STATE POLICE MEDIA CENTRE
KERALA POLICE

Police Headquarters
Vazhuthacaud
Thiruvananthapuram - 695010
0471 2318188
info.pol@kerala.gov.in
statepolicemediacentre

No.483/PR/SPMC/PHQ/2026 Date:13.10.2026

പത്രക്കുറിപ്പ്

ഓൺലൈൻ ഷോപ്പിങ് സെയിലുകളുടെ പേരിൽ വ്യാജ ഓഫറുകൾ; ജാഗ്രത പാലിക്കുക

ഉത്സവകാല ഓൺലൈൻ ഷോപ്പിങ് സെയിലുകളുടെ ഭാഗമായി ആമസോൺ ഗ്രേറ്റ് ഇന്ത്യൻ ഫെസ്റ്റിവൽ, ഫ്ളിപ്കാർട്ട് ബിഗ് ബില്യൺ ഡേയ്സ് തുടങ്ങിയവയുടെ പേരിൽ വ്യാജ ഓഫറുകൾ പ്രചരിപ്പിച്ച് സൈബർ തട്ടിപ്പുകൾ നടത്താൻ സാധ്യതയുള്ളതിനാൽ പൊതുജനങ്ങൾ ജാഗ്രത പാലിക്കുക.

സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകൾ, വാട്സ്ആപ്പ് സന്ദേശങ്ങൾ, എസ്എംഎസ്, ഇമെയിലുകൾ എന്നിവയിലൂടെ ആകർഷകമായ വിലക്കുറവുകളും സമ്മാനങ്ങളും വാഗ്ദാനം ചെയ്താണ് തട്ടിപ്പുകാർ ഇരകളെ കണ്ടെത്തുന്നത്. പ്രമുഖ ഓൺലൈൻ ഷോപ്പിങ്

വെബ്സൈറ്റുകളുടെ പേരും ലോഗോയും ദുരുപയോഗം ചെയ്ത് വ്യാജ വെബ്സൈറ്റുകളും ലിങ്കുകളും പ്രചരിപ്പിക്കുന്നതും തട്ടിപ്പിന്റെ ഭാഗമാണ്.

തട്ടിപ്പുകൾ നടത്തുന്ന രീതി:

വിപണി വിലയേക്കാൾ വളരെ കുറഞ്ഞ വിലയ്ക്ക് ഉൽപ്പന്നങ്ങൾ വാഗ്ദാനം ചെയ്ത് ഉപഭോക്താക്കളെ വ്യാജ വെബ്സൈറ്റുകളിലേക്ക് എത്തിക്കുന്നു. ഓർഡർ നൽകുന്നതിനും പണമടയ്ക്കുന്നതിനുമായി ബാങ്ക് അക്കൗണ്ട് വിവരങ്ങൾ, കാർഡ് വിവരങ്ങൾ, ഒ.ടി.പി. തുടങ്ങിയവ കൈക്കലാക്കുന്നു. വ്യാജ കസ്റ്റമർ കെയർ നമ്പറുകൾ വഴിയും തട്ടിപ്പുകൾ നടക്കാം. പണം അടച്ചശേഷം ഉൽപ്പന്നം ലഭിക്കാതിരിക്കുകയോ നിലവാരമില്ലാത്ത ഉൽപ്പന്നങ്ങൾ ലഭിക്കുകയോ ചെയ്യുന്നതും തട്ടിപ്പുകളുടെ ഭാഗമാണ്. ചില സന്ദർഭങ്ങളിൽ റീഫണ്ട്, ജി.എസ്.ടി., പ്രോസസ്സിങ് ഫീസ് തുടങ്ങിയ പേരുകളിൽ വീണ്ടും പണം ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.

ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ:

1. സോഷ്യൽ മീഡിയയിലെ പരസ്യങ്ങളിലെ ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിനു മുമ്പ് അവയുടെ വിശ്വാസ്യത ഉറപ്പാക്കുക.

2. ആമസോൺ, ഫ്ളിപ്കാർട്ട് തുടങ്ങിയവയുടെ ഔദ്യോഗിക വെബ്സൈറ്റുകളിലൂടെയോ ആപ്പുകളിലൂടെയോ മാത്രം ഷോപ്പിംഗ് നടത്തുക.

3. വെബ്സൈറ്റ് വിലാസത്തിലെ അക്ഷരപ്പിശകുകളും വ്യാജ ഡൊമെയ്നുകളും പരിശോധിക്കുക.

4. വാട്സ്ആപ്പ് സന്ദേശങ്ങളിലൂടെയും അപരിചിത നമ്പറുകളിൽനിന്നും ലഭിക്കുന്ന ഓഫർ ലിങ്കുകൾ സൂക്ഷിച്ച് മാത്രം കൈകാര്യം ചെയ്യുക.

5. യു.പി.ഐ. പിൻ, ഒ.ടി.പി., എ.ടി.എം. പിൻ, കാർഡ് സി.വി.വി., ബാങ്കിങ് പാസ്‌വേഡ് തുടങ്ങിയ രഹസ്യവിവരങ്ങൾ ആരുമായും പങ്കുവയ്ക്കരുത്.

6. പണം ലഭിക്കാനായി യു.പി.ഐ. പിൻ നൽകേണ്ടതില്ലെന്ന് ഓർക്കുക.

7. സമ്മാനമോ ഓഫറോ ലഭിക്കുന്നതിനായി മുൻകൂർ പണം ആവശ്യപ്പെടുന്നവരെ വിശ്വസിക്കരുത്.

8. പണം നൽകിയശേഷം റീഫണ്ട് ലഭിക്കുന്നതിനായി അപരിചിതരുടെ നിർദേശപ്രകാരം ആപ്പുകൾ ഇൻസ്റ്റാൾ ചെയ്യുകയോ ബാങ്ക് വിവരങ്ങൾ കൈമാറുകയോ ചെയ്യരുത്.

സൈബർ സാമ്പത്തിക തട്ടിപ്പിനിരയായാൽ 1930 എന്ന ദേശീയ സൈബർ ക്രൈം ഹെൽപ്പ്‌ലൈൻ നമ്പറിൽ ബന്ധപ്പെടുക. കൂടാതെ https://cybercrime.gov.in എന്ന വെബ്സൈറ്റ് വഴിയും പരാതി നൽകാം.

തട്ടിപ്പുമായി ബന്ധപ്പെട്ട സന്ദേശങ്ങൾ, ഫോൺ നമ്പറുകൾ, വെബ്സൈറ്റ് ലിങ്കുകൾ, പണമിടപാട് വിവരങ്ങൾ എന്നിവ തെളിവായി സൂക്ഷിക്കുക.

ഓൺലൈൻ ഷോപ്പിങ് നടത്തുമ്പോൾ അമിതമായ വിലക്കുറവിന്റെ വാഗ്ദാനങ്ങളിൽ വീഴരുത്. ജാഗ്രതയോടെയും ഉത്തരവാദിത്വത്തോടെയും ഇടപാടുകൾ നടത്തുക.

ഡോ. അഞ്ചൽ കൃഷ്ണകുമാർ,
ഡെപ്യൂട്ടി ഡയറക്ടർ,
സ്റ്റേറ്റ് പോലീസ് മീഡിയ സെന്റർ

****