിൽ, മൊബൈൽ ഉപയോഗിക്കുമ്പോൾ അത് ശരിയായ രീതിയിൽ ചെരിച്ചുവെക്കുക.

***Slide 4***

മൊബൈൽ ഫോണുകൾ ഒഴിച്ചുകൂടാനാകാത്ത ഒന്നാണ് എന്ന് നമുക്കറിയാം. അപ്പോൾ അവ സുരക്ഷിതമായി എങ്ങനെ ഉപയോഗിക്കാം, അതിനുള്ള ചില മാർഗങ്ങൾ നമുക്ക് നോക്കാം.

താരതമ്യേന കുറഞ്ഞ വികിരണങ്ങൾ പുറക്കപ്പെടുവിക്കുന്നതായാലും എല്ലാ മൊബൈൽ ഫോണുകളും radiio ആക്റ്റീവ് ട്രാൻസ്മിറ്റർസ് ആണ്. അതുകൊണ്ടു തന്നെ അവയിൽ നിന്നും അകലം പാലിക്കേണ്ടത് റേഡിയോവികിരണങ്ങളിൽ നിന്ന് രക്ഷനേടുന്നതിൽ അത്യന്താപേക്ഷിതമാണ്.

- മൊബൈൽ ഫോണിൽന്റെ ഉപയോഗം സുപ്രധാനമായ വിളികളിലേക്കും ദൈർഘ്യംകുറഞ്ഞ വിളികളിലേക്കും ചുരുക്കുക.
- അവ പോക്കറ്റിലോ ബെൽറ്റിനടുത്തോ വെക്കാതിരിക്കുക. തലയിലേതിനേക്കാൾ മറ്റു ശരീരഭാഗങ്ങളിലെ കോശങ്ങൾ വികിരണങ്ങളെ എളുപ്പത്തിൽ വലിച്ചെടുക്കുന്നവയാണ്.
- ഒരാളെ വിളിക്കുമ്പോൾ ഫോൺ റിംങ് ചെയുന്നത് വരെ ഫോൺ ചെവിയിൽ വെക്കാതിരിക്കുക.
- കുറഞ്ഞ SAR (Specific Absorption Rate) ഉള്ള ഫോണുകൾ ഉപയോഗിക്കുക
- എല്ലാ സമയവും സംസാരിക്കുന്നതിനു പകരം മെസ്സേജുകൾ ഉപയോഗിക്കുക.
- പറ്റുന്നിടത്തോളം ലാൻഡ് ഫോണുകൾ ഉപയോഗിക്കുക.
- സിഗ്നൽ ഇല്ലാത്തപ്പോൾ പരമാവധി ഫോൺ വിളി കുറക്കുക. കാരണം ആ സമയത്തു ഫോൺ കൂടുതൽ ശക്തിയോടെയുള്ള വികിരണങ്ങൾ പുറപ്പെടുവിക്കുന്നു
- ഫോൺ സമീപത്തുവെച്ച് ഉറങ്ങാതിരിക്കുക, പ്രത്യേകിച്ചു തലയുടെ അടുത്തു്.
- വാഹനം ഓടിക്കുമ്പോൾ ഫോൺ ഉപയോഗിക്കാതിരിക്കുക.

ശാരീരിക പ്രശ്നങ്ങൾ കുറയ്ക്കുന്നതിനായി ഫോൺ ഉപയോഗിക്കുമ്പോൾ Earphone കൾ ഉപയോഗിക്കാവുന്നതാണ്. ഇത് ചെവി സംബന്ധമായ പ്രശ്നങ്ങൾ കുറയ്ക്കാൻ സഹായിക്കുന്നു.

## ***Slide 5***

ഫോൺ ഉപയോഗിക്കുമ്പോൾ ശരിയായി ഇരിക്കാനും നിൽക്കാനും ശ്രദ്ധിക്കണം. സ്ക്രീൻ എപ്പൊഴും കണ്ണിനു നേരെ ആയിരിക്കണം. കണ്ണിനും കഴുത്തിനുമുള്ള വ്യായാമങ്ങൾ ചെയ്യുന്നതും നല്ലതാണ്.

മണിക്കൂറിൽ കുറച്ചു മിനിറ്റ്കൾ കഴുത്തിന് ആയാസം കുറക്കുന്ന വ്യായാമം ചെയ്യുക.

## ***Slide 6***

Earphone ഉപഗോഗിക്കുന്നതാണ് നല്ലത് എന്ന് സൂചിപ്പിച്ചു എങ്കിലും അതിനു അതിന്റെതായ ദോഷങ്ങൾ ഉണ്ട്. കൂടിയ ശബ്ദത്തിൽ ഉള്ള തുടർച്ചയായ ഉപയോഗം കേൾവിശക്തിയ്ക്ക് സ്ഥിരമായ ദോഷം വരുത്തിയേക്കാം. റോഡ് യാത്രയ്ക്കിടെ Earphone ഉപയോഗിക്കുന്നവർക്ക് ചുറ്റുപാടുകളെ കുറിച്ച് അറിയാൻ സാധിയ്ക്കാതെ വരുകയും ഇതുമൂലം അപകടങ്ങൾ ഉണ്ടാകുകയും ചെയ്യും.

## ***Slide 7***

### Earphone ഉപയോഗിക്കുമ്പോൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

- ചെവിയിലേക്ക് നേരിട്ടു കടന്നുചെല്ലുന്ന തരം Earphone ഉപയോഗിക്കാതിരിക്കുക.

ചെവിക്കു പുറത്തു നിൽക്കുന്ന തരം earphone അല്ലെങ്കിൽ headphone ഉപയോഗിക്കുക.
- മറ്റുള്ളവരുമായി നിങ്ങളുടെ earphone പങ്കുവെയ്ക്കാതിരിക്കുക.
- ഓരോ മാസവും നിങ്ങളുടെ എയർഫോണിന്റെ സ്പോഞ്ച്/റബ്ബർ കവർ മാറ്റുക.
- കാറിലോ ട്രെയിനിലോ യാത്രചെയ്യുമ്പോഴോ നടക്കുമ്പോഴോ അവ ഉപയോഗിയ്ക്കാതിരിക്കുക
- കൂടിയ ശബ്ദത്തിൽ ഉപയോഗിയ്ക്കാതിരിക്കുക

കഴിയാവുന്നത്രയും മൊബൈൽ ഫോൺ ഉപയോഗം കുറയ്ക്കുകയും അത് ശരീരത്തിൽ നിന്നും 20cm എങ്കിലും അകലത്തിൽ സൂക്ഷിയ്ക്കുകയും ചെയ്യുക

## ***Slide 8***

### മൊബൈൽ ആപ്പുകളും ഉപയോഗങ്ങളും

വിവരലഭ്യതയ്ക്കും ആശയവിനിമയത്തിനും എല്ലാം വേണ്ടിയാണ് മൊബൈൽ ആപ്പുകൾ ഉപയോഗിച്ച് തുടങ്ങിയത്. എങ്കിലും ജനങ്ങളുടെ ആവശ്യങ്ങൾക്കനുസരിച്ചു് അവ മറ്റു പല മേഖലകളിലേക്കും വ്യാപിച്ചു. ഇന്ന് മനുഷ്യ ജീവിതത്തിലെ പല കാര്യങ്ങൾക്കും സഹായകമായ വിധം ആപ്പുകൾ വികസിപ്പിയ്ക്കപ്പെട്ടിരിക്കുന്നു

- e-മെയിൽ
- കലണ്ടർ
- കോൺടാക്ട്
- സ്റ്റോക്ക് മാർക്കറ്റ്
- കാലാവസ്ഥ വ്യതിയാനങ്ങളെക്കുറിച്ചുള്ള വിവരങ്ങൾ

### വ്യാപകമായി ഉപയോഗിക്കുന്ന ചില Applications

- E-മെയിൽ (gmail, yahoo, outlook): മെയിലുകൾ അയക്കാനും സ്വീകരിക്കാനും
- മെസ്സേജിങ് & സോഷ്യൽ മീഡിയ ആപ്പുകൾ (Facebook,Whatsapp,Instagram)
- ഗെയിമിംഗ് ആപ്പുകൾ (Temple Run, SubwaySurf)
- വിനോദത്തിനായുള്ളവ (Play Music, Videoplayer, etc.)
- ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്നതിന് (Chrome, UC Browser)

## ***Slide 9***

ഫോണിൽ Applications ഡൌൺലോഡ് ചെയ്യുമ്പോൾ വിശ്വസനീയമായ സ്ഥലത്തുനിന്നുമാണ് നിങ്ങൾ അവ എടുക്കുന്നത് എന്ന് ഉറപ്പു വരുത്തുക. ഓരോ OS -നും ഇതിനായി ഒരിടം (STORE) ഉണ്ടാകും.

ഏതൊരു സാമൂഹ്യമാധ്യമം ഉപയോഗിക്കുമ്പോഴും നമ്മൾ ശ്രദ്ധാലുക്കളായിരിക്കണം

ശാരീരികപ്രശ്നങ്ങൾ കൂടാതെ മറ്റു പല കാര്യങ്ങളും മൊബൈൽ ഉപയോഗിക്കുമ്പോൾ നമ്മൾ പരിഗണിക്കേണ്ടതുണ്ട്. അതും പൊതുസ്ഥലങ്ങളിൽ മൊബൈൽ ഉപയോഗിക്കുമ്പോൾ. പലപ്പോഴും ചുറ്റും ആളുകൾ ഉണ്ടെന്നുകൂടി ഓർക്കാതെ ആളുകൾ ഫോണിൽ സംസാരിക്കുന്നതു

നമ്മൾ കേൾക്കാറുണ്ട്

മൊബൈൽ ഫോൺ ഉപയോഗിക്കുമ്പോൾ ശ്രദ്ധിക്കേണ്ട ചില പൊതുവായ കാര്യങ്ങൾ

- *സാധാരണ ശബ്ദത്തിൽ സംസാരിക്കുക*: ഒരാൾ പറയുന്നത് നിങ്ങൾക്ക് കേൾക്കുന്നില്ല എന്നതുകൊണ്ട് തിരിച്ചും അങ്ങനെ തന്നെ ആണെന്ന് വിചാരിക്കരുത്. അതുകൊണ്ടു സാധാരണ ശബ്ദത്തിൽ സംസാരിക്കുക
- *നേരിട്ട് സംസാരിക്കുന്നവരെ അവഗണിക്കാതിരിക്കുക(Phubbing):* ആളുകളുടെ ഇടയിൽ, അവർ സംസാരിക്കുമ്പോൾ ഫോണിൽ നോക്കിയിരുന്നു അവരെ അവഗണിക്കാതിരിക്കുക
- *സിനിമ തിയേറ്ററിൽ ഫോൺ ഉപയോഗിക്കാതിരിക്കുക:* തിയേറ്ററിൽ മൊബൈൽ ഫോൺ ഓഫ് ആക്കി വെക്കുക. ഇനി ഓഫ് ആകാൻ മറന്നാൽ, റിങ് ചെയ്താലും എടുക്കാതിരിക്കുക, disconnect ചെയ്യുക.
- *പൊതുസ്ഥലങ്ങളിൽ അകലം പാലിക്കുക:* ഫോൺ ഉപയോഗം ഒഴിവാക്കാനാകാത്തപ്പോൾ, ചുറ്റുമുള്ളവരിൽ നിന്ന് കുറച്ചു ദൂരെ മാറി നിന്ന് സംസാരിക്കുക
- *പൊതുസ്ഥലങ്ങളിൽ സ്പീക്കർ ഫോണിലിടാതിരിക്കുക*: ചുറ്റുമുള്ളവർക്കെല്ലാം കേൾക്കേണ്ട ആവശ്യം ഇല്ലാത്തിടത്തോളം ഫോൺ സ്പീക്കറിൽ ഇടാതിരിക്കുക
- ഒരാളോട് ഫോണിൽ സംസാരിക്കുമ്പോൾത്തന്നെ ഫോണിൽ നോക്കി കൊണ്ടിരിക്കാതിരിക്കുക. സംസാരത്തിൽ പൂർണ്ണശ്രദ്ധ ചെലുത്താൻ സാധിക്കാതെ വരുന്നു
- ജോലി ചെയ്യുമ്പോഴും പഠിയ്ക്കുമ്പോഴും Phone മാറ്റി വെക്കുക
- ആരുടെയെങ്കിലും കൂടെയിരുന്നു ഭക്ഷണം കഴിയ്ക്കുമ്പോൾ ഫോൺ ഉപയോഗിക്കാതിരിയ്ക്കുക. വീട്ടിലും പുറത്തും ഇത് ബാധകമാണ്. അവരുടെ കൂടെ ഭക്ഷണം ആസ്വദിയ്ക്കുക.
- മറ്റുള്ളവരുമായി മുഖാമുഖം സംസാരിയ്ക്കുമ്പോൾ ഫോണിൽ സംസാരിയ്ക്കുന്നതും മെസ്സേജ് ചെയ്യുന്നതും ഒഴിവാക്കു. ഒരു അത്യാവശ്യ സന്ദർഭത്തിൽ അല്ലാത്തിടത്തോളം മുന്നിൽ ഇരിയ്ക്കുന്നവർക്കാണ് ഫോണിന്റെ അറ്റത്തുള്ളവരേക്കാൾ പ്രാധാന്യം നൽകേണ്ടത്.

## ഇന്റർനെറ്റ് നിങ്ങളെ എങ്ങനെ സ്വാധീനിക്കുന്നു?

ഇന്ന് ഇന്റർനെറ്റ് നമ്മുക്ക് അനന്തമായ സാധ്യതകൾ തുറന്നുതരുന്നു എന്നതാണ് നിങ്ങൾ കണ്ടത്. എന്നാൽ അതേ സമയം, പ്രത്യേകിച്ച് തുടർച്ചയായും സുരക്ഷിതമല്ലാത്തതുമായ ഇന്റർനെറ്റ് ഉപയോഗം, നമ്മുക്ക് പല ദോഷങ്ങളും ഉണ്ടാക്കാം .

കമ്പ്യൂട്ടറിന്റെയും ഇന്റർനെറ്റിന്റെയും തുടർച്ചയായ ഉപയോഗം നിങ്ങളെ ശാരീരികമായും മാനസിക മായും ബാധിക്കുന്നു. ഇന്റർനെറ്റ് നിങ്ങളുടെ ജീവിതത്തെ വിപരീതമായി എങ്ങനെ ബാധിക്കുന്നു എന്നാണ് ഇനിയുള്ള ഭാഗങ്ങളിൽ നമ്മൾ കാണാൻ പോകുന്നത്

### ***Slide1***

സങ്കേതികതയുടെ അതിപ്രസരം ചുറ്റും ഉണ്ടെങ്കിലും ഇക്കാലത്ത് ചെറുപ്പക്കാർ ആവർത്തിച്ചുപറയുന്ന കാര്യമാണ് അവർക്ക് വിരസത അനുഭവപ്പെടുന്നു എന്നത് . ഇതെന്തുകൊണ്ടാണെന്ന് നിങ്ങൾ അത്ഭുത പ്പെട്ടിട്ടുണ്ടോ? വളരെ ലളിതമായ ഒരു ഉത്തരമാണ് ഈ ചോദ്യത്തിന് ഉള്ളത്. അവർ അവരുടെ അധിക സമയവും ചിലവിടുന്നത് വാസ്തവികമല്ലാത്തൊരു ലോകത്താണ്. അവിടെ അവർക്ക് ലഭിക്കുന്ന അതേ വേഗതയും തെളിച്ചവും യഥാർത്ഥജീവിതത്തിലും വേണമെന്ന് അവർ ആഗ്രഹിക്കുന്നു അസംഭവ്യമായ അത് കണ്ടെത്താൻ സാധിക്കാതെ വരുമ്പോൾ അവർക്ക് വിരസത അനുഭവപ്പെടുകയും അവർ അതേ ലോകത്തിലേക്ക് മടങ്ങിപ്പോകാൻ ശ്രമിക്കുകയും ചെയ്യുന്നു.

തുടർച്ചയായ ഉപയോഗം മനശ്ശാസ്ത്രപരമായി ചെലുത്തുന്ന സാധീനം

***Slide 2,3***

## നിങ്ങൾ ഇന്റർനെറ്റിന് അടിമപ്പെടുന്നുണ്ടോ ?

ലോകത്താകമാനം യുവാക്കളും, അധികസമയവും ചിലവിടുന്നത് ഇന്റർനെറ്റിലാണ് .വളരെ ചെറിയ പ്രായത്തിൽ തന്നെയുള്ള ഇന്റർനെറ്റ് ഉപയോഗം ശാരീരികവും മാനസികവുമായ ഒരുപാട് അപകടങ്ങൾ വരുത്തി വയ്ക്കുന്നു. അധികമായ ഇന്റർനെറ്റ് ഉപയോഗം മൂലം ഇന്നത്തെ ചെറുപ്പക്കാർ ഒരുപാട് അപകടങ്ങൾ നേരിടുന്നു.

അമിതമായ ഇന്റർനെറ്റ് ഉപയോഗം നിങ്ങൾക്ക് നല്ലതല്ല.

- യഥാർത്ഥ സുഹൃത്തുക്കളേക്കാൾ ഓൺലൈൻ സുഹൃത്തുക്കളോടൊപ്പം നിങ്ങൾ സന്തോഷവാന്മാരായിരിക്കുമ്പോൾ
- ഗെയിമുകളും, ചാറ്റിങ്ങും, ഇന്റർനെറ്റ് ഉപയോഗിക്കലും ഒന്നും നിങ്ങൾക്ക് നിർത്താനാകാതെ വരുമ്പോൾ
- നിങ്ങൾ സന്തം കുടുംബത്തെയും, സുഹൃത്തുക്കളേയും ദൈനംദിന ആവശങ്ങളേയും വരെ ഇന്റർനെറ്റിനു വേണ്ടി അവഗണിക്കുമ്പോൾ

ഇങ്ങനെയുള്ള അവസ്ഥയെയാണ് Internet Addiction എന്ന് പറയുന്നത്.

ഒരാൾ ഇന്റർനെറ്റിന് അടിമപ്പെട്ടിട്ടുണ്ടോ എന്ന് എങ്ങിനെ തിരിച്ചറിയാം? ശ്രദ്ധിക്കേണ്ട ലക്ഷണങ്ങൾ ഇവയാണ .

1. എല്ലായ്പ്പോഴും ഓൺലൈൻ പ്രവർത്തനങ്ങളെക്കുറിച്ച് ചിന്തിച്ചു കൊണ്ടിരിക്കുക (പഴയ ചാറ്റുകൾ/ഗെയിമുകൾ തുടങ്ങിയവ) – സ്വപ്നത്തിൽപ്പോലും .
2. പ്രതിക്ഷിക്കുന്നതിലും കൂടുതൽ സമയം ഇന്റർനെറ്റ് ഉപയോഗിക്കുക.
3. ഇന്റർനെറ്റ് ഉപയോഗിക്കാനാകാതെ വരുമ്പോൾ സങ്കടപ്പെട്ട് ഇരിക്കുക
4. ഇന്റർനെറ്റ് ഉപയോഗിക്കാനായി കുടുംബങ്ങളോട് നുണ പറയുക.
5. ഇന്റർനെറ്റിനുവേണ്ടി കുടുംബത്തേയും സുഹൃത്തുക്കളേയും അവഗണിയ്ക്കുക.
6. ഇന്റർനെറ്റിനുവേണ്ടി ഉറക്കം പോലും മറക്കാൻ തയ്യാറാകുക.

***Slide 4***

ഉപയോഗിക്കുന്ന രീതിയനുസരിച്ച് ഇന്റർനെറ്റിനോടുള്ള അടിമത്തത്തെ നമുക്ക് പലതായി തരം തിരിയ്ക്കാം.

- സമൂഹമാധ്യമങ്ങളോടുള്ള അടിമത്തം (സൈബർ ബന്ധങ്ങളോടുള്ള അടിമത്തം)– ഓൺലൈൻ സുഹൃത്തുക്കളോടൊപ്പം അധികസമയം ചിലവിടുന്നത്.
- ഗെയിമുകളോടുള്ള അളവിൽ കവിഞ്ഞ താൽപര്യം–നിത്യ ജീവിതത്തിനു കുറുകെ വരുന്ന തരത്തിലുള്ള ഗെയിമുകളുടെ ഉപയോഗം.
- അശ്ലീല ചിത്രങ്ങളോടുള്ള താത്പര്യം - അശ്ലീല വെബ്സൈറ്റുകളുടേയും വീഡിയോകളുടേയും ചിത്രങ്ങളുടേയുമൊക്കെ അമിതമായ ഉപയോഗം.
- അളവിൽ കവിഞ്ഞ വിവരങ്ങൾ (Information Overload) – കൈകാര്യം ചെയ്യാവുന്നതിലും കൂടുതലുള്ള വിവരങ്ങളുടെ ലഭ്യത അവ കൈകാര്യം ചെയ്യുന്നതും നിഗമനങ്ങളിലെത്തുന്നതും പോലുള്ള കാര്യങ്ങൾ ബുദ്ധിമുട്ടിലാക്കുന്നു.

സമൂഹമാധ്യമങ്ങളോടുള്ള  അടിമത്തം (സൈബർ ബന്ധങ്ങളോടുള്ള അടിമത്തം)

## ***Slide 5***

അമേരിക്കൻ ഐക്യനാടുകൾ മനോരോഗങ്ങളുടെ വിഭാഗത്തിൽ പെടുത്തിയിട്ടുള്ള ഒന്നാണ് സമൂഹമാധ്യമങ്ങളോടുള്ള അടിമത്തം. ഇന്ത്യയും ഇക്കാര്യത്തിൽ അധികം പുറകിലല്ല. ഈ അവസ്ഥയിൽ ലഭ്യമായതിൽ കൂടുതൽ സമയവും ഓൺലൈൻ സുഹൃത്തുക്കൾക്കൊപ്പം ചിലവഴിയ്ക്കാൻ ശ്രമിക്കുകയാണ് ഒരാൾ ചെയ്യുന്നത്.

**ഇതിന്റെ അനന്തര ഫലങ്ങൾ ഇവയാണ്.**

a) കുടുംബത്തോടും സുഹൃത്തുക്കളോടും ഒപ്പം ചിലവഴിയ്ക്കാൻ ഉള്ള സമയം കുറയുന്നു.

b) കുടുംബവും ബന്ധുക്കളുമായുള്ള അടുപ്പം കുറയുന്നു.

c) സമൂഹവുമായുള്ള ഇടപെടലുകൾ കുറയുന്നതുമൂലം സാമൂഹ്യപരമായ കഴിവുകൾ ക്ഷയിയ്ക്കുന്നു.

d) സാങ്കൽപ്പികലോകത്തെ സ്വീകാര്യതയെക്കുറിച്ചുള്ള ആകാംക്ഷ.

e) യഥാർത്ഥ ജീവിതത്തിൽ ഉള്ളതിനേക്കാൾ  പല വിധത്തിലുള്ള വ്യക്തിത്വങ്ങളായി, ഓൺലൈൻ ലോകത്ത് നിങ്ങളെ അവതരിപ്പിക്കുക. ഇത് സ്വയം ബോധത്തിൽ കുറവു വരുന്നതിനു കാരണമാകുന്നു.

f) തെറ്റായ വിവരങ്ങൾ കാരണം ചതിയ്ക്കപ്പെടുന്നു. ഓൺലൈനിൽ കാണുന്ന എല്ലാവരും യഥാർത്ഥമാകണമെന്നില്ല.

g) പഠനത്തിനോടുള്ള താത്പര്യം കുറവാകുക.

(Reference - www.yutobe.com/watch?v=vsq95m-kzwy)

തന്റെ വിവരങ്ങൾ ഓൺലൈൻ വഴി പരിചയപ്പെടുന്നവരുമായി പങ്കുവെയ്ക്കുന്നവരാണ് ഇന്നുള്ള കൗമാരപ്രായക്കാരിൽ പകുതിയും എന്നാണ് പഠനങ്ങൾ തെളിയിക്കുന്നത്. സൈബർ ലോകത്ത് ഇത് ഒരിക്കലും ചെയ്യാൻ പാടുള്ളതല്ല.

## ***Slide 6***

Explain the comic

നമ്മുടെ കുടുംബത്തേയും സുഹൃത്തുക്കളേയും നമ്മളെത്തന്നെയും എങ്ങനെ രക്ഷിയ്ക്കാം..

**നിങ്ങൾ കളിപ്പിക്കപ്പെടുന്നു എന്ന് തിരിച്ചറിയുക**

സമൂഹമാധ്യമങ്ങൾ അധികമായി ഉപയോഗിയ്ക്കുക എന്നത് മുഴുവനായും നിങ്ങളുടെ  തെറ്റല്ല. വീണ്ടും വീണ്ടും ഉപയോഗിയ്ക്കാൻ നിങ്ങളെ പ്രേരിപ്പിക്കും വിധമാണ് എല്ലാ സമൂഹ മാധ്യമങ്ങളും രൂപകല്പന ചെയ്തിരിക്കുന്നത്.

**ആവശ്യത്തിനു മാത്രം ഉപയോഗിക്കുക.**

സാധാരണയായി വിരസത അനുഭവിയ്ക്കുമ്പോൾ സമൂഹമാധ്യമങ്ങളിലേയ്ക്ക് ഇറങ്ങിച്ചെല്ലുന്നവരാണ് നമ്മളിൽ അധികവും. ഇത് ചുരുക്കുന്നതിനായി ഒരു പരിധി നിശ്ച യിക്കുക. നിങ്ങൾ നിങ്ങളോടുതന്നെ ചോദിയ്ക്കുക ‘‘ഇപ്പോൾ ഇന്റർനെറ്റ് ഉപയോഗിയ്ക്കാനുള്ള കൃത്യമായ കാരണം /ആവശ്യം ഇപ്പോൾ എനിയ്ക്കുണ്ടോ’’?

**കർക്കശമായി ചിന്തിക്കുന്നവരാകുക**

ഒരു അഭിപ്രായമോ ചിത്രമോ സമൂഹമാധ്യമങ്ങളിൽ പരസ്യമാക്കുന്നതിനുമുമ്പ്, നിങ്ങളുടെ ഉദ്ദേശശുദ്ധിയെക്കുറിച്ച് നിങ്ങളോടു തന്നെ ചോദ്യങ്ങൾ ചോദിയ്ക്കുക. കുറച്ചു സമയത്തെ സന്തോഷത്തിനു

വേണ്ടി മാത്രമാണോ നിങ്ങൾ ഇത് ചെയ്യുന്നത്? ഒരു ചിത്രം ഇത്തരത്തിൽ പ്രചരിപ്പിക്കുന്നതിന് അതിന്റേതായ ഫലങ്ങൾ ഉണ്ട്. നിങ്ങൾ സ്വന്തം അനുഭവങ്ങളെക്കുറിച്ച് ചിന്തിക്കാതിരിക്കുകയും മറ്റുള്ളവരുടെ പ്രതികരണങ്ങൾക്ക് പ്രാധാന്യം കല്പിക്കുകയും ചെയ്യും.

**ഇന്റർനെറ്റിലൂടെയല്ലാതെ മറുപടി കൊടുക്കുക**

നിങ്ങളുടെ സുഹൃത്തിന്റെ ജന്മദിനമാണെന്ന് ഫേസ്ബുക്ക് നിങ്ങളെ ഓർമ്മപ്പെടുത്തിയാൽ, നേരിട്ട് ആശംസകൾ അറിയിക്കുക. സ്വീകർത്താവിന് ആ രീതി ആയിരിക്കും കൂടുതൽ സ്വീകാര്യമായത്.

**(സെറ്റിംഗ്സ്) മാറ്റുക.**

നിങ്ങളെ പൂർണ്ണമായും അടിമപ്പെടുത്തുന്ന തരം ആപ്പുകൾ (. . .) ഒഴിവാക്കുക. പ്രവർത്തനക്ഷമമാക്കിവെച്ചിരിക്കുന്ന ഓർമ്മപ്പെടുത്തലുകൾ (..) ഒഴിവാക്കുക.

ഗെയിമുകളോടുള്ള അളവിൽ കവിഞ്ഞ താൽപര്യം

## *Slide 7*

നിങ്ങളിൽ ഭൂരിഭാഗവും കമ്പ്യൂട്ടറിൽ ഗെയിമുകൾ കളിയ്ക്കുന്നവരായിരിക്കും. അവയോട് അടിമപ്പെട്ടിട്ടുള്ളവർ കളിക്കിടയിൽ ഒരു ഇടവേള എടുക്കാൻപോലും പ്രയാസപ്പെടുന്നവരായിരിക്കും. സമയം കളയാൻ വേണ്ടി തുടങ്ങുന്ന ഒരു പ്രവർത്തി, പിന്നീട് മുഴുവൻ സമയത്തേയ്ക്കും വ്യാപിയ്ക്കുന്നു.

മയക്കുമരുന്ന് ഉപയോഗിക്കുന്നതിന്റേയോ മാനസികരോഗങ്ങളുടേയോ ചിലതോ അല്ലെങ്കിൽ മുഴുവനായോ ഉള്ള ലക്ഷണങ്ങൾ ഗെയിമുകളോടുള്ള അമിതാസക്തിയ്ക്കുള്ള ലക്ഷണങ്ങളാണ്. യഥാർത്ഥ ജീവിത്തതിലുള്ള ഇടപെടലുകളേക്കാൾ ഗെയിമുകളിലെ സാങ്കൽപിക ഇടപെടലുകൾക്ക് പ്രാധാന്യം നൽകുന്നവരാണ് ചില കളിക്കാർ. പലരും ദിവസത്തിൽ മണിക്കൂറുകണക്കിന് കളിയ്ക്കുന്നു., വ്യക്തിശുചിത്വം അവഗണിയ്ക്കുന്നു. ശരീരഭാഗത്തിൽ വ്യതിയാനങ്ങൾ വരുന്നു, ഉറക്കത്തെ പ്രതികൂലമായി ബാധിയ്ക്കുന്നു. ജോലി സമയത്തും കളിച്ചുകൊണ്ടിരിക്കുന്നു. സുഹൃത്തുക്കളുമായുള്ള ഫോൺ സംഭാഷണങ്ങൾ ഒഴിവാക്കുന്നു, വീഡിയോ ഗെയിമുകളിൽ ചിലവിടുന്ന സംയത്തെക്കുറിച്ച് നുണ പറയുന്നു.

ദിവസത്തിൽ 15 മണിക്കൂറോളം ഊണും ഉറക്കവും ഉപേക്ഷിച്ച് ഗെയിം കളിച്ചുകൊണ്ടിരുന്ന ഒരു 17 വയസ്സുകാരനെക്കുറിച്ചുള്ള വാർത്തകൾ രേഖപ്പെടുത്തപ്പെട്ടിരിക്കുന്നത് ഇതിന്റെ പാരമ്യതയെ കാണിയ്ക്കുന്നു. കൂടാതെ അക്രമാസക്തമായ ഗെയിംസിൽ കാണുന്ന കാര്യങ്ങൾ കുട്ടികൾ യഥാർത്ഥ ജീവിതത്തിലും ആവിഷ്കരിക്കാൻ ശ്രമിക്കുന്നു. കുട്ടികൾ കൂടുതൽ അക്രമാസക്തരാകാനും ഇത് കാരണമാകുന്നു.

## *Slide 8*

### പരിധിയിൽ കൂടുതലുള്ള ഗെയിംസിന്റെ പാർശ്വ ഫലങ്ങൾ എന്തെല്ലാമാണ്.

1. സമയ നഷ്ടം–ഇത് വിദ്യാഭ്യാസത്തെ പ്രതികൂലമായി ബാധിയ്ക്കുന്നു.
2. സാമൂഹികമായ ഒറ്റപ്പെടൽ
3. ധനനഷ്ടം–പല ഗെയിംസുകൾക്കും ഉയർന്ന വില നൽകേണ്ടി വരുന്നതാണ്.
4. യഥാർത്ഥ ലോകത്തിൽ നിന്ന് അകന്നു പോകുന്നു. പല അഡിക്റ്റഡ് gamers അവർ ഗെയിംസ് ലോകത്തിന്റെ ഭാഗമാണെന്ന് ചിന്തിച്ചു തുടങ്ങുന്നു.
5. വിദ്യാഭ്യാസം– കളിക്കുന്നതിനുവേണ്ടി പഠിപ്പുമാറ്റി വെക്കുകയും ഹോം വർക്കും അസ്സൈൻമെന്റും ചെയ്യാൻ സമയമില്ലാതെ വരികയും ചെയ്യുന്നു.
6. കുട്ടികളെ തെറ്റായ വഴിയിലൂടെ നയിക്കുന്നു.
7. കുട്ടികളിലെ ഏകാഗ്രതയ്ക്കു കോട്ടം തട്ടുന്നു.

8. ശാരീരികമായ ബുദ്ധിമുട്ടുകൾക്ക് കാരണമാകുന്നു.

**എങ്ങനെ നമുക്ക് ഇതിൽ നിന്ന് രക്ഷ നേടാം**

1. കുട്ടികളുടെ ഗെയിമിംഗ് രീതികൾ മാതാപിതാക്കളും രക്ഷിതാക്കളും ശ്രദ്ധിക്കേണ്ടതാണ്.
2. കുട്ടികൾക്ക് ഗെയിമിംഗ് അല്ലാതെ മറ്റു വിനോദങ്ങൾ കണ്ടെത്തുക.
3. ഗെയിം കളിക്കാൻ സമയപരിധി നിശ്ചയിക്കുക. അത് പാലിക്കുക.
4. കുട്ടികളിൽ ഗെയിമിന്റെ പാർശ്വഫലങ്ങൾ കണ്ടു തുടങ്ങുമ്പോൾ തന്നെ ഗെയിമിന്റെ ഉപയോഗം നിർത്തുക.
5. കുട്ടികൾ പഠിപ്പിനേക്കാൾ കൂടുതൽ ഗെയിമിൽ ശ്രദ്ധ കേന്ദ്രീകരിക്കുമ്പോൾ ഗെയിമിന്റെ ഉപയോഗം കുറയ്ക്കുക.
6. മറ്റു കളികളിൽ ഏർപ്പെടാതിരിക്കുമ്പോൾ ഗെയിമുനു നിയന്ത്രണം കൊണ്ടുവരിക.
7. കുട്ടികളിലെ പെരുമാറ്റത്തിലുള്ള മാറ്റങ്ങൾ നിരീക്ഷിക്കുക.

**ഒരു ഗെയിം തിരഞ്ഞെടുക്കുന്നതിന് മുമ്പ് ശ്രദ്ധിക്കേ കാര്യങ്ങൾ എന്തെല്ലാമാണ്**

1. ഒരു പാട് ചിന്തിച്ച് തീരുമാനങ്ങൾ എടുക്കേണ്ട രിതിയിലുള്ള ഗെയിം തിരഞ്ഞെടുക്കുക.
2. അക്രമാസക്തമായ ഗെയിം ഒരിക്കലും തിരഞ്ഞെടുക്കരുത്.
3. ഒരു ഗെയിം വാങ്ങുന്നതിനു മുൻപായി മാതാപിതാക്കളോടും കൂടി നിർദ്ദേശങ്ങൾ ചോദിയ്ക്കുക.
4. നിങ്ങൾ വാങ്ങാൻ ഉദ്ദേശിക്കുന്ന ഗെയിം മുൻപ് ഉപയോഗിച്ചവർ ഈ ഗെയിമിനെക്കുറിച്ച് എന്ത് അഭിപ്രായമാണ് രേഖപ്പെടുത്തിയത് എന്നും കൂടെ നോക്കുക.
5. ഒരേ സമയം ഒന്നിലധികം പേർക്ക് കളിക്കാവുന്ന രിതിയിലുള്ള ഗെയിം തിരഞ്ഞെടുക്കുക. ഇത് ഒരു ഗ്രൂപ്പിൽ പ്രവർത്തിയ്ക്കാനുള്ള കഴിവ് കൂട്ടാൻ സഹായിക്കുന്നു.

## Cyber Sex Addiction

**എന്തെല്ലാമാണ് Cyber sex addiction-ന്റെ ലക്ഷണങ്ങൾ.**

***Slide 9***

1. Porn വെബ്സൈറ്റുകളിൽ അമിതമായി സമയം ചിലവിടുക.
2. അശ്ലീല ചാറ്റുകളിൽ ഏർപ്പെടുക
3. Pornography സൈറ്റുകളുടെ സ്ഥിരം സന്ദർശകരാവുക.
4. Web camera, മുതലായവ ഉപയോഗിച്ച് നഗ്ന ചിത്രങ്ങൾ പകർത്തി അശ്ലീല സൈറ്റുകളുടെ ഭാഗമാകുക.
5. മാതാപിതാക്കളിൽ നിന്നും നിങ്ങൾ ഇന്റർനെറ്റിലൂടെ ചെയ്യുന്ന കാര്യങ്ങൾ മറച്ചുവെയ്ക്കുക.

നിങ്ങളുടെ വ്യക്തിപരമായ വിവരങ്ങൾ, പുറത്തറിയില്ല എന്നുള്ളതും ഇത്തരം അശ്ലീല സൈറ്റുകൾ എളുപ്പത്തിൽ വിരൽതുമ്പിൽ ലഭ്യമാകുന്നു എന്നുള്ളത് നിങ്ങളെ ഇത്തരം പ്രവർത്തനങ്ങളിലേയ്ക്ക് ആകർഷിച്ചേക്കാം.

***Slide 10***

**എന്നാൽ ഇതിന്റെ അനന്തര ഫലങ്ങൾ എന്തെല്ലാമാണെന്ന് നോക്കാം.**

1. ശാരീരികമായും മാനസികമായും ആരോഗ്യ പ്രശ്നങ്ങൾ
2. സെക്സ് കുറ്റകൃത്യങ്ങൾ ചെയ്യുവാനുള്ള വാസന.
3. സ്ത്രീകളെ സെക്സ് objects മാത്രമായി കാണാനുള്ള പ്രവണത.
4. സമയനഷ്ടം
5. പ്രായപൂർത്തി ആകാത്തവരിലെ ഗർഭധാരണം .

**ഇത് എങ്ങനെ ഒഴിവാക്കാം?**

1. അനാവശ്യകാര്യങ്ങൾക്കായി ഓൺലൈനിൽ ചിലവിടുന്ന സമയം കുറച്ചുകൊണ്ടുവരിക.
2. അസ്ലീല സൈറ്റുകൾ ബ്ലോക്ക് ചെചെയ്യുക.
3. പാചകം, വ്യായാമം, വായന മുതലായ മറ്റു വിനോദങ്ങൾക്കായി സമയം ചിലവിടുക.
4. അശ്ലീല സൈറ്റുകൾ ഉപയോഗിക്കുന്നതിൽ നിന്നും നിങ്ങൾക്ക് സ്വയം പിൻതിരിയാൻ സാധിക്കുന്നില്ലെങ്കിൽ മാതാപിതാക്കളുടേയോ സുഹൃത്തുക്കളുടേയോ സഹായം അഭ്യർത്ഥിക്കുക.

## വിഷാദരോഗം

***Slide 11***

നിങ്ങൾക്കറിയാമോ, ഇന്റർനെറ്റിന് അടിമപ്പെട്ട കുട്ടികളിലാണ് വിഷാദരോഗവും മറ്റു മാനസികവൈകല്യങ്ങളും കൂടുതലായി കണ്ടു വരുന്നത്. ഇന്റർനെറ്റിന് അടിമപ്പെട്ട കുട്ടികൾക്ക് യഥാർത്ഥ ലോകവും ഇന്റർനെറ്റിൽ അവർ കണ്ടുവരുന്ന സാങ്കൽപിക ലോകവും തമ്മിലുള്ള അന്തരം ഉൾകൊള്ളാൻ ബുദ്ധിമുട്ടുണ്ടാകുന്നു. കാരണം സാങ്കൽപികലോകം യാഥാർത്ഥ്യലോകത്തേക്കാൾ എത്രയോ ആകർഷണീയവും രസകരവുമായി അവർക്ക് അനുഭവപ്പെടുന്നു.

## ദീർഘകാലത്തെ ഇന്റർനെറ്റ് ഉപയോഗം മൂലമുണ്ടാകുന്ന ശാരീരിക വൈകല്യങ്ങൾ

***Slide 12***

അമിതവണ്ണം – ഇന്റർനെറ്റിന്റെ അമിത ഉപയോഗം വ്യായാമം ഇല്ലാതാക്കുകയും അതുമൂലം ശരീരത്തിൽ കൊഴുപ്പ് അടിഞ്ഞുകൂടി അമിത വണ്ണം വരുത്തുന്നതിന് കാരണമാകുന്നു.

Posture തകരാറുകൾ – ഒരുപാട് നേരത്തെ കമ്പൂട്ടർ ഉപയോഗത്തിനിടയ്ക്ക് ഇടക്കിടെ ഇടവേളകൾ എടുക്കുകയും, കമ്പൂട്ടർ ഉപയോഗിക്കുമ്പോൾ ശരിയായ രീതിയ്ൽ ഇരിക്കുകയും ചെയ്യുന്നതിലൂടെ ഇത്തരത്തിലുള്ള തകരാറുകൾ ഒഴിവാക്കാം. ഇല്ലെങ്കിൽ ഇത് പുറം കഴുത്ത്, തോൾ, തല, കണ്ണ്, കൈകൾ എന്നിവിടങ്ങളിൽ വേദനയ്ക്കു കാരണമാകുന്നു.

സന്ധിവേദന  കമ്പൂട്ടറിനുമുന്നിൽ ഒരുപാട് നേരം ഇരിക്കുന്നതും ഉപയോഗിക്കുന്നതും സന്ധിവേദനയ്ക്ക് കാരണമാകുന്നു. ഞരമ്പുകളിൽ നേരിട്ട് വരുന്ന സമ്മർദ്ദം വേദനകൾക്ക് കാരണമാകുന്നു. കൈകുഴകളും കൈ മുട്ടുകളും വേദന ഉണ്ടാക്കാൻ സാധ്യതകളുള്ള സ്ഥലങ്ങളാണ്.

***Slide 13/14/15***

കമ്പ്യൂട്ടർ ഉപയോഗിക്കുമ്പോൾ posture- ൽ സാധാരണയായി കണ്ടുവരുന്ന ചില തെറ്റുകൾ

1. കണ്ണിന്റെ ഒരേ നിലയിൽ മോണിറ്റർ വെയ്ക്കാതിരിക്കുന്നത്.
2. കാലുകൾ കൂടുതൽ നേരം ഒരേ രീതിയിൽ വെക്കുന്നത്.
3. തോളുകൾ മുന്നോട്ടാഞ്ഞ് ഇരിക്കുന്നത്
4. മൗസും കീബോർഡും ദൂരത്തിൽ വെക്കുന്നത്.
5. ഫോൺ തോളിൽ വെച്ച് സംസാരിക്കുന്നത്.

ഇതിനു പുറമെ മൗസും കീ ബോർഡും തെറ്റായ രീതിയിൽ ഉപയോഗിക്കുന്നതിന്റെ ചിത്രങ്ങളും ഇവിടെ കാണാം.

***Slide 16***

ഇതിൽ കമ്പ്യൂട്ടർ ഉപയോഗിക്കുമ്പോൾ ഇരിക്കേണ്ട ശരിയായ posture കാണിച്ചിരിക്കുന്നു.

**ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ**

1. കണ്ണിന്റെ അതേ ലെവലിൽ മോണിറ്റർ വെക്കണം
2. കാലുകൾ നിലത്ത് ഉറപ്പിച്ചിരിക്കണം

3. കൈകുഴകളും കീബോഡും മൗസും ഒരേ ലെവൽ ആയിരിക്കണം.
4. ഫോൺ തോളിൽ വെക്കാതെ headphone ഉപയോഗിക്കുക.
5. മുന്നോട്ടോ, പിന്നോട്ടോ ആയാതെ നേരെ ഇരിക്കുക.
   ഒപ്പം തന്നെ കീ ബോർഡും മൗസും എങ്ങനെ ശരിയായി ഉപയോഗിക്കാം എന്നും ഇതിൽ കാണാം.

# Cyber Threats and Laws

## ***Slide -1***

Computer- ന്റെയും Internet-ന്റെയും ഉപയോഗം കൂടി വരുന്നതിനനുസരിച്ച് നമ്മുടെ സമൂഹത്തിൽ ഇന്റർനെറ്റിൽ കൂടിയുള്ള കുറ്റ കൃത്യങ്ങളും കൂടി വരികയാണ്. എന്തെല്ലാമാണ് അവയെന്നും അതിലെങ്ങനെ അകപ്പെടാതി രിക്കാം എന്നും നമുക്ക് നോക്കാം.

## ***Slide -2***

ഇന്റർനെറ്റ് വഴിയുള്ള കുറ്റകൃത്യങ്ങളിൽ പലതിന്റേയും പ്രധാന കാരണം Password- ന്റെ തെറ്റായ രീതി യിലുള്ള ഉപയോഗം ആണ്. 5-ൽ ഒരാൾ വീതം ഡാറ്റയുടെ ദുരുപയോഗത്തിന് വിധേയമാകുന്നു എന്നാണ് കണക്കുകൾ കാണിക്കുന്നത്.

ഏതൊരു account ഉണ്ടാകുമ്പോഴും അതിനു ഒരു password ഉണ്ടാകും. ഈ password ആണ് ആ വെബ് സൈറ്റ് അല്ലെങ്കിൽ അക്കൗണ്ടിലേക്കുള്ള key. നിങ്ങളുടെ password മറ്റുള്ളവർ ദുരുപയോഗിക്കുന്നതിനു പല മാർഗ്ഗങ്ങൾ ഉണ്ട്. ഒരു വഴി നിങ്ങൾ തന്നെ നിങ്ങളുടെ password മറ്റുള്ളവർക്കു പറഞ്ഞു കൊടുക്കുന്നതാണ് (password sharing), മറ്റൊരു വഴി നിങ്ങൾ അറിയാതെ നിങ്ങളുടെ password മറ്റുള്ളവരുടെ അടുത്ത് എത്തുന്നതും (password leak)

## ***Slide -3***

നാം പലപ്പോഴും കേൾക്കാറുണ്ട് പല പ്രമുഖ വെബ് സൈറ്റിലും അക്കൗണ്ട് വിവരങ്ങൾ (പാസ് വേഡ് അടക്കം) ലീക്ക് ആകുന്നതിനെപ്പറ്റി എന്തുകൊണ്ട് ഇത് സംഭവിക്കുന്നു എന്നോ ആരാണ് ഇതിന്റെ പുറ കിൽ എന്നോ നിങ്ങൾ ചിന്തിച്ചിട്ടുേ ാ.

## *Slide 4*

നിങ്ങളുടെ password leak ആകുന്നതിനു പ്രധാനമായും 2 കാരണങ്ങൾ ആണ് ഉള്ളത്.

### ബാഹ്യശക്തികളുടെ പ്രഭാവം-

ഇത് പലപ്പോഴും കൂട്ടായ അക്കൗണ്ട് ഡീറ്റെയിൽസ് ലീക്കിന് കാരണമാകുന്നു. ഇത് രണ്ടു വിധത്തിൽ സംഭവിക്കാം

- മറ്റുള്ളവർ പാസ്സ്വേർഡ് ടൈപ്പ് ചെയുന്നത് അവർ അറിയാതെ മനസ്സിലാകുക
- പാസ്സ്വേർഡ് ഹാക്ക് ചെയ്തു കണ്ടു പിടിക്കുക

### ഇതിൽ നിന്ന് രക്ഷ നേടാനുള്ള വഴികൾ എന്തെല്ലാം

1. എപ്പോഴും എല്ലാ അക്കൗണ്ടുകൾക്കും ശക്തമായ Password ഉപയോഗിക്കുക.
2. മറ്റു ആപ്ലിക്കേഷൻസിന് അക്കൗണ്ട് ഉപയോഗിക്കാനുള്ള **Access** എടുത്തു കളയുക.

3. അനുവദനീയമെങ്കിൽ 2 സ്റ്റെപ്പ് authentication (password-ന്റെ കൂടെ മറ്റൊരു step –ന്റെ കൂടെ മറ്റൊരു സ്റ്റെപ്പ് authentication കൂടെ, eg..one time password ഉപയോഗിക്കുക.)

### അശ്രദ്ധമായ ഉപയോഗം

Password നഷ്ടപ്പെടുന്നതിന് മറ്റൊരു കാരണം ആണ് അശ്രദ്ധമായ ഉപയോഗം. ഇതൊഴിവാക്കാൻ വേണ്ടി ഇനി പറയുന്ന കാര്യങ്ങൾ ശ്രദ്ധിക്കണം.

1. പാസ്വേഡ് ഒരിക്കലും എഴുതിവെയ്ക്കരുത്
2. പല സൈറ്റിലെ അക്കൗ ുകൾക്ക് ഒരേ പാസ്വേഡ് ഉപയോഗിക്കരുത്
3. പൊതുവായ വാക്കുകൾ പാസ്വേഡ് ആയി ഉപയോഗിക്കാതിരിക്കുക.
4. വ്യക്തിപരമായ വിവരങ്ങൾ പാസ്വേഡിൽ ഉപയോഗിക്കാതിരിക്കുക.
5. കഫേയിലോ മറ്റോ അക്കൗണ്ട് പരിശോധിച്ച ശേഷം ലോഗ് ഔട്ട് ചെയ്യാൻ ശ്രദ്ധിക്കുക.

## ***Slide 5***

### Password Sharing

നിങ്ങളുടെ കൂട്ടുകാരുമായോ മറ്റുള്ളവരുമായോ password പങ്കുവെയ്ക്കാൻ ഉള്ള പ്രവണത ഇടയ്ക്ക് നിങ്ങൾക്ക് ഉണ്ടായേക്കാം. എന്തെന്നാൽ അതുവഴി നിങ്ങളുടെ ജോലി എളുപ്പം ആകാം എന്ന് നിങ്ങൾ കരുതുന്നു. എന്നാൽ പ്രധാനപ്പെട്ട അക്കൗണ്ടുകളിലൂടെ സുഹൃത്തുക്കളുമായോ, എന്തിന് കുടുംബാംഗങ്ങളുമായി പോലും പങ്കുവെയ്ക്കാൻ പാടുള്ളതല്ല. കാരണം അവർ നിങ്ങളുടെ password ദുരുപയോഗം ചെയ്താൽ അതിന്റെ പൂർണ്ണ ഉത്തരവാദിത്വം നിങ്ങൾക്കുമാത്രമായിരിക്കും.

നിങ്ങളിൽ പലരും ചിന്തിക്കുന്നുണ്ടാകും നിങ്ങളുടെ password കിട്ടിയതുകൊണ്ട് മറ്റുള്ളവർക്കുള്ള ഗുണമെന്താണെന്ന്. അതൊരു e-commence-site –ന്റെ password ആണെങ്കിൽ അവർക്ക് നിങ്ങളുടെ വിവരങ്ങൾ ഉപയോഗിച്ച് സാധനങ്ങൽ വാങ്ങാൻ സാധിക്കും. പോട്ടെ, നിങ്ങളുടെ ഇ–മെയിലിൽ നിന്ന് മറ്റുള്ളവർക്ക് അനാവശ്യമായ ഒരു mail അയച്ചാലുള്ള ഭവിഷ്യത്തുകൾ എന്തായിരിക്കും എന്ന് ആലോചിച്ചുനോക്കാൻ സാധിക്കുമോ.

## ***Slide -6***

നിങ്ങളുടെ password ആരെങ്കിലും ദുരുപയോഗിച്ചാലുള്ള ഫലങ്ങൾ എന്താണെന്നു അറിയാമോ

- നിങ്ങളുടെ പാസ്വേഡ് ഉപയോഗിച്ച് നിങ്ങളുടെ അക്കൗണ്ടിൽ നിന്ന് ആരെങ്കിലും നിയമ വിപരീതമായി എന്തു ചെയ്താലും അതിന്റെ ഉത്തരവാദിത്വം ഏറ്റെടുക്കേണ്ടി വന്നേക്കാം.
- ബാങ്ക് അക്കൗണ്ട് മുതലാവയുടെ വിവരങ്ങൾ ചോരുന്നതുമൂലം അക്കൗണ്ടിൽ നിന്ന് പണം നഷ്ടമാകാൻ സാധ്യതയേറുന്നു.
- നിങ്ങളുടെ വ്യക്തിപരമായ കാര്യങ്ങൾ മറ്റുള്ളവർ അറിയാൻ ഇട വരുന്നു. നിങ്ങളുടെ മെയിലിൽ നിന്ന് അനാശ്യാസ പ്രവർത്തനങ്ങൾ നടത്താൻ ഇട വരികയും അതിലൂടെ നിങ്ങളുടെ പ്രതിച്ഛായ മോശമാവാനുള്ള അവസ്ഥ വരികയും ചെയ്യും.
- രാജ്യത്തെ സുരക്ഷാ ഉദ്യോഗസ്ഥരുടെ അക്കൗണ്ട് വിവരങ്ങൾ ചോരുന്നതുമൂലം രാജ്യ രക്ഷാ സംബന്ധമായ കാര്യങ്ങൾ ശത്രുക്കൾക്ക് ലഭിക്കാൻ ഇടവരുന്നു.

## ***Slide 7***

അത് കൊണ്ട് എപ്പോഴും സ്ട്രോങ്ങ് ആയുള്ള പാസ്വേഡ് ഉപയോഗിക്കുക. അതിനായി passphrases കണ്ടു പിടിക്കുക.

## *Slide 8/9*

**കമ്പ്യൂട്ടർ ഹാക്കിംഗ്**

ഹാക്കിംഗ് എന്ന സാങ്കേതിക വിദ്യ ആദ്യകാലങ്ങളിൽ ഉപയോഗിച്ചിരുന്നത്, കമ്പ്യൂട്ടറുകളുടെ പ്രവർത്തന മികവിനുവേണ്ടിയും പ്രവർത്തന വേഗത കൂട്ടുന്നതിനുവേണ്ടിയുമായിരുന്നു. എന്നാൽ പിന്നീട് ഹാക്കിംഗ് ദുരുപയോഗപ്പെടുത്താൻ തുടങ്ങി. ഹാക്കിംഗിനെ വെറ്റ് ഹാക്ക് ഹാക്കിംഗ് എന്നും ബ്ലാക്ക് ഹാറ്റ് ഹാക്കിംഗ് എന്നും തരം തിരിക്കാം. നല്ല പ്രവർത്തനങ്ങൾ ചെയ്യുന്നതിന് വെറ്റ് ഹാക്കിംഗ് എന്നും ദുരിപയോഗപ്പെടുത്തുന്നതിനെ ബ്ലാക്ക് ഹാക്കിംഗ് എന്നും പറയുന്നു.

## *Slide 10*

**നിങ്ങളുടെ കമ്പ്യൂട്ടർ എത്ര സുരക്ഷിതമാണ്?**

കമ്പ്യൂട്ടറിനെ ആക്രമിക്കുവാനായി ഹാക്കർസ് ദിനംപ്രതി പുതിയ വഴികൾ കണ്ടുപിടിച്ചുകൊണ്ടിരിക്കുകയാണ്. ഇതിനെ ചെറുക്കുവാൻ സോഫ്റ്റ് വെയർ കമ്പനികൾ തങ്ങളുടെ സോഫ്റ്റ് വെയർ കോഡുകൾ സങ്കീർണ്ണമാക്കുകയും പുതിയ പാച്ചുകൾ കണ്ടെത്തുകയും ചെയ്യുന്നു.

## *Slide 11*

**ഹാക്കറെ എങ്ങനെ കണ്ടു പിടിക്കാം**

ഹാക്ക് ചെയ്ത് കടന്നുകളയാൻ എളുപ്പമല്ല. മറ്റു കുറ്റകൃത്യങ്ങൾക്ക് എന്ന പോലെ സൈബർ കുറ്റകൃത്യങ്ങൾ ചെയ്യുന്നവരെ കണ്ടു പിടിക്കാനും ഇന്ന് മാർഗ്ഗങ്ങൾ ഏറെ ആണ്. ഹാക്കർ ഉപേക്ഷിച്ചുപോകുന്ന ഒരു ചെറിയ തെളിവിലൂടെ പോലും ഇത് സാധ്യമാകും. കുറ്റവാളി ഉപയോഗിച്ച കമ്പ്യൂട്ടറിന്റെ ഐ.പി. അഡ്രസ്സിലൂടെ ലൊക്കേഷൻ കണ്ടുപിടിക്കാനും സാധിക്കും.

മുബൈ പോലീസ് കൽബേഷ് എന്ന യുവാവിനെ ഒരു ധനകാര്യ സ്ഥാപനത്തിന്റെ വെബ്സൈറ്റ് ഹാക്കിംഗ് ചെയ്തു എന്ന കുറ്റകൃത്യത്തിന്റെ പേരിൽ അറസ്റ്റ് ചെയ്തത് ഈ അടുത്താണ്.

## *Slide 12/13*

**മാൽവെയർ, സ്പൈവെയർ, ട്രോജൻ പോഴ്സ്, വൈറസ്**

കംമ്പ്യൂട്ടറിനെ തകരാറിലാക്കുന്ന പ്രോഗ്രാമുകളെ ആണ് മാൽവെയർ എന്ന് പറയുന്നത്.

## *Slide 14*

**ട്രോജൻ ഹോഴ്സ്**

ഇത് ഒരു തരം മാൽവെയർ ആണ്. ഒറ്റ നോട്ടത്തിൽ വ്യാജമാണെന്ന് തോന്നാത്ത ഫയലുകളോ പ്രോഗ്രാമുകളോ ആവാം. ഉപഭോക്താക്കൾ ഇവ ഡൗൺലോഡ്-ഉം ഇൻസ്റ്റാളും ചെയ്യുന്നതിലൂടെ അവരുടെ കംമ്പ്യൂട്ടറുകൾ ആക്രമിക്കപ്പെടുന്നു.

## *Slide 15*

**സ്പൈവെയർ**

ഉപഭോക്താക്കൾ അറിയാതെ അവർ കംമ്പ്യൂട്ടറിൽ ചെയ്യുന്ന പ്രവർത്തനങ്ങളെ റെക്കോർഡ് ചെയ്യുകയും ദുരുപയോഗം ചെയ്യുകയും ചെയ്യുന്നതാണ് സ്പൈവെയർ. (അക്കൗണ്ട് ഇൻഫൊർമേഷൻ, ലോഗിൻ, സാമ്പത്തിക വിവരങ്ങൾ എന്നിവ ചോർത്താൻ സ്പൈവെയർ ഉപയോഗിക്കുന്നു.

## *Slide 16*

**വൈറസ്**

സ്വയം മറ്റ് കംമ്പ്യൂട്ടറുകളിലേയ്ക്ക് പടർന്ന് പിടിക്കാനും ആക്രമിക്കാനും കഴിവുള്ള മാൽവെയറുകൾ ആണ് വൈറസ്. വൈറസ് ഉള്ള പ്രോഗ്രാമുകൾ ഉപയോഗിക്കുന്നതിലൂടെ കംമ്പ്യൂട്ടറിലെ വിവരങ്ങൾ

മോഷ്ടിക്കപ്പെടുവാനും തുടർന്ന് ദുരുപയോഗപ്പെടുത്തുവാനും സാധിക്കുന്നു. സ്വയം പകർപ്പുണ്ടാക്കുകയും മറ്റു കംമ്പ്യൂട്ടറുകളിലേയ്ക്ക് പടരുകയും ചെയ്യുന്ന മാൽവെയറുകളെ worm എന്നും പറയാറുണ്ട്.

Adware
നിങ്ങളുടെ കംമ്പ്യൂട്ടറുകളിൽ ചെയ്യുന്ന ജോലിയെ തടസ്സപ്പെടുത്തികൊണ്ട് സ്ക്രീനിൽ ഇടയ്ക്ക് ഇടയ്ക്ക് പരസ്യങ്ങൾ പ്രത്യക്ഷപ്പെടാൻ കാരണം ഈ വിരുതനാണ്.

----------Supporting Document----------

## സ്റ്റോറി (Story)

ദിലീപിന്റെ ബാങ്ക് അക്കൗണ്ടിൽ നിന്ന് 10,20, രൂപ കണക്കിൽ ചെറിയ രീതിയിൽ പണം നഷ്ടപ്പെടാൻ തുടങ്ങി. ആദ്യം അദ്ദേഹം അത് അവഗണിച്ചെങ്കിലും പിന്നീട് അക്കൗണ്ടിൽ നിന്നും നഷ്ടപ്പെടുന്ന തുക കൂടാൻ തുടങ്ങി. ദിലീപ് തന്റെ ബാങ്ക് അക്കൗണ്ട് പാസ്വേർഡ് മാറ്റുകയും ബാങ്കിന്റെ കാർഡുകൾ ക്യാൻസൽ ചെയ്യുകയും ചെയ്തു. എന്നാൽ പണം നഷ്ടപ്പെടുന്നത് തുടർന്നു കൊണ്ടേയിരുന്നു. ഇത്തരം സന്ദർഭങ്ങളിൽ നമ്മൾ എന്ത് ചെചെയ്യണം. എത്രയും പെട്ടന്ന് ബാങ്കുമായി ബന്ധപ്പെട്ട് വിവരങ്ങൾ അറിയിക്കുക. നിങ്ങളുടെ കംമ്പ്യൂട്ടറിൽ ഏറ്റവും  നൂതനമായ ആന്റി വൈറസ് ഇൻസ്റ്റാൾ ചെയ്യുകയും വേണം.

## സ്റ്റോറി (Story)

ഗോപി തന്റെ പഴയ കാർ വിൽക്കുന്നതിനായി ഒരു ഓൺ ലൈൻ സൈറ്റിൽ പരസ്യം ചെയ്തു. ദിവസങ്ങൾക്കുള്ളിൽ കാർ വിൽപ്പന നടക്കുകയും ചെയ്തു. അതുകൊണ്ടു തന്നെ താൻ കൊടുത്ത പരസ്യം പിൻവിലച്ചു. എന്നാൽ അടുത്ത ദിവസം താൻ കൊടു ത്ത അതേ പരസ്യം ഇമെയിൽ അഡ്രസ്സ് മാത്രം മാറ്റി മറ്റൊരാൾ അതേ സൈറ്റിൽ പോസ്റ്റ് ചെയ്തത് ഗോപി കണ്ടു. ഇയാളെ പിടികൂടുന്നതിനായി ഗോപി, കാർ വാങ്ങുവാൻ താൽപര്യപ്പെടുന്ന ഒരു ആൾ എന്ന വ്യാജേന ഇയാളെ ബന്ധപ്പെടുകയും ഇയാളുടെ പേരു വിവരങ്ങൾ പോലീസിനു കൈമാറുകയും ചെയ്തു.

*ഇത്തരം അവസരങ്ങളിൽ എന്ത് ചെയ്യണം?*
വ്യാജം എന്ന് തോന്നുന്ന ഏതൊരു ഇന്റർനെറ്റ് ഇടപാടിന്റേയും വിശ്വസനീയമല്ലാത്ത ഒരു സൈറ്റുകളിലും പരസ്യപ്പെടാതിരിക്കുക.

----------Supporting Document----------

## ***Slide 17***

മാൽവെയറുകളുടെ ലക്ഷണങ്ങൾ

മാൽവെയറുകളാൽ ആക്രമിക്കപ്പെട്ട കംമ്പ്യൂട്ടറുകൾ താഴെ പറയുന്ന ലക്ഷണങ്ങൾ കാണിക്കുന്നു.

- CPU ഉപയോഗം കൂടുന്നു.
- കംമ്പ്യൂട്ടർ വേഗത കുറയുന്നു.
- നെറ്റ് വർക്ക് സംബന്ധമായ പ്രശ്നങ്ങൾ
- കംമ്പ്യൂട്ടർ ക്രാഷ് ആകുന്നു.
- അപരിചിതമായ ഫയലുകൾ, പ്രോഗ്രാമുകൾ മുതലായവ പ്രത്യക്ഷപ്പെടുന്നു.
- നിങ്ങളറിയാതെ നിങ്ങളുടെ ഇ-മെയിലിൽ നിന്നും മറ്റുള്ളവർക്ക് മെയിലുകൾ അയക്കപ്പെടുന്നു.

## *Slide 18*

**സ്പാം** (Spam)

**email സ്പാം**

അനാവശ്യമായ പരസ്യ വാചകങ്ങളും ചിത്രങ്ങളും ഉൾപ്പെട്ട ഇ–മെയിലുകൾ ഒരു കൂട്ടം ആളുകൾക്ക് മെയിൽ രൂപത്തിൽ അയയ്ക്കുന്നതിനെയാണ് സ്പാം എന്ന് പറയുന്നത്. ഇത്തരം സ്പാം മെയിലുകളെ ചെറുക്കുന്നതിന് ഗവൺമെന്റ് തലത്തിൽ എടുത്തു വരുന്ന നടപടികൾ വഴി ഒരു പരിധിവരെ ഫലം കാണുന്നുണ്ട്.

**SMS സ്പാം**

ഇ–മെയിൽ സ്പാമിന്റെ അത്രയും അപകടകാരികൾ അല്ല എസ്.എം.എസ്. സ്പാം. ഇൻസ്റ്റന്റ് മെസെജിംഗ് സംവിധാനങ്ങൾ ആയ സ്കൈപ്പ് മുതലായവയിലൂടെ ആണ് എസ്.എം.എസ് സ്പാം പടരുന്നത്. വ്യാജ പരസ്യങ്ങൾ, അതായത് തടി കുറയ്ക്കാം, ലോൺ ചൂതുകളി, അശ്ലീല വെബ്സൈറ്റുകൾ മുതലായവയുടെ പരസ്യങ്ങൾ, ആയാണ് ഇവ പ്രത്യക്ഷപ്പെടുന്നത്. ഇവയ്ക്ക് പുറമെ മൊബൈൽ ഫോൺ സ്പാം സോഷ്യൽ നെറ്റ് വർക്കിംങ്ങ് സ്പാം എന്നിവയും ഇന്ന് ഒരുപാട് കാണപ്പെടുന്നു ്.

## *Slide 19*

**ഫിഷിംഗ്** (Phishing)

ആളുകളുടെ യൂസർ നെയിം, പാസ്വേഡ്, ക്രെഡിറ്റ് കാർഡ് വിവരങ്ങൾ എന്നിവ ചോർത്തുന്നതിനെ ആണ് ഫിഷിംഗ് എന്ന് പറയുന്നത്.

## *Slide 20/21*

**വിവിധ തരം ഫിഷിംഗ്**

1. **തെറ്റായ** URL- **കൾ**

ഫിഷിംഗ് മെസേജുകളിലും മെയിലുകളിലും പ്രത്യക്ഷപ്പെടുന്ന URL ഒറ്റ നോട്ടത്തിൽ വ്യാജമെന്ന് തോന്നുകയില്ല. ഈ URL കളുടെ മുകളിൽ നിങ്ങൾ മൗസ് കൊണ്ടുവെയ്ക്കുമ്പോൾ യഥാർത്ഥത്തിൽ ഉള്ള അഡ്രസ്സ് കാണാവുന്നതാണ്. ഈ അഡ്രസ്സ് നേരത്തേ കണ്ടതിൽ നിന്നും വ്യത്യസ്തമാണെങ്കിൽ ഈ മെസേജ് വ്യാജനാവാൻ സാധ്യത കൂടുതലാണ്.

2. **തെറ്റായ ഡൊമൈൻ നെമിം ഉൾപ്പെട്ട URL**

ഡൊമൈൻ നെയിമിന്റെ അവസാന ഭാഗത്തുനിന്നു വേണം URL വ്യാജമോ അല്ലയോ എന്ന് കണ്ടുപിടിക്കാൻ. ഡൊമൈൻ നെയിമിന്റെ ആദ്യ ഭാഗത്ത് ആപ്പിൾ, മൈക്രോസോഫ്റ്റ് മുതലായ കമ്പനികളുടെ പേരുകൾ വ്യാജന്മാർ ഉപയോഗിക്കുന്നു.

ഉദാഹരണം

Apple.abc.com ഇത്തരം ഒരു URL കാണുമ്പോൾ ആപ്പിൾ എന്ന കമ്പനിയിലുള്ള വിശ്വാസത്തിനു പുറത്ത് ക്ലിക്ക് ചെയ്യുകയും തുടർന്ന് ഉപയോഗിക്കുകയും ചെയ്യുന്നു. ഇതിൽ ‘‘sbc’’ വ്യാജനാണ്.

3. e-mail അഥവാ മെസേജുകളിൽ ഉപയോഗിച്ചിരിക്കുന്ന ഭാഷ, വ്യാകരണം മുതലായവയിൽ തെറ്റുകൾ ഉണ്ടെങ്കിൽ അത് വ്യാജമാവാൻ ആണ്. സാധ്യത. പ്രശസ്തമായ കമ്പനികൾ അയക്കുന്ന മെയിലുകളിൽ ഇത്തരം തെറ്റുകൾ വരില്ല.
4. നിങ്ങളുടെ ഏതെങ്കിലും ഓൺലൈൻ ഇടപാടുകളുടെ അക്കൗണ്ടിന്റെ യൂസർ നെയിം, പാസ്വേഡ് മുതലായവ വിവരങ്ങൾ ചോദിച്ചുകൊണ്ട് വരുന്ന അഭ്യ ർത്ഥനകൾ വ്യാജമാവാനാണ് സാധ്യത.

5. അവിശ്വസനീയമായ രീതിയിലുള്ള ഓഫറുകൾ/ വാഗ്ദാനങ്ങൾ മുതലായവ നൽകികൊണ്ട് വരുന്ന മെസേജ്/മെയിൽ വ്യാജമാവാൻ സാധ്യത ഏറെയാണ്.
6. ഓൺലൈൻ ആയി പണം അടച്ചാൽ മോഹിപ്പിക്കുന്ന ഓഫറുകൾ/ജോലിവാഗ്ദാനങ്ങൾ മുതലായവ തരുന്ന ലെയിലുകൾ 90% വ്യാജമായിരിക്കും.
7. നിങ്ങൾ എടുക്കാത്ത ലോട്ടറി എടുത്തു എന്നു പറഞ്ഞുവരുന്ന മെയിൽസ്
8. പണം ആവശ്യപ്പെട്ടുകൊണ്ടുള്ള മെയിലുകൾ
9. ഭീഷണിയുടെ സ്വരത്തിലുള്ള മെയിലുകൾ

## ***Slide 21***

Phishing-ൽ പെടാതെ എങ്ങനെ ശ്രദ്ധിക്കാം.

1. നേരത്തെ പറഞ്ഞ സൂചനകളിൽ നിന്ന Phishing mails കണ്ടു പിടിക്കാൻ പഠിക്കുക.
2. വരുന്ന മെയിലുകളുടെ ശ്രോതസ്സ് ഉറപ്പു വരുത്തുക.
3. മെയിലുകളിലെ links ഉപയോഗിച്ച് ബാങ്കിംങ്ങ് സൈറ്റ് സന്ദർശിക്കാതിരിക്കുക.
4. കംമ്പ്യൂട്ടർ സെക്യൂരിറ്റി എപ്പോഴും അപ്ഡേറ്റഡായി സൂക്ഷിക്കുക.
5. വ്യക്തിപരമായ വിവരങ്ങൾ Secure ആയിട്ടുള്ള (htips) sitil- ൽ മാത്രം കൊടുക്കുക.
6. അക്കൗണ്ട്സ് കൃത്യമായി ചെക്ക് ചെയ്യുകയും പാസ്വേഡ് മാറ്റുകയും ചെയ്യുക.
7. ഏതെങ്കിലും തരത്തിലുള്ള സംശയം ഉണ്ടെങ്കിൽ ആ മെയിലുകൾ തുറക്കാതിരിക്കുക.
8. അനുവദനീയമായ എല്ലാ സൈറ്റിലും 2 സ്റ്റെപ്പ് authentification enable ചെയ്യുക

# അശ്ലീല സാഹിത്യം /അസഭ്യചിത്രം (Pornography)

## ***Slide - 22***

Pornography– യുടെ അപകടങ്ങൾ എന്തെല്ലാം എന്ന് നോക്കാം

### 1. ശാരീരികാസ്വാസ്ഥ്യങ്ങൾ

Pornography ഓരോരുത്തരിലും ഉണ്ടാക്കുന്ന പ്രഭാവം വ്യത്യസ്തമാണ്. പലതരത്തിലുള്ള ലൈംഗിക പ്രശ്നങ്ങളും ഉണ്ടാകാൻ ഇത് കാരണമാകാം.

### 2. ബാലപീഢനം

ലോകത്താകമാനം ഒരുപാട് കുട്ടികളാണ് Pornography-.യുടെ അതിപ്രസരം മൂലം ബാലപീഢനത്തിന് ഇരയാകുന്നത്. രേഖപ്പെടുത്തപ്പെടുത്തപ്പെട്ടിട്ടുള്ള കേസുകളിൽ നിന്നു തന്നെ ഊഹിക്കാവുന്നതാണ്. യഥാർത്ഥത്തിൽ എത്രപേർ ഇതിന് ഇരകളാകുന്നുണ്ടാകും എന്നത്.

### 3. സ്ത്രീകളോടുള്ള ബഹുമാനം നഷ്ടപ്പെടാൻ കാരണം

അശ്ലീല ചിത്രങ്ങൾ തുടർച്ചയായി കാണുന്നത് സ്ത്രീകളെ തരം താഴ്ത്തി കാണാൻ ഇടയാക്കുന്നു. ആഗ്രഹങ്ങൾ പൂർത്തീകരിക്കാനുള്ള വെറും വസ്തുക്കൾ മാത്രമായി സ്ത്രീകൾ ചിത്രീകരിക്കപ്പെടുന്നു.

### 4. സ്ത്രീകളെയും കുട്ടികളെയും അപമാനിക്കുന്ന തരം കുറ്റ കൃത്യങ്ങളിൽ ചെന്നു ചാടാൻ കാരണമാകുന്നു.

നിങ്ങൾ അശ്ലീലചിത്രങ്ങൾ കാണുന്നതുവഴി അതിന്റെ നിർമ്മാതാക്കളെ സാമ്പത്തികപരമായി സഹായിക്കുകയും അവരെ വീണ്ടും വീണ്ടും ഇത് തുടരാൻ പ്രോത്സാഹിപ്പിക്കുകയുമാണ് ചെയ്യുന്നത്. ലൈംഗികമായി ഒരു കുട്ടിയെ ഒരിക്കലും ഉപയോഗിക്കില്ല എന്ന് പറയുന്ന ഒരാളാണെങ്കിൽ കൂടിയും, അശ്ലീല ചിത്രങ്ങൾ കാണുക വഴി, അത്തരം പ്രവൃത്തികളെ പ്രോത്സാഹിപ്പിക്കുകയാണ് നിങ്ങൾ ചെയ്യുന്നത്.

**5. അത് നിങ്ങളുടെ ഭാവി നശിക്കുന്നതിനും പഠനം നഷ്ടമാകുന്നതിനും കാരണമാകുന്നു.**

നിങ്ങളുടെ മനസ് ഇത്തരം കാര്യങ്ങളിൽ മുഴുകിതുടങ്ങിയാൽ, നിങ്ങൾക്ക് പഠനത്തിൽ ശ്രദ്ധിക്കാൻ സാധിക്കാതെ വരും. Schools ഇത്തരം കാര്യങ്ങൾ നിരോധിച്ചിട്ടുണ്ടെങ്കിലും മറ്റുള്ള സമയത്ത് തുടർച്ചയായി അവ കാണുക വഴി അത് നിങ്ങളുടെ മനസ്സിനെ കീഴടക്കുകയും, മറ്റു കാര്യങ്ങളിൽ താൽപര്യം കുറയുകയും ചെയ്യും.

**6. നാണക്കേടിനും സ്വയം തരംതാഴ്ത്തലിനും ഇടയാക്കുന്നു.**

തെറ്റാണെന്ന് ഉറപ്പുള്ള ഒരു കാര്യം ചെയ്യുന്നതുകൊണ്ട് നിങ്ങൾക്ക് നിങ്ങളെ പറ്റി തന്നെ ഒരു മോശം അഭിപ്രായം രൂപപ്പെടുന്നു. അശ്ലീല ചിത്രങ്ങൾ കാണുമ്പോൾ അത് തെറ്റാണ് എന്ന് നിങ്ങൾക്കു തന്നെ ഒരു തോന്നൽ ഉണ്ടാകുന്നു.

## അശ്ലീല ചിത്രങ്ങളിൽ നിന്നും എങ്ങനെ രക്ഷപ്പെടാം

1. നിങ്ങളുടെ സെർച്ച് എൻജിൻ സുരക്ഷിതമായ തിരച്ചിൽ (Safe Search) എന്ന സംവിധാനം. ചിട്ടപ്പെടുത്തി വെയ്ക്കുക
   ഗൂഗിൾ ഉപയോഗിക്കുന്നവർ
   //www.gogle.com/family safety/:
   യുട്യൂബ് പോലുള്ള സംവിധാനങ്ങൾ ഉപയോഗിക്കുന്നുണ്ടെങ്കിൽ അവയെല്ലാം സുരക്ഷിതമാണെന്ന് ഉറപ്പു വരുത്തുക.
2. നിങ്ങളുടെ കംമ്പ്യൂട്ടറോ, ഓപ്പറേറ്റിംഗ് സിസ്റ്റമോ നൽകിയിട്ടുള്ള "family safety tolls"എന്ന സംവിധാനം ഉപയോഗിക്കുക.
   വിൻഡോസ് & Mac ഓപ്പറേറ്റിംഗ് സിസ്റ്റങ്ങൾ ഈ സൗകര്യം ലഭ്യമാക്കിയിട്ടുണ്ട്.
3. ഇന്റർനെറ്റ് സെൻസർ പ്രവർത്തനക്ഷമമാക്കുക.
   a. Stay Focused ഉപയോഗിക്കുക. ഏതെല്ലാം വെബ്സൈറ്റുകൾ എത്ര സമയം ഉപയോഗിക്കാം തുടങ്ങിയ കാര്യങ്ങൾ നിയന്ത്രിക്കാനുള്ള സംവിധാനമാണ്. ഇത് നിങ്ങൾ അശ്ലീല ചിത്രങ്ങളുടെ വലയിൽ കുടുങ്ങിയിരിക്കുകയാണെങ്കിൽ അതിൽ നിന്നും രക്ഷ നേടാൻ ഇത് വളരെ ഫലപ്രദമാണ്.
   b. എല്ലാ വെബ് ബ്രൗസറുകളുടെയും ഇന്റർനെറ്റ് ഉപയോഗം നിയന്ത്രിയ്ക്കാൻ സഹായിക്കുന്ന Stop procrastinaling App ഉപയോഗിക്കുക. ഉപയോക്താക്കളെ അവരുടെ ആസക്തിയിൽ നിന്നും വിമുക്തരാക്കാൻ ഇത് സഹായിക്കുന്നു.
   c. നിങ്ങളുടെ വീട്ടിലെ ഉപകരണങ്ങൾ എല്ലാം ആക്ഷേപാർഹമായ ഉള്ളടക്കം ഉപ യോഗിക്കാൻ ആകാത്ത വിധം ആക്കാനായി Open DNS ഉപയോഗിക്കുക. സൗജന്യമായി ലഭ്യമായ ഈ സോഫ്റ്റ്വെയർ ഇത്തരത്തിലുള്ള എല്ലാ ഉള്ളടക്കത്തെയും തടഞ്ഞു നിർത്തും. സ്കൂളുകളെല്ലാം തുടർച്ചയായി ഉപയോഗിക്കുന്ന സംവിധാനമാണിത്. നിങ്ങളുടെ കുടുംബത്തെ ഇത് നന്നായി സംരക്ഷിക്കുകയും ചെയ്യുന്നു.

# സൈബർ തീവ്രവാദം (Cyber Terrorisum)

***Slide -23***

ബോംബിനേക്കാൾ വലിയ ആഘാതം കീബോർഡിലൂടെ സൃഷ്ടിക്കാൻ കഴിവുള്ളവരായിരിക്കും നാളത്തെ തീവ്രവാദികൾ.

തീവ്രവാദ പ്രവർത്തനങ്ങളിലെ ഇന്റർനെറ്റ് ഉപയോഗത്തെ സൂചിപ്പിക്കുന്ന വാക്കാണ് സൈബർ ഭീകര പ്രവർത്തനം (Cyber Terrorisum). വൈറസ്സുകളെയും മറ്റും ഉപയോഗിച്ച് പേഴ്സണൽ കംമ്പ്യൂട്ടറുകളെ ലക്ഷ്യം വെച്ച് ചെയ്യുന്ന പ്രവർത്തനങ്ങളെല്ലാം ഇതിന് ഉദാഹരണമാണ്.

**ഉദാഹരണം**

Logic Bomb

1982–ലെ ശീതയുദ്ധകാലത്ത്, റഷ്യയുടെ സൈബീരിയൻ പൈപ്പ് ലൈൻ ഓപ്പറേഷൻ പരാജയപ്പെടുത്താനായി (മിസൈൽ, ബോംബ് തുടങ്ങിയ പരമ്പരാഗത ആയുധങ്ങൾ ഉപയോഗിയ്ക്കാതെ CLA ഒരു വഴി കണ്ടു പിടിച്ചു. ''ലോജിക് ബോംബ്'' എന്ന ഒരു സംവിധാനം വഴി കംമ്പ്യൂട്ടർ പ്രോഗ്രാം കോഡിന്റെ ചെറിയ ഭാഗം ഉപയോഗിച്ച് സൈബീരിയൻ പൈപ്പ്ലൈൻ പ്രവർത്തനത്തെ നിയന്ത്രിക്കുന്ന കംമ്പ്യൂട്ടർ ശൃംഖലയെ തകർക്കാനുള്ള മാർഗ്ഗം വികസിപ്പിച്ചു. ഇതിന്റെ ആഘാതം വളരെ വലുതായിരുന്നു. ശൂന്യാകാശത്തു നിന്നുപോലും അത് ദൃശ്യമായിരുന്നുവെന്നത് ഇത് വ്യക്തമാക്കുന്നു.

## എപ്സിലോൺ (Epsilon)

ചരിത്രത്തിലെ ഏറ്റവും വലിയ സൈബർ ഭീകര പ്രവർത്തനങ്ങളിലൊന്നാണ് Epsilon – ലു ായ വിവരം ചോർത്തൽ. ജെ.പി.മോർഗൻ, ചേസ് ബെസ്റ്റ് മറ്റു പ്രധാന സാമ്പത്തിക ഇടപാടുകാർ, 2011–ലെ പ്രധാന കമ്പനികൾ തുടങ്ങിയവർക്ക് മാർക്കറ്റിംങ്ങ് സർവ്വീസുകൾ പ്രദാനം ചെയ്യുന്ന ഒരു പ്രധാന കമ്പനിയാണ് Epsilon. രേഖപ്പെടുത്തിയ കണക്കുകൾ പ്രകാരം 225 Million ഡോളർ വരെയാണ് അവർക്കു വന്ന നഷ്ടം. ഇ–മെയിൽ അഡ്രസ്സുകളായിരുന്നു അവരുടെ ലക്ഷ്യം. ക്രൂരകൃത്യങ്ങൾക്ക് അവ ഉപയോഗിക്കുകവഴി വളരെ വലിയ പ്രത്യാഘാതങ്ങൾ തന്നെ ഉണ്ടാകാൻ ഇടയു ായിരുന്നു.

### സൈബർ ഭീകര പ്രവർത്തനങ്ങളുടെ പ്രത്യേകതകൾ

- **അക്രമികളെ തിരിച്ചറിയാനുള്ള ബുദ്ധിമുട്ട്**
  ഭൂരിഭാഗം സൈബർ ക്രൂരകൃത്യങ്ങളുടേയും ശരിയായ ഉറവിടം കണ്ടെത്തുക എന്നത് ദുഷ്കരമായ കാര്യമായിതന്നെ നിലനിൽക്കുന്നു.
- **അതിർത്തികളുടെ അഭാവം**
  ലോകത്തിന്റെ ഏതു കോണിൽ നിന്നും, ചിലപ്പോൾ ഒരേ സമയം തന്നെ പലയിടങ്ങളിൽ നിന്നായി ആക്രമണങ്ങൾ മുളപൊട്ടാം.
- **പുരോഗമനത്തിന്റെ വേഗത**
  പുതിയ പുതിയ കാര്യങ്ങൾ കണ്ടെത്തുന്നതിന്റേയും, അത് ഉപയോഗിക്കാനുള്ള സാങ്കേതിക വിദ്യകൾ വികസിപ്പിച്ചെടുക്കുന്നതിന്റേയും ഇടയിലുള്ള ഇടവേള കുറഞ്ഞു വരുന്നു.
- **ചുരുങ്ങിയ ചിലവ്:-** ഇത്തരം ആക്രമണങ്ങൾക്കുപയോഗിക്കുന്ന സാങ്കേതിക വിദ്യകൾ ഉപയോഗിയ്ക്കാൻ എളുപ്പമുള്ളതും, ചിലവു കുറഞ്ഞതും, വ്യാപകമായി ലഭ്യമായതുമാണ്.

## ആന്റി വൈറസ്

***Slide -24***

കംമ്പ്യൂട്ടറിന് ഹാനികരമായ സോഫ്റ്റ് വെയറുകൾ കണ്ടുപിടിച്ച്, തടഞ്ഞ്, അവയെ ഇല്ലാതാക്കാനായ് ഉപയോഗിക്കുന്ന സോഫ്റ്റ് വെയർ ആണ് ആന്റി വൈറസ് അല്ലെങ്കിൽ ആന്റി മാൽവയർ സോഫ്റ്റ് വയറുകൾ.

കംമ്പ്യൂട്ടർ ലോകത്തിലെ പെനിസിലിൻ എന്നാണ് ആന്റി വൈറസ് അറിയപ്പെടുന്നത്.

### പ്രവർത്തിക്കുന്നത് എങ്ങനെ

അറിയപ്പെടുന്ന വൈറസുകളുടെ വിവരങ്ങൾ ഒരു ഡാറ്റാ കേബിൾ ആക്കി മെമ്മറിയിൽ ആന്റി വൈറസുകൾ സൂക്ഷിക്കുന്നു. ഇവയെ സ്കാൻ ചെയ്ത ഫയൽസുമായി താരതമ്യം ചെയ്ത് വൈറസുകളെ കണ്ടെത്തുന്നു. ഇങ്ങനെയാണ് ആന്റി വൈറസ് സോഫ്റ്റ്വെയറുകൾ പ്രവർത്തിക്കുന്നത്. ഇങ്ങനെ കണ്ടെത്തുന്ന

വൈറസുകളെ കംമ്പ്യൂട്ടറിന്റെ ഒരു സുരക്ഷിതമായ സ്ഥലത്തേയ്ക്ക് മാറ്റുന്നു. ആയതിനാൽ വൈറസുകൾക്ക് മറ്റു ഫയൽസിലേയ്ക്ക് പ്രവേശിക്കുവാനോ മറ്റു പ്രവർത്തനങ്ങൾക്ക് തടസ്സപ്പെടുത്തുവാനോ കഴിയില്ല.

### അടിസ്ഥാന ധർമ്മങ്ങൾ

1. കംമ്പ്യൂട്ടറിന്റെ പ്രവർത്തനത്തെ ബാധിക്കുമെന്ന് കരുതുന്ന ഫയൽസിനെ സ്കാൻ ചെയ്യുക.
2. നിശ്ചിത സമയങ്ങളിൽ നമ്മുടെ ഇടപെടലുകൾ ഇല്ലാതെ തനിയെ സ്കാൻ നടത്തുവാൻ അനുവദിക്കുന്നു.
3. ഏത് സമയത്തും ഏതൊരു ഫയലിനേയോ folder-നേയോ സ്കാൻ ചെചെയ്യാൻ അനുവദിക്കുന്നു.
4. കണ്ടെത്തിയ വൈറസുകളെ മാറ്റുക
5. കംമ്പ്യൂട്ടറിന്റെ ആരോഗ്യം (Health) കാണിക്കുക.

### പത്ത് സൗജന്യ അന്റി വൈറസ് സോഫറ്റ്വയറുകൾ

- Avast ! Free Antivirus
- Panda cloud Antivirus
- Microsoft security Essentials
- AviraAntivirus personal edition
- AVG Antivirus Free Edition
- Comodo Antividus
- Immunet Protect free
- PC tools Antivirus free
- Malware bytes
- Calm win free antivirus

### ആന്റി വൈറസിന്റെ പരിമിതികൾ

1. വൈറസിനെ കണ്ടെത്താൻ ആന്റി വൈറസിന് ഒരു പാട് വഴികൾ ഉണ്ടെങ്കിലും ചില ആന്റി വൈറസുകൾ ഒരു നിശ്ചിത രീതിയിൽ മാത്രമേ കണ്ടെത്തൂ. ഇത് വലിയ പോരായ്മയാണ്.
2. പല രീതിയിൽ വൈറസിനെ കണ്ടെത്താനുള്ള മാർഗ്ഗങ്ങൾ ഉള്ള ആന്റി വൈറസ് ഉണ്ടെങ്കിലും അത് 100 ശതമാനം സുരക്ഷിതമല്ല. വൈറസുകളെ ഒഴിവാക്കാനായി സെക്യൂരിറ്റി ഇന്റർനെറ്റ് ഫയർവാൾ എന്ന ആശയം മുന്നോട്ട് വയ്ക്കുന്നുണ്ട്. ഹാക്കർമാരെയും വൈറസുകളെയും തടയുന്ന ഒരു പ്രോഗ്രാമാണ് ഫയർവാൾ. ഫയർവാൾ ശക്തിപ്പെടുത്താൻ വേണ്ടി റൗട്ടർ (Router) പോലുള്ള ഹാർഡ് വയറുകൾ ഉപയോഗിക്കുന്നതാണ്.
3. ആന്റി വൈറസുകൾ ഇൻസ്റ്റാൾ ചെയ്ത് ഉപയോഗിക്കുന്നത് ഒരുപാട് മെമ്മറി ഉപയോഗിക്കാൻ കാരണമാകുന്നു. ഇത് കംമ്പ്യൂട്ടർ പ്രവർത്തന വേഗത കുറയ്ക്കുന്നു.
4. ഒന്നിൽ കൂടുതൽ ആന്റി വൈറസുകൾ ഉപയോഗിക്കുമ്പോൾ അവ ഒരുമിച്ച് പ്രവ ർത്തിക്കുന്നത് ചിലപ്പോൾ നടക്കില്ല

## ***Slide - 25***

ഇന്റർനെറ്റിൽ എന്തൊക്കെ സുരക്ഷിതമായി ചെയ്യാം. എന്തൊക്കെ ചെയ്യാൻ പാടില്ല എന്നതിനെക്കുറിച്ച് നിങ്ങളെ ബോധവാന്മാരാക്കാൻ താഴെ കൊടുത്തിരിക്കുന്ന നിർദ്ദേശങ്ങൾ പാലിക്കുക

1. **വ്യക്തിപരമായ വിശദാംശങ്ങൾ വെളിപ്പെടുത്താതിരിക്കുക.**
   ഒരു പാട് ആളുകൾ മറ്റുള്ളവരെ പ്രത്യേകിച്ച് കുട്ടികളേയും കൗമാരക്കാരെയും ദുരുപയോഗം ചെയ്യുവാൻ പരതി നടക്കുകയാണ്. ഇന്റർനെറ്റ് അതിന് ഏറ്റവും യോജിച്ച ഇടമാണ് അതുകൊണ്ട് ഒരിക്കലും നിങ്ങളുടെ വ്യക്തിപരമായ വിശദാംശങ്ങൾ ഇന്റർനെറ്റി ൽ നൽകാതിരിക്കുക. പ്രത്യേകിച്ചും പ്രൊഫൈൽ പേജുകൾ,

ബ്ലോഗുകൾ, ചാറ്റ്, ഇ-മെയിൽ എന്നിവയിൽ എപ്പോഴും നിങ്ങളുടെ യഥാർത്ഥ പേരിനുപകരം അപരനാമം ഉപയോഗിക്കുക.

നിങ്ങളുടെ വിലാസം, ഫോൺ നമ്പർ, നിരന്തരം പോകുന്ന സ്ഥലങ്ങൾ തുടങ്ങിയ വിവരങ്ങൾ പൊതുവായ വെബ്സൈറ്റുകൾക്ക് നൽകാതിരിക്കുക.

- അജ്ഞാതർക്ക് നിങ്ങളുടെ ചിത്രങ്ങൾ നൽകാതിരിക്കുക.
- അജ്ഞാതർക്ക് നിങ്ങളുടെ സുഹൃത്തുക്കളുടേയും, വീട്ടുകാരുടേയും വിരരം നൽകാതിരിക്കുക.
- നിങ്ങൾ പൂർണ്ണമായും അജ്ഞാതനാമാവ് ആണെന്നു കരുതരുത്. കാരണം നിങ്ങളുടെ വ്യരക്തിപരമായ കാര്യങ്ങൾ പൊതുവായി നൽകിയിട്ടില്ലെങ്കിലും മറ്റു പല വിധേയനയും ആ വിവരങ്ങൾ ചോർത്താൻ മറ്റുള്ളവർക്കാകും.

2. **നിങ്ങളുടെ പാസ്വേഡ് മറ്റാർക്കും (മാതാപിതാക്കൾക്കൊഴികെ) നൽകരുത്.**
നിങ്ങളുടെ ഇ-മെയിൽ ചാറ്റ് വെബ്സൈറ്റ്, പാസ്വേഡ്, എന്നിവ നിങ്ങളുടെ സുഹൃത്തുക്കളുമായോ, അപ രിചിതരുമായോ, പങ്കിടരുത്. കാരണം സുഹൃത്തുക്കൾ നിങ്ങളുടെ പാസ്വേഡ് അശ്രദ്ധമായി ഉപയോഗികാ കൻ സാദ്ധ്യതയാകുന്നു. എന്നാൽ നിങ്ങൾ പാസ്വേഡ് മാതാപിതാക്കളുമായി പങ്കിടുമ്പോൾ നിങ്ങൾ സുര ക്ഷിതമായാണ് ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്നത് എന്ന് ഉറപ്പിയ്ക്കാം.

3. **അപരിചിതരുമായി കണ്ടു മുട്ടലുകൾ ആസുത്രണം ചെയ്യരുത്.**
നിങ്ങൾ ഒരു വ്യക്തിയുടെ ചിത്രം കണ്ടെന്നോ, അവരെക്കുറിച്ച് വായിച്ചെന്നോ കരുതി അവരുടെ വ്യക്തിത്വം മനസ്സിലാക്കാൻ സാധിക്കണമെന്നില്ല. പല വ്യക്തികളും ഓൺലൈനിൽ അവരെക്കുറിച്ച് തെറ്റായ വിവരങ്ങൾ നൽകുകയും അവരുടെ യഥാർത്ഥ ഉദ്ദേശം നമ്മൾ അിറയാതെയിരിക്കുകയും ചെയ്യും. ഓൺലൈനിൽ നല്ലവ നായി ചിത്രീകരിക്കപ്പെട്ട വ്യക്തി യഥാർത്ഥത്തിൽ നല്ലവനാകണമെന്നില്ല. അവർ നിങ്ങളെ ഉപദ്രവിക്കാൻ സാധ്യത ഏറെയുണ്ട്. അതിനാൽ അപരിചിതരുമായി ഒരുക്കലും കണ്ടുമുട്ടലുകൾ ആസൂത്രണം ചെയ്യരുത്. തിര ക്കേറിയ സ്ഥലത്തുവെച്ചാണ് അവർ നിങ്ങളെ കണ്ടുമുട്ടുന്നതെങ്കിലും അവർ നിങ്ങളെ പിൻതുടരാൻ സാധ്യത യുണ്ട്. നിങ്ങൾക്ക് ഓൺലൈൻ വഴി പരിചയപ്പെട്ട ഒരു വ്യക്തിയെ കാണണമെന്നുണ്ടെങ്കിൽ നിങ്ങളുടെ മാതാ പിതാക്കളോടൊപ്പം കണ്ടുമുട്ടുന്ന രീതിയിൽ കാര്യങ്ങൾ ക്രമീകരിക്കുക. നിങ്ങളുടെ മാതാപിതാക്കൾ നിങ്ങ ളുടെ ഓൺലൈൻ സുഹൃത്തിനെ കാണുന്നത് നിങ്ങൾക്ക് വിഷമഹേതു ആകുമെങ്കിൽ ആ സുഹൃത്ബന്ധം ഒഴിവാക്കുന്നതാണ് ഉചിതം.

4. നിങ്ങൾ ഓൺലൈനിൽ കാണുന്നതും വായിക്കുന്നതുമായ വിവരങ്ങളുടെ ഉറവിടം വിശ്വാസ യോഗ്യമാണോ എന്നു പരിശോധിക്കുക. ചില വ്യക്തികൾ അവരുടെ പ്രായം, നാമം, കാണാൻ എങ്ങനെ, അവർക്ക് നിങ്ങളെ എങ്ങനെ അറിയാം എന്നിവയെ തെറ്റിദ്ധരിപ്പിക്കുന്നതും അസത്യങ്ങളുമായ വിവരങ്ങൾ നൽകാം. പല വെബ് സൈറ്റുകളിലും സത്യവും മിഥ്യയും തിരിച്ചറിയാൻ മാതാപിതാക്കളുടെ സഹായം തേടാവുന്നതാണ്.

5. **നിങ്ങളുടെ മാതാപിതാക്കളുടെ അനുവാദം കൂടാതെ സോഫ്റ്റ് വയറുകൾ ഫയലുകൾ എന്നിവ ഡൗൺ ലോഡ് ചെയ്യാതിരിക്കുക.** ഇന്റർനെറ്റിൽ ഉള്ള അനേകം ഫയലുകൾ അപകടകാരികളായിരിക്കും. ചിലത് നിരന്തരം പോപ്പ് അപ്പ് നൽകി നിങ്ങലെ ബുദ്ധിമുട്ടിയ്ക്കാം. മറ്റ് ചില ഫയലുകൾ നിങ്ങളുടേയോ മാതാപിതാക്കളുടേയോ ബാങ്ക് വിവരങ്ങൾ പാസ്സ് വേഡ് ലോഗിൻ വിവരങ്ങൾ ക്രെഡിറ്റ് കാർഡ് വിവരങ്ങൾ എന്നിവ ചോർക്കുകയും കുറ്റവാളികൾ ഈ വിവരങ്ങൾ ഉപയോഗിച്ച് നിങ്ങളെ കവർച്ച ചെയ്യാനും സാധ്യത യേറെയുണ്ട്. നല്ല ഫയൽ ഏത്, ചീത്ത ഫയൽ ഏത്, എന്ന് തിരിച്ചറിയാൻ വളരെയധികം ബുദ്ധിമുട്ടാണ്. നിങ്ങളുടെ മാതാപിതാക്കളുടെ അനുവാദത്തോടുകൂടി മാത്രം ഫയൽ സോഫ്റ്റ് വെയർ എന്നിവ ഡൗൺലോഡ് ചെയ്യുക.

6. **അപരിചിതമായ സന്ദേശങ്ങൾ, ഇ-മോയിലുകൾ എന്നിവയോട് പ്രതികരിക്കരുത്.**
ചിലർ അനുചിതമായ സന്ദേശങ്ങൾ നിങ്ങൾക്കയക്കാം. നിങ്ങൾ അതിനോട് പ്രതികരിക്കുന്നു ാ എന്നറി യാൻ വേണ്ടിയാണത്. നിങ്ങൾ പ്രതികരിച്ചാൽ കൂടുതൽ മോശമായ സന്ദേശങ്ങൾ വരും. അതുകൊണ്ട് അപ രിചിത സന്ദേശങ്ങളോടു പ്രതികരിക്കാതിരിക്കുക. പകരം നിങ്ങളുടെ മാതാപിതാക്കളുമായി ചർച്ച ചെയ്ത് അത് ബന്ധപ്പെട്ടവരെ അറിയിക്കുക.
നമുക്കേവർക്കും അറിയാവുന്നതുപോലെ ഇന്റർനെറ്റ് എന്നത് പുതിയ കാര്യങ്ങൾ പഠിക്കുവാനും സുഹൃത്തു ക്കളുമായി സല്ലപിക്കാനുമുള്ള ഒരു മേഖലയാണ്. അതേ സമയം അതിന് ഏറെ ദോഷ ഫലങ്ങളും ഉണ്ട് എന്ന വസ്തുത നിങ്ങൾ ഒരു ഇന്റർനെറ്റ് ഉപഭോക്താവാണെങ്കിൽ മറക്കരുത് . ജാഗ്രത പാലിക്കുക.

7. **പ്രായത്തിനു യോജിച്ച വേബ് സൈറ്റുകൾ മാത്രം കാണുക**
കുട്ടികൾ കാണാനും ഉപയോഗിക്കാനും പാടില്ലാത്ത പല തരം വെബ്സൈറ്റുകൾ ഉണ്ട്. നിങ്ങൾ ഇന്റർനെറ്റിൽ ഒരുപാട് ജ്ഞാനം ഉള്ളവരാണ്. എങ്കിലും, മുതിർന്നവർക്കായി ഉള്ള വെബ്സൈറ്റ് ഒരിക്കലും ഉപയോഗിക്കാൻ

പാടില്ല. കുട്ടികൾക്കായുള്ള ഒരു പാട് നല്ല വെബ് സൈറ്റുകൾ ഇന്റർനെറ്റിൽ ലഭ്യമാണ്. ആ വെബ്സൈറ്റു-കൾ നോക്കി അറിവുനേടി ആസ്വദിക്കുക.

8. **എന്തെങ്കിലും ഇന്റർനെറ്റിൽ ഇടുന്നതിനുമുമ്പ് ആലോചിച്ച് മനസ്സിലാക്കി ഇടുക**

നിങ്ങൾ ഇന്റർനെറ്റിൽ ഇടുന്ന പടങ്ങൾ എഴുതുന്ന മെയിൽ, ബ്ലോഗ്, വാർത്താ പത്രിക (Journal) എല്ലാം എല്ലാകാലത്തും ഇന്റർനെറ്റിൽ തന്നെ ഉണ്ടാവും. ഒരു പാട് സേർച്ച് ഏജൻസീസ് (goggle, yahoo, etc) ഇന്റർനെറ്റ്-ലെ പേജുകൾ സൂക്ഷിക്കും. അതിനാൽ നമ്മൾ ഇന്റർനെറ്റിൽ ഇട്ട കാര്യങ്ങൾ നമ്മൾ കളഞ്ഞാലും, അത് ഇന്റർനെറ്റിൽ തന്നെ ഉണ്ടാവും. അതിനാൽ ഇന്റർനെറ്റിൽ എന്തെങ്കിലും പരസ്യമാക്കും മുമ്പ് ഒരുവട്ടം കൂടി ആലോചിക്കുക.

9. **നല്ല പാസ് വേഡുകൾ തിരഞ്ഞെടുക്കുക**

നിങ്ങൾ ഉപയോഗിക്കുന്ന കമ്പ്യൂട്ടറിനും ഇന്റർനെറ്റ് സേവനങ്ങൾക്കും (chatting, e-mail, online shoping) നിങ്ങൾക്ക് തീർച്ചയായും ഒരു പാസ്വേഡ് ഉണ്ടാവണം. ഒരിക്കലും നിങ്ങളുടെ പാസ്വേഡ് ഒരിടത്തും എഴുതിവെയ്ക്കുകയോ, വേറെ ഒരാളുമായി പങ്കുവെയ്ക്കുകയോ ചെയ്യരുത്. അത് നിങ്ങളുടെ ആത്മാർത്ഥ സുഹൃത്ത് ആണെങ്കിൽ പോലും.

പലതരം തന്ത്രങ്ങൾ ഉപയോഗിച്ച് ഇന്ന് പാസ് വേഡുകൾ കണ്ടുപിടിക്കാൻ കഴിയുന്നതിനാൽ വളരെ സൂക്ഷ്മതയോടുകൂടി വേണം പാസ്വേഡ് തിരഞ്ഞെടുക്കാൻ.

നിങ്ങളുടെ പാസ്വേഡിൽ അക്ഷരങ്ങളും, അക്കങ്ങളും, ചിഹ്നങ്ങളും ഉൾപ്പെടുത്താൻ ശ്രമിക്കുക. കൂടാതെ പാസ്വേഡിന്റെ നീളം കഴിയുന്നത്ര കൂട്ടുക.

10. **സൗജന്യ wi-fi ഉപയോഗിക്കരുത്**

സൗജന്യ wi-fi ഹാക്കർമാർക്ക് ഒരു സുവർണ്ണാവസരമാണ്. കാരണമെന്തെന്നാൽ ഒരേ സമയം പല ആളുകൾ ഈ സൗജന്യ wi-fi ഉപയോഗിക്കും. ഇതേസമയം ഹാക്കർമാരും, ഈ wi-fi ഉപയോഗിച്ച് ഇതെ wi-fi ഉപയോഗിക്കുന്ന ആളുകളുടെ ഫെയിസ് ബുക്കിലും വേറെ വെബ്സൈറ്റിലും എല്ലാം കയറാൻ സാധിക്കും. എന്നിരുന്നാലും ഇതെ കാര്യങ്ങൾ ഹാക്കർമാർക്ക് സൗജന്യമല്ലാത്ത നെറ്റ് വർക്കിലും ചെയ്യാൻ സാധിക്കും. പക്ഷെ കൂടുതൽ സാധ്യത സൗജന്യ wi-fi-ൽ തന്നെയാണ്. കാരണം ഇതിൽ ഹാക്കർമാർക്ക് ധനനഷ്ടം ഒന്നും ഉണ്ടാവുന്നില്ല. അതിനാൽ കഴിവതും സൗജന്യ wi-fi ഉപയോഗിക്കാതെ ഇരിക്കുക. മൊബൈൽ ഇന്റർനെറ്റ് ഉപയോഗിക്കാൻ ശ്രമിക്കുക.

11. **ഉപയോഗത്തിനുശേഷം** Bluetooth **മറക്കാതെ ഓഫ് ചെയ്യുക.**

Bluetooth നമ്മുടെ ഫോണിൽ ഓൺ ആയിരിക്കുമ്പോൾ ഹാക്കർമാർക്ക് ഇതുവഴി പലതരം ഡാറ്റകൾ നമ്മുടെ മൊബൈലിൽ ഇടാൻ സാധിക്കും. അതിനാൽ Bluetooth സൂക്ഷിച്ച് കൈകാര്യം ചെയ്യുക.

12. **അജ്ഞാത ലിങ്കുകൾ, സന്ദേശങ്ങൾ, തുടങ്ങിയവയിൽ ക്ലിക്ക് ചെയ്യരുത്.**

അപരിചിതമായ സന്ദേശങ്ങൾ ഇ-മെയിലുകൾ എന്നിവയിലുള്ള ലിങ്കുകൾ ഒഴിവാക്കുക. സന്ദേശത്തിന്റെ ഉറവിടം തിരിച്ചറിയാൻ സാധിക്കാത്തതാണെങ്കിൽ അത് ബോധപൂർവ്വം ഒഴിവാക്കുക. ഒരിക്കലും നിങ്ങളുടെ വിവരങ്ങൾ ഇത്തരം സന്ദേശങ്ങളിലൂടെ കൈമാറാതിരിക്കുക.

13. **ഔദ്യോഗികമായ ആപ്പ് സ്റ്റോറുകളിൽ നിന്നും ആപ്ലിക്കേഷനുകൾ ഡൗൺ ലോഡ് ചെയ്യുക.**

ഔദ്യോഗികമമായ ആപ്പ് സ്റ്റോറുകൾ (App store-കൾ (Apple-App Store or google play) എന്നിവയിൽ നിന്നു മാത്രം ആപ്ലിക്കേഷൻ ചെയ്യുക. നമ്മൾ കാണുന്ന പലവിധ തട്ടിപ്പ് ആപ്ലിക്കേഷനുകളും അനൗദ്യോഗികമായ വെബ്സൈറ്റുകൾ ആപ്ലിക്കേഷൻ സ്റ്റോറുകളിൽ നിന്നാണ് വിതരണം ചെയ്യുന്നത്. ഔദ്യോഗികമായ ആപ്പ് സ്റ്റോറുകളിൽ വിശ്വസ്ഥരായി ഇരിക്കുന്നതുമൂലം തട്ടിപ്പുകൾക്ക് ഇരയാവാൻ സാധ്യത കുറയുന്നു.

## Cyber Laws

Slide 26

ഇന്ത്യയിൽ 2000 ത്തിൽ ആണ് ആദ്യമായി ഇൻഫർമേഷൻ ടെക്നോളജി ആക്ട് പ്രാബല്യത്തിൽ വരുന്നത്. Parliament ഈ ആക്ട് 2000 മെയ്-ൽ പാസ് ആക്കുകയും October -ൽ നിലവിൽ

വരികയും ചെയ്തു. IT ആക്ട് 2000 -ൽ 13 chapters ആണ് ഉള്ളത്. ഇതിൽ 4 schedule -കളും 94 sections ആണുള്ളത്.

കമ്പ്യൂട്ടർ ഉപയോഗിച്ച് തയ്യാറാക്കുന്ന വ്യാജരേഖകൾ, ഇന്റർനെറ്റ്, മൊബൈൽ ഫോൺ എന്നിവവഴി പ്രചരിക്കുന്ന ദേശവിരുദ്ധസന്ദേശങ്ങൾ എന്നിവ നിയന്ത്രിക്കുന്നതിനാണ് 2000 ൽ ആണ് ഇന്ത്യയിൽ ഒരു സമഗ്ര ഐടി നിയമം നിലവിൽ ന്നത്. സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിന് ഇത് ഒരു പരിധിവരെ സഹായകമായിരുന്നു.

എന്നാൽ ടെക്നോളജിയുടെ ദ്രുതഗതിയിലുള്ള വളർച്ച നമ്മുടെ നിയമത്തിനുപരിയായിരുന്നു (മുംബൈ ഭീകരാക്രമണത്തിൽ, കമ്പ്യൂട്ടർ നെറ്റ് വർക്ക് ഉപയോഗിച്ചുള്ള ഫോൺ സംഭാഷണങ്ങൾ ആക്രമണത്തിന്റെ ആസൂത്രണത്തിൽ ഉപയോഗിച്ചിരുന്നു എന്ന കണ്ടെത്തലായിരുന്നു നിയമം ഭേദഗതി ചെയ്യാനുണ്ടായ പ്രധാന കാരണം). തുടർന്ന് 2008 ൽ ഐ ടി ആക്ട് ഭേദഗതി ചെയ്യുകയും 2009 ഒക്ടോബർ 27 നു നിലവിൽ വരികയും ചെയ്തു. വിവര സാങ്കേതിക വിദ്യ (ഭേദഗതി) നിയമം ഇന്റർനെറ്റ്, മൊബൈൽ ഫോൺ, ഇന്റർനെറ്റ് ഫോൺ (VoIP) എന്നിവയുടെ ഉപയോക്താക്കൾക്കു കടുത്ത മുന്നറിയിപ്പാണു നൽകുന്നത്.

## ഐ ടി നിയമത്തിലെ സുപ്രധാന വകുപ്പുകൾ

***slide - 27***

**വകുപ്പ് 65**

കമ്പ്യൂട്ടറോ കമ്പ്യൂട്ടർ ശൃഖലയെയോ കംപ്യൂട്ടറിലെ സോഴ്സ് കോഡോ കമ്പ്യൂട്ടർ പ്രോഗ്രാമോ മനഃപൂർവം നശിപ്പിക്കുകയോ മാറ്റം വരുത്തുകയോ ഒളിപ്പിക്കുകയോ ചെയ്താൽ അതിനു 3 വർഷം വരെ തടവോ 2 ലക്ഷം രൂപ പിഴയോ അല്ലെങ്കിൽ രണ്ടും ലഭിക്കാവുന്ന കുറ്റമാണ്.

**വകുപ്പ് 66**

66-ആം വകുപ്പിൽ ഒരാളുടെ അനുവാദം കൂടാതെ അയാളുടെ കമ്പ്യൂട്ടറിൽ ഉള്ള വിവരങ്ങൾ നശിപ്പിക്കുകയോ ദുരുപയോഗം ചെയ്യുകയോ ചെയ്യുന്നതിനെ പറ്റി(ഹാക്കിങ്) പരാമർശിക്കുന്നു .കൂടുതൽ സൈബർ കുറ്റങ്ങളെപ്പറ്റിയും അവക്കുള്ള ശിക്ഷാ വിധികളെയും വിശദീകരിക്കുന്നത് 66 ആം വകുപ്പിലെ ഉപ വകുപ്പുകളിൽ ആണ്

ഐടി നിയമത്തിലെ 66 (എ) വകുപ്പനുസരിച്ച് മൊബൈൽ ഫോൺ, കമ്പ്യൂട്ടർ തുടങ്ങിയ ഇലക്ട്രോണിക് മാധ്യമങ്ങൾവഴി, കുറ്റകരമായതോ സ്പർദ്ധ ഉളവാക്കുന്നതോ ആയ വിവരങ്ങൾ, തെറ്റാണെന്നറിഞ്ഞിട്ടും ശത്രുതയോ, പരിക്കോ, വിദ്വേഷമോ, അനിഷ്ടമോ, അപകടമോ, മോശക്കാരനാക്കലോ, അസൗകര്യം ഉണ്ടാക്കലോ, ചെയ്യാൻ ഉദ്ദേശിച്ചുള്ള വിവരങ്ങൾ, തെറ്റിദ്ധാരണാജനകമായ ഇലക്ട്രോണിക് സന്ദേശങ്ങൾ എന്നിവയുടെ സൃഷ്ടി, കൈമാറ്റം, സ്വീകരിക്കൽ എന്നിവയെല്ലാം മൂന്നു വർഷം വരെ തടവും പിഴയും ലഭിക്കാവുന്ന കുറ്റമായി കണക്കാക്കുന്നു (എന്നാൽ ഐ ടി നിയമത്തിലെ ഈ വകുപ്പ് സോഷ്യൽ മീഡിയകളിൽ ഉപയോക്താക്കളുടെ അഭിപ്രായ സ്വാതന്ത്രത്തിനു കൂച്ചുവിലങ്ങിടുമെന്ന കണ്ടെത്തലിനെ തുടർന്നു സുപ്രീംകോടതി റദ്ദാക്കി).

**വകുപ്പ് 66B**

മോഷ്ടിക്കപ്പെട്ട കമ്പ്യൂട്ടർ, മൊബൈൽ ഫോൺ, സിഡിറോം, പെൻഡ്രൈവ് ഉൾപ്പെടെയുള്ള കമ്മ്യൂണിക്കേഷൻ ഉപകരണങ്ങൾ അതു മോഷ്ടിക്കപ്പെട്ടതാണെന്നറിഞ്ഞുകൊണ്ട് ഉപയോഗിച്ചാൽ മൂന്നു വർഷം വരെ തടവോ ഒരുലക്ഷം വരെ പിഴയോ ലഭിക്കാവുന്നതാണ്. കംപ്യൂട്ടർ

വഴിയുള്ള തട്ടിപ്പ്, വഞ്ചന, ഡിജിറ്റൽ ഒപ്പ് മോഷ്ടിക്കൽ, പാസ്സ്വേർഡ് ദുരുപയോഗം എന്നിവയ്ക്കും സമാനശിക്ഷയാണുള്ളത് [വകുപ്പ് 66C].

**വകുപ്പ് 66 D**

ഫേസ്ബുക്, Twitter പോലുള്ള സോഷ്യൽ നെറ്റ്വർക്ക് സൈറ്റുകളിൽ വ്യാജപ്രൊഫൈലുകളുണ്ടാക്കി അപകീർത്തികരമായ പ്രവർത്തനം നടത്തുന്നവരും കേസിലാകും. സിനിമ താരങ്ങളുടെയോ മറ്റു പ്രശസ്ത വ്യക്തികളുടേതോ ഫോട്ടോ പ്രൊഫൈലിൽ വച്ചു മനപ്പൂർവം കബളിപ്പിക്കുന്നവരും പരാതിയുടെ അടിസ്ഥാനത്തിൽ പിടിയിലാകും.

**വകുപ്പ് 66E**

ഒരു വ്യക്തിയുടെ അനുവാദമില്ലാതെ അവരുടെ സ്വകാര്യഭാഗങ്ങളുടെ ചിത്രങ്ങൾ എടുക്കുന്നതും അയയ്ക്കുന്നതും അവരുടെ സ്വകാര്യതയിലോട്ടുള്ള കടന്നുകയറ്റമായി കരുതും. മൂന്നു വർഷം വരെ തടവോ രണ്ടുലക്ഷത്തിലധികം പിഴയോ ലഭിക്കാവുന്ന കുറ്റമാണ്

**വകുപ്പ് 66F (സൈബർ തീവ്രവാദം)**

രാജ്യത്തിന്റെ അഖണ്ഡത, സുരക്ഷ, വിദേശ രാജ്യങ്ങളുമായുള്ള സൌഹൃദം എന്നിവയ്ക്കു ഭീഷണിയുണ്ടാക്കുന്നതോ, വ്യക്തികൾക്ക് അപകടം സംഭവിക്കാൻ കാരണമാക്കുന്നതോ, സമൂഹത്തെ പൊതുവായി ബാധിക്കുകയോ ചെയ്യുന്ന പ്രവൃത്തികളാണു സൈബർ തീവ്രവാദത്തിൽ ഉൾപ്പെടുന്നത്. ജീവപര്യന്തം വരെ ശിക്ഷ ലഭിക്കാവുന്നതാണ് ഈ കുറ്റകൃത്യങ്ങൾ.

വകുപ്പ് **67**

ഇലക്ട്രോണിക് മാധ്യമത്തിൽ കൂടി പ്രസിദ്ധീകരിക്കുന്ന / പ്രസരിപ്പിക്കുന്ന ഏതുതരം അശ്ലീലങ്ങളേയും ഈ വകുപ്പിൽ പെടുത്താം. ഇവിടെയാണു ബ്ലോഗുകൾ പ്രസക്തമാകുന്നത്. അതായത് അശ്ളീലചിത്രങ്ങൾ /ലേഖനങ്ങൾ എന്നിവ വെബ്സൈറ്റിൽ /ബ്ലോഗിൽ പ്രസിദ്ധീകരിക്കുക, പ്രസരണം നടത്തുക എന്നിവയ്ക്കു മൂന്നുവർഷം തടവും അഞ്ചുലക്ഷം രൂപ വരെ പിഴയുമാണുള്ളത്. കുറ്റം ആവർത്തിച്ചാൽ തടവിന്റെ കാലാവധി അഞ്ച് വർഷം പിഴയുടേതു 10 ലക്ഷവുമാകും. മറ്റു കുറ്റങ്ങളിൽ പിഴയോ തടവോ ഏതെങ്കിലുമൊന്ന് അനുഭവിച്ചാൽ മതിയെങ്കിൽ അശ്ളീലപ്രസാരണത്തിനു രണ്ടും ഒന്നിച്ചനുഭവിക്കണം.

ഇലക്ട്രോണിക് മാധ്യമത്തിലുടെ ലൈംഗിക പ്രവർത്തനം വ്യക്തമാകുന്ന ഏതുതരം കാര്യങ്ങളും ഇതു പോലെ പ്രസിദ്ധീകരിക്കുന്നതും പ്രസരണം നടത്തുന്നതും 67-ആം വകുപ്പ് പ്രകാരം കുറ്റകരമാണ്.

**വകുപ്പ് 67B**

Child Pornography യുടെ കാര്യത്തിൽ ഈ നിയമം വളരെ കർക്കശമാണു. 18 വയസ്സിനു താഴെയുള്ള കുട്ടികളുടെ നഗ്ന, ലൈംഗിക ചിത്രങ്ങൾ പ്രസാരണം നടത്തുകയോ പ്രസിദ്ധീകരിക്കുകയോ കൈമാറുകയോ ചെയ്യുന്നത് കുറ്റകരം. അതുകൊണ്ട് അപ്രകാരമുള്ള ചിത്രങ്ങൾ/ചിത്രീകരണങ്ങൾ ഇന്റർനെറ്റുഴി സ്വന്തം കമ്പ്യൂട്ടറിൽ ബ്രൌസ് ചെയ്യലും ഡൌൺലോഡ് ചെയ്യലും തെരച്ചിൽ നടത്തുന്നതും ശിക്ഷാർഹമാണ്. ലൈംഗികമായി പ്രലോഭിപ്പിക്കുന്ന ഇ-മെയിൽ, ചാറ്റിങ്, എസ്എംഎസ് എന്നിവയ്ക്കും സമാനശിക്ഷയാണുള്ളത്.

# കമ്പ്യൂട്ടർ മേഖലയിലെ ജോലി സാധ്യതകൾ

***Slide 1***

ഇന്ന് കമ്പ്യൂട്ടർ ഇല്ലാത്ത ഒരു ലോകത്തെ കുറിച്ച് ചിന്തിക്കാനേ സാധിക്കില്ല. ചെറിയ വ്യാപാര സ്ഥാപനങ്ങൾ മുതൽ ISRO, NASA തുടങ്ങിയ ബഹിരാകാശ ഗവേഷണ കേന്ദ്രങ്ങളിൽ വരെ കമ്പ്യൂട്ടർ ഒരു അവിഭാജ്യ ഘടകമാണ്. അത് കൊണ്ട് തന്നെ ഈ മേഖലയിൽ ജോലി സാധ്യതകളും ഒരു പാടുണ്ട്. ഇനി കമ്പ്യൂട്ടറിന്റെയും ഇന്റർനെറ്റിന്റെയും ജോലി സാധ്യതകളെ കുറിച്ച് നമുക്കൊന്ന് നോക്കാം.

***Slide 2***

ഇന്ന് ജീവിതത്തിന്റെ പല മേഖലകളിലും കമ്പ്യൂട്ടർ പരിജ്ഞാനം ഉള്ളവർക്ക് ജോലി സാധ്യത ഉണ്ട്. നമ്മുടെ ദൈനം ദിന ജീവിതത്തിൽ നിന്ന് തന്നെ നിരവധി ഉദാഹരണങ്ങൾ ലഭ്യമാണ്. താഴെ പറയുന്നവ അതിൽ ചിലതാണ്

- ആരോഗ്യ മേഖല
- പ്രതിരോധ മേഖല
- ടെലി കമ്മ്യൂണിക്കേഷൻ
- ബാങ്കിങ്
- വിദ്യഭ്യാസം
- ഗവേഷണം
- എത്തിക്കൽ ഹാക്കിങ്

ഉദാഹരണത്തിന് ആരോഗ്യ മേഖല ഇന്ന് ഒരു പാട് പുരോഗമിച്ചു കഴിഞ്ഞു. സ്കാനിംഗ്, ECG, ശസ്ത്രക്രിയകൾ എന്നിങ്ങനെ ഒരു ആശുപത്രിയുമായി ബന്ധപ്പെട്ട ഒരു വിധം ജോലികളെല്ലാം കമ്പ്യൂട്ടർ ഏറ്റെടുത്തു കഴിഞ്ഞു. ഡോക്ടർ'സ് കൺസൽറ്റേഷൻ വരെ ഇന്ന് ഓൺലൈൻ ആയി കഴിഞ്ഞു.

***Slide 3***

## അടിസ്ഥാന കമ്പ്യൂട്ടർ പരിജ്ഞാന ഉള്ളവർക്ക് നേടാവുന്ന തൊഴിലുകൾ

ഈ ജോലിക്കൾക്കെല്ലാം വേണ്ടത് അടിസ്ഥാന കമ്പ്യൂട്ടർ പരിജ്ഞാനം മാത്രമാണ്. ഇവയെല്ലാം നല്ല വരുമാന മാർഗം കൂടിയാണ്.

- ടാറ്റ എൻട്രി
- ഡി ടി .പി
- ഡിസൈനിങ്

## ഐ ടി യിലെ മറ്റു ജോലി സാദ്ധ്യതകൾ

- കമ്പ്യൂട്ടർ പ്രോഗ്രാമർ
- ക്വാളിറ്റി അഷുറൻസ്
- കമ്പ്യൂട്ടർ സിസ്റ്റം അനലിസ്റ്റ്
- ഇൻഫർമേഷൻ സെക്യൂരിറ്റി അനലിസ്റ്റ്
- റിസർച്ച് അനലിസ്റ്റ്

നാം ദിവസവും ഒരു പാട് computer programmes ഉപയോഗിക്കാറുണ്ട്. ഉദാഹരണത്തിന് മൊബൈൽ ഉപയോഗിച്ച് Call ചെയുന്നത്. അതിനു പുറകിലും ഒരു സോഫ്റ്റ്വെയർ ഉണ്ട്. അത് തയ്യാറാക്കുന്ന വ്യക്തി ആണ് കമ്പ്യൂട്ടർ പ്രോഗ്രാമർ. ആ പ്രോഗ്രാം കൃത്യമായി

പ്രവർത്തിക്കുന്നു എന്ന് ടെസ്റ്റർ ഉറപ്പു വരുത്തുന്നു. അനലിസ്റ്റ് ഈ ജോലികളെല്ലാം മേൽനോട്ടം വഹിക്കുന്നു. സെക്യൂരിറ്റി അനലിസ്റ്റ് ഈ പ്രവർത്തനങ്ങൾ കാര്യക്ഷമമാണെന്നു ഉറപ്പാക്കുന്നു. റിസർച്ച് സയന്റിസ്റ്റ് ഇത്തരം പ്രവർത്തനങ്ങളിൽ കൊണ്ട് വരാവുന്ന പുതിയ പ്രവർത്തനങ്ങളെ കുറിച്ച് ഗവേഷണം നടത്തുന്നു. ഈ പറഞ്ഞ ജോലികൾക്കു മിനിമം യോഗ്യത അത്യാവശ്യമാണ്. അതായതു MCA, MSc, B.Tech എന്നിങ്ങനെ ഏതെങ്കിലും വിദ്യാഭ്യാസ പശ്ചാത്തലത്തിൽ നിന്നുള്ളവരാകണം.

## ***Slide 4***

### ഫ്രീലാൻസെർ

അടുത്ത കാലങ്ങളിലായി വളരെ ഏറെ പ്രചാരം നേടിയ മറ്റൊരു തൊഴിൽ മേഖല ആണ് ഫ്രീലാൻസിങ്. കൃത്യമായ മാസ ശമ്പളത്തിന് ഒരു സ്ഥാപനത്തിന്റെയോ വ്യക്തിയുടെയോ കീഴിൽ ജോലി ചെയ്യുന്നതിന് പകരം സ്വന്തം കഴിവുകൾക്കും ഭാവനയ്ക്കും അനുസൃതമായി ഇഷ്ടമുള്ള മേഖലയിൽ ഇന്റർനെറ്റിന്റെയും കമ്പ്യൂട്ടറിന്റെയും സഹായത്തോടെ ജോലി ചെയ്യുന്നതിനെയാണ് ഫ്രീലാൻസിങ് എന്ന് പറയുന്നത്.

### യാത്ര വിവരണങ്ങൾ

യാത്രകളോടും എഴുത്തിനോടും താല്പര്യവും അഭിരുചിയും ഉള്ള ആർക്കും ഈ ജോലി തിരഞ്ഞെടുക്കാവുന്നതാണ്.

### അദ്ധ്യാപനം

ലോകമെമ്പാടുമുള്ള ആളുകൾക്ക് വേണ്ടി ട്യൂട്ടോറിയൽ വിഡിയോകൾ, ലേഖനങ്ങൾ മുതലായവ ഉണ്ടാക്കുകയും ഇന്റർനെറ്റിന്റെ സഹായത്തോടെ ആളുകളിലേക്ക് എത്തിക്കുകയും ചെയ്യാം.

### ഫോട്ടോഗ്രാഫി

അഭിരുചിയും നല്ലൊരു ക്യാമറയും ഉണ്ടെങ്കിൽ ഫോട്ടോഗ്രാഫി എന്നത് രസകരമായ ഒരു തൊഴിൽ മേഖല ആണ്.

### ഓൺലൈൻ വ്യാപാരം

സ്വന്തമായി ഉത്പന്നങ്ങൾ ഉണ്ടാക്കുകയും ഭക്ഷണ സാധനങ്ങൾ, പെയിന്റിംഗ് എന്നിവ സ്വയം വെബ്സൈറ്റ് വഴി വിൽക്കുകയും ചെയ്യാം.

## ***Slide 5***

### തൊഴിൽ വാഗ്ദാനങ്ങൾ നൽകുന്ന വ്യാജ മെയിൽ

വ്യാജ തൊഴിൽ വാഗ്ദാനങ്ങൾ നൽകി, ജോലി തേടുന്ന യുവ തലമുറയെ കബളിപ്പിക്കുന്ന ഒരു പാട് വെബ്സൈറ്റുകൾ ഇപ്പോൾ നിലവിലുണ്ട്. വലിയ സ്ഥാപനങ്ങളുടെ, എന്ന് തോന്നിപ്പിക്കുന്ന മെയിൽ ഐ ഡി കളിൽ നിന്ന് അപ്പോയ്ന്റ്മെന്റ് ലെറ്ററുകൾ അയച്ചാണ് ഇവർ ആളുകളെ പറ്റിക്കുന്നത്. അതിനാൽ വിശ്വസിക്കാം എന്ന് ഉറപ്പുള്ള മെയിലുകൾ മാത്രം തുറക്കുകയും മറുപടി അയക്കുകയും ചെയ്യുക.

ഇങ്ങനെയുള്ള മെയിൽ കിട്ടിയാൽ അതാത് കമ്പനിയുമായി ബന്ധപ്പെട്ടു അതിന്റെ വിശ്വാസ്യത ഉറപ്പു വരുത്തുക. അതിനായി പക്ഷെ നിങ്ങൾക്കു കിട്ടിയ മെയിൽ-ൽ തന്നിരിക്കുന്ന ഫോൺ

നമ്പറോ ഇമെയിൽ ഐഡിയോ ഉപയോഗിക്കരുത്. കമ്പനിയുടെ യഥാർത്ഥ വെബ് സൈറ്റിൽ നിന്നും കിട്ടുന്ന നമ്പറിലോ ID-യിലോ മാത്രം ബന്ധപ്പെടുക. ഇതിനു മുൻപായി അവർ ചോദിക്കുന്ന രേഖകളോ പണമോ അവർക്കു നൽകരുത്.

***Slide 6***

നിങ്ങളുടെ അറിവിലേക്കായി ചില ഓൺലൈൻ ജോബ് സൈറ്റുകൾ.

- Www.naukri.com
- www.timesjob.com
- www.mosterindia.com

## Curriculum Vitae

***Slide 7, 8***

എന്താണ് CV അഥവാ Curriculum Vitae യുടെ ആവശ്യകത. പഠനശേഷം നിങ്ങൾ തൊഴിൽ തേടുമ്പോൾ നിങ്ങളുടെ കഴിവുകളും പ്രായോഗിക അറിവുകളും അക്കാദമിക് വിവരങ്ങളും തൊഴിൽ ദാതാവിനു എഴുതി തയ്യാറാക്കി നൽകേണ്ടതാണ്. വിവിധ CV കളിൽ നിന്ന് ജോലിക്കു അനുയോജ്യമായവരെ തിരഞ്ഞെടുക്കുന്നു. CV തയ്യാറാക്കുമ്പോൾ താഴെ പറയുന്ന കാര്യങ്ങൾ ഉൾപ്പെടുത്താം.

- നിങ്ങളുടെ സവിശേഷതകളും ഈ ജോലിക്കു നിങ്ങൾ എന്തുകൊണ്ട് അനുയോജ്യരാകുന്നു എന്നുമുള്ള ഒരു ചെറു വിവരണം. (Self-Introduction)
- ഹൈസ്കൂൾ തലത്തിൽ നേടിയിട്ടുള്ള പുരസ്കാരങ്ങൾ, നേട്ടങ്ങൾ (Achievements/Awards/appreciations)
- സാമൂഹ്യ സേവനങ്ങൾ, നേതൃത പാടവം , ഏതു ചുറ്റുപാടുമായും ഇഴുകിച്ചേരാനുള്ള നിങ്ങളുടെ കഴിവുകൾ എന്നിവയുടെ വിശദീകരണം (Demonstrate personal attitude)

അതൊക്കെ കൂടാതെ :

- ഏതങ്കിലും കായിക/സാമൂഹ്യ ക്ലബ്ബിൽ അംഗത്വം
- ജോലിക്കു അനുയോജ്യമായ മറ്റു താല്പര്യങ്ങൾ
- തൊഴിൽപരമായ പരിസ്ഥിതിയിൽ പ്രവർത്തി പരിചയം
- സൂപ്പർവൈസർ, കായിക അധ്യാപകൻ, പ്രധാന അദ്ധ്യാപകൻ നിന്നുമുള്ള യോഗ്യതാപത്രം

നേരത്തെ പറഞ്ഞ ജോബ് സൈറ്റുകളിൽ നിങ്ങൾക്കു CV ഉണ്ടാക്കി അപ്ലോഡ് ചെയാൻ സാധിക്കും. ഇതിനായി site -ൽ രജിസ്റ്റർ ചെയേണ്ടതായിട്ടുണ്ട്