ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍

លេខ : ២៧៨.ប.ទ. ថ្ងៃអង្គារ ៧កើត ខែមាឃ ឆ្នាំរោង ឆស័ក ព.ស.២៥៦៨
រាជធានីភ្នំពេញ ថ្ងៃទី ៤ ខែកុម្ភៈ ឆ្នាំ២០២៥

សេចក្តីជូនដំណឹង
ស្តីពី
វិធីសាស្ត្រការពារខ្លួនពីឧបាយកលឆបោកដោយការប្រើប្រាស់បច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត

ក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ (**ក.ប.ទ.**) សូមជម្រាបជូនសាធារណជនទាំងអស់មេត្តាជ្រាបថា ស្របពេលដែលបច្ចេកវិទ្យាកំពុងអភិវឌ្ឍឥតឈប់ឈរ ការឆបោកកាន់តែមានច្រើនដែលជាបញ្ហាសកលកំពុងកើនឡើង គួរឱ្យកត់សម្គាល់។ ថ្មីៗនេះ ក្រុមឆបោកបានប្រើប្រាស់បច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត (AI) ក្នុងការបោកប្រាស់តាមប្រព័ន្ធទូរសព្ទ ក៏ដូចជាប្រព័ន្ធទូរគមនាគមន៍ផ្សេងៗ ដើម្បីឱ្យអ្នកផ្ញើរប្រាក់ឬចែករំលែកទិន្នន័យសំខាន់ៗមួយចំនួន ដោយក្លែងបន្លំជាការសន្ទនាសំឡេង រូបភាព ឬវីដេអូដែលមានមុខមាត់ពិតរបស់សមាជិកគ្រួសារ មិត្តភក្តិ ឬអ្នកស្គាល់គ្នា ដែលធ្វើឱ្យមានការពិបាកក្នុងការកំណត់អត្តសញ្ញាណថាពិត ឬក្លែងក្លាយ។

ក. ឧបាយកលឆបោក

ឧបាយកលឆបោកតាមរយៈការក្លែងបន្លំជាសំឡេង រូបភាព ឬវីដេអូរបស់សមាជិកគ្រួសារ មិត្តភក្តិ ឬអ្នកស្គាល់គ្នា មានទម្រង់ ដូចខាងក្រោម៖

- ការប្រើប្រាស់បច្ចេកវិទ្យាបញ្ញាសិប្បនិម្មិត (AI) ដើម្បីបង្កើតជាការសន្ទនាសំឡេង រូបភាព ឬវីដេអូ ដែលសឹងតែដូចទាំងស្រុងនឹងម្ចាស់ដើម មានលក្ខណៈស្ទាប់ប្រវត្តិ និងពិបាកសម្គាល់ថាពិតឬក្លែងក្លាយ ដែលធ្វើឱ្យអ្នកងាយនឹងចាញ់បោក និងធ្លាក់ចូលក្នុងឧបាយកលរបស់ជនទុច្ចរិត បើសិនមិនបានពិនិត្យ និងផ្ទៀងផ្ទាត់ច្បាស់លាស់
- ការទាមទារ ស្នើសុំ ឬខ្ចីប្រាក់ ដែលតម្រូវឱ្យអ្នកផ្ញើរប្រាក់តាមប្រព័ន្ធអនឡាញតែម្តង
- ការស្នើសុំឱ្យចែករំលែកទិន្នន័យផ្ទាល់ខ្លួន ជាអាទិ៍ លេខកូដសម្ងាត់គណនីធនាគារ លេខកូដបណ្តាញទំនាក់ទំនងសង្គម លេខកូដផ្ទៀងផ្ទាត់ ឬព័ត៌មានសំខាន់ផ្សេងៗ។

ខ. វិធីសាស្ត្រការពារខ្លួនពីការឆបោក

ដើម្បីការពារខ្លួនពីការឆបោកខាងលើ រាល់ពេលទទួលបានការហៅទូរសព្ទ សារ សំឡេង រូបភាព ឬវីដេអូ ដែលមានលក្ខណៈគួរឱ្យសង្ស័យ សូមអនុវត្តវិធីសាស្ត្រ ដូចខាងក្រោម៖

- ផ្ទៀងផ្ទាត់អត្តសញ្ញាណរបស់បុគ្គលនោះឱ្យបានច្បាស់លាស់ ដោយពិនិត្យលេខទូរសព្ទ ឬរូបភាពគណនី និងតម្រូវឱ្យបុគ្គលនោះបើកកាមេរ៉ាវីដេអូបង្ហាញមុខភ្លាមៗ
- ពិនិត្យផ្ទៀងផ្ទាត់អាកប្បកិរិយារបស់បុគ្គលនោះថា ដូចប្រក្រតី ឬប្លែកពីអ្នកដែលយើងស្គាល់

- សូរសំណួរផ្ទាល់ខ្លួន ឬសកម្មភាពដែលបានទាក់ទងគ្នាចុងក្រោយដែលគិតថាត្រូវតែដឹង
- បង្កើនការប្រុងប្រយ័ត្នចំពោះការចែករំលែកព័ត៌មាន សំឡេង រូបភាព ឬវីដេអូ របស់អ្នកជាសាធារណៈ ព្រោះវាអាចឱ្យជនខិលខូចយកមាតិកាទាំងនោះទៅក្លែងបន្លំជាអ្នក ដើម្បីប្រព្រឹត្តបទល្មើសផ្សេងៗ និង
- មិនត្រូវផ្តល់ទិន្នន័យផ្ទាល់ខ្លួន ជាអាទិ៍ លេខកូដសម្ងាត់គណនីធនាគារ លេខកូដបណ្តាញទំនាក់ទំនងសង្គម លេខកូដផ្ទៀងផ្ទាត់ ឬព័ត៌មានសំខាន់ផ្សេងៗ ទៅជនដែលសង្ស័យ ជាដាច់ខាត។

សម្រាប់ព័ត៌មានបច្ចេកទេសពាក់ព័ន្ធនឹងបញ្ហានេះ អ្នកប្រើប្រាស់អាចស្វែងយល់បន្ថែមក្នុងគេហទំព័ររបស់ "ការិយាល័យឆ្លើយតបបញ្ហាបន្ទាន់នៃកុំព្យូទ័រ (CamCERT)" របស់នាយកដ្ឋានសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍និងព័ត៌មាននៃ **អ.ប.ទ**. ដែលមានអាសយដ្ឋាន www.camcert.gov.kh ឬរាយការណ៍ ឬសុំជំនួយបច្ចេកទេសបន្ថែមតាមរយៈអ៊ីមែល incident@camcert.gov.kh ឬទូរសព្ទលេខ ០២៣ ៧២២ ៣៩១ / ០១៦ ៨៥១ ៦៧៨។

អាស្រ័យដូចបានជម្រាបជូនខាងលើ សូមសាធារណជនទាំងអស់ មេត្តាជ្រាបជាព័ត៌មាន និងសូមបង្កើនការប្រុងប្រយ័ត្នខ្ពស់ចំពោះឧបាយកលឆបោកនេះ។