

ကိရိယာအစုစု တည်ဆောက်နည်း 2026 လမ်းညွှန် ကိုယ်ပိုင် ဒစ်ဂျစ်တယ်ကာကွယ်ရေး



01 ဖုန်းခေါ်ဆိုမှုများ၊ မက်ဆေ့ချ်များနှင့် အီးမေးလ်ဝန်ဆောင်မှုများကို ညှစ်ဖျက်မှု အသုံးပြုပါ

မိမိ၏ ဖုန်းခေါ်ဆိုမှုနှင့် စာပို့မှတ်တမ်းများကို တရားဥပဒေစိုးမိုးရေးအဖွဲ့က ဝင်ရောက်ကြည့်ရှုခြင်းမှ ကာကွယ်ရန် သင့်ကိုယ်ပိုင်ဖုန်းနံပါတ်နှင့် ချိတ်ဆက်မထားသော **End-to-end ကုဒ်ဝှက်စနစ် (E2EE)** ပါရှိသည့် Signal သို့မဟုတ် Hushed ကဲ့သို့ အက်ပ်များကို အသုံးပြုပါ။

Kakao Talk နှင့် Telegram တွင် “Secret Chats” ကို ဖွင့်၍ E2EE ကို ဖွင့်နိုင်သည်။

အရေးကြီးစာရွက်စာတမ်းများ ပေးပို့သည့်အခါ သင့် ကိုယ်ပိုင်အီးမေးလ်နှင့် ချိတ်ဆက်မထားသော အခြားအီးမေးလ်အကောင့်တစ်ခုကို အသုံးပြုပါ။

အချို့သော အီးမေးလ်ဝန်ဆောင်မှုပေးသူများသည် သင့်ဒေတာကို ကြော်ငြာရှင်များ သို့မဟုတ် တရားဥပဒေစိုးမိုးရေးအဖွဲ့များနှင့် မျှဝေနိုင်သည်။ အောက်ပါကဲ့သို့သော စကားလုံးများကို သတိထားပါ-

“ကျွန်ုပ်တို့သည် ဒေတာကို ပါတနာများနှင့် မျှဝေနိုင်သည်” သို့မဟုတ် “ကျွန်ုပ်တို့၏ဝန်ဆောင်မှုများ ပိုမိုကောင်းမွန်လာစေရန် အီးမေးလ်များကို စကန်ဖတ်နိုင်ခြေရှိသည်”

02 ဆိုရှယ်မီဒီယာတွင် အကောင်းဆုံးပြုမှုနည်းများကို ကျင့်သုံးပါ

သင့်ပို့စစ်များ၊ သူငယ်ချင်းများနှင့် တည်နေရာများအား မြင်နိုင်မည့်သူကို ကန့်သတ်ရန် သင့်အကောင့်များကို သီးသန့်သတ်မှတ်ထားပါ။
အလိုအလျောက် တည်နေရာခြေရာခံခြင်းကို ပိတ်ထားပြီး မွေးနေ့များ သို့မဟုတ် အလုပ်တည်နေရာကဲ့သို့ ကိုယ်ရေးကိုယ်တာအချက်အလက်များအား မျှဝေခြင်းကို ရှောင်ကြဉ်ပါ။

လတ်တလော DHS မူဝါဒ ဖော်ဆောင်ထားမှုများအရ လူဝင်မှုကြီးကြပ်ရေးဥပဒေအရာရှိများအား ဆိုရှယ်မီဒီယာရှိ သင်၏ လှုပ်ရှားမှုများကို လွန်ခဲ့သော 5 နှစ်အထိ ပြန်လည်ကြည့်ရှုခွင့်ပေးထားသည်။

03 အွန်လိုင်းခြေရာခံခြင်းနှင့် ပစ်မှတ်ထားကြော်ငြာခြင်းကို ကန့်သတ်ပါ

DHS တံမှ မိမိဆန္ဒအလျောက် နေရပ်ပြန်ခြင်းနှင့်ပတ်သက်သည့် ကြော်ငြာစာများကို ရရှိနေပါသလား။ အခြားသူများမြင်ရသည့် ဈေးနှုန်းများထက် ပိုများသော ကုန်ပစ္စည်းဈေးနှုန်းများကို မြင်တွေ့နေရပါသလား။ သင့် ပစ်မှတ်ထားခံနေရပါပြီ။

ဆိုရှယ်မီဒီယာပေါ်တွင် တစ်ဦးချင်းနှင့်ကိုက်ညီအောင် ပြုလုပ်ထားသော ကြော်ငြာများကို ငြင်းပယ်ပါ။ သင့်ဖုန်းတွင် မိုဘိုင်းကြော်ငြာ ID ကို ပိတ်ပါ။ သင့်အက်ပ်များအတွက် တည်နေရာခွင့်ပြုချက်များကို ပိတ်ထားပါ။ ထို့အပြင် “reject all cookies” ကို အမြန်ပိတ်ပါ။ **ကျန်းမာရေးဆေးခန်းများ၊ ဥပဒေရေးရာရုံးဌာနများ သို့မဟုတ် ဆန္ဒပြပွဲများသို့ သွားရောက်လျှင် တည်နေရာဝန်ဆောင်မှုများကို အမြဲပိတ်ထားပါ။**

04 ခရီးသွားနေစဉ် သို့မဟုတ် ထိခိုက်လွယ်သော လှုပ်ရှားမှုများတွင် ပါဝင်နေစဉ် ဒစ်ဂျစ်တယ်လိုဒြိုရေကို ကျင့်သုံးပါ

သင် သွားလိုသည့်နေရာသို့ ရောက်ရန်အတွက် လမ်းကြောင်းပြစနစ်ကို အသုံးပြုရန် လိုအပ်ပါက အင်တာနက်ချိတ်ဆက်မှုမလိုအပ်သော အော့ဖ်လိုင်းအက်ပ်များကို အသုံးပြုပါ။

အလိုအလျောက်လိုင်စင်နံပါတ်ဖတ်စက်များ (ALPR's) က သင့်ကား၏ သွားလာမှုကို ပြည်နယ်အနှံ့ ခြေရာခံနိုင်သည်ကို သတိပြုပါ။ ယင်းအစား အများပြည်သူ သုံးသယ်ယူပို့ဆောင်ရေးယာဉ်များ သို့မဟုတ် တက္ကစီများကို အသုံးပြုသင့်သည်။”



ကိုယ်ရေးလိုဒြိုမုဆိုင်ရာ အကာအကွယ်များသည် များသောအားဖြင့် နယ်စပ်ရှိ နယ်ခြားစောင့်အရာရှိများ၏ ဆုံးဖြတ်ချက်အပေါ်တွင် မူတည်သည်။

ကိုယ်ရေးကိုယ်တာ ခရီးသွားလာမှု အန္တရာယ်ကို အကဲဖြတ်သည့်အခါ နိုင်ငံရေးအခြေအနေနှင့် လက်ရှိ သတင်းများကို ထည့်သွင်းစဉ်းစားပါ။

မျက်နှာ ID နှင့် လက်မေ့ စကန်ဖတ်ခြင်းကို ပိတ်ထားပါ—သင့်ဖုန်းကို သိမ်းဆည်းခံရပါက တရားဥပဒေစိုးမိုးရေးအဖွဲ့သည် သင့်ဖုန်းကို လော့ခံဖွင့်ရန်အတွက် ထိုအရာများကို အသုံးပြုနိုင်သော်လည်း ပင်နံပါတ်ကိုမူ သုံးမရနိုင်ပါ။

05 AI ချတ်ဘော့များကို သတိကြီးစွာချင့်ချိန်၍ လျော့၍အသုံးပြုပါ

သင့်အမည်၊ နေရပ်လိပ်စာ၊ အမှုကိစ္စ အသေးစိတ်အချက်အလက်များ၊ လူဝင်မှုကြီးကြပ်ရေးအခြေအနေ သို့မဟုတ် အထောက်အထားအချက်အလက်များကဲ့သို့ ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို AI ချတ်ဘော့များထံသို့ မည်သည့်အခါမှ မထည့်ပါနှင့်။

စကားပြောထားသည့် မှတ်တမ်းကို သိမ်းဆည်းထားပြီး အနာဂတ် မော်ဒယ်များ ထုတ်လုပ်ရာတွင် ၎င်းကို အသုံးချနိုင်သည်။

“ကျွန်ုပ်တို့သည် အထောက်အထားမရှိသူဖြစ်ပြီး ICE က ကျွန်ုပ်တို့၏ အိမ်ရှေ့သို့ ရောက်လာပါက သတိထားရန်လိုအပ်သည့် ရပိုင်ခွင့်များ” ဟု ထည့်မည့်အစား

“ICE နှင့်ကြုံတွေ့ချိန်တွင် ရွှေ့ပြောင်းနေထိုင်သူများ၏ အကြမ်းဖျင်းရပိုင်ခွင့်များမှာ အဘယ်နည်း။” ဟု ChatGPT ကို မေးပါ။

06 စောင့်ကြည့်ရေးကင်မရာများနှင့် စမတ်အိမ်သုံးစက်ပစ္စည်းများကို သတိဖြင့် အသုံးပြုပါ

ခွင့်ပြုထားသော အသုံးပြုသူများနှင့် တရားဥပဒေစိုးမိုးရေးအဖွဲ့သည် စမတ်အိမ်သုံးစက်ပစ္စည်းများရှိ အရေးကြီးသော သက်သေ၊ မှတ်တမ်းများ သို့မဟုတ် စက်ကိရိယာထိန်းချုပ်စနစ်များကို သင့်အား အသိပေးခြင်းမရှိဘဲ ဝင်ရောက်ကြည့်ရှုနိုင်သည်။

သင့်ကင်မရာများနှင့် စမတ်စပီကာများကို ဝင်ရောက်ကြည့်ရှုခွင့်ရှိသူများအား သိရှိရန် စက်ပစ္စည်းခွင့်ပြုချက်များကို ပုံမှန်စစ်ဆေးပါ သို့မဟုတ် သင့် စမတ်အိမ်သုံးစက်ပစ္စည်းများကို လုံးဝဖယ်ရှားပစ်ရန် စဉ်းစားပါ။

07 အများပြည်သူသုံးနေရာများတွင် ကိုယ်ရေးလိုဒြိုမုကို ထည့်သွင်းစဉ်းစားပါ

အစိုးရအဆောက်အအုံများ၊ ဘူတာရုံများ၊ ဈေးဝယ်ရာနေရာများနှင့် နယ်စပ်များကဲ့သို့ အများပြည်သူသုံးနေရာများတွင် ပိုမိုတင်းကျပ်စွာ စောင့်ကြည့်နေတတ်ပါသည်။ **စောင့်ကြည့်ရေးကင်မရာများ၊ လိုင်စင်နံပါတ်ဖတ်စက်များ၊ မျက်နှာခွဲခြားသိနိုင်သောနည်းပညာနှင့် အနီးနားရှိ ကြိုးမဲ့ကွန်ရက်များကိုပင် ဥပဒေစိုးမိုးရေးအဖွဲ့က သင့်အား ခွဲခြားသိရှိရန် အသုံးပြုနိုင်သည်ကို သတိပြုပါ။**



ICE သည် ၎င်းတို့၏ လူဝင်မှုကြီးကြပ်ရေး ဖမ်းဆီးမှုများကို အရှိန်မြှင့်ရန် မျက်နှာခွဲခြားသိနိုင်သော နည်းပညာအက်ပ်များကို အသုံးပြုလျက်ရှိသည်။

ထိုကိရိယာများသည် အာရှတိုက်သား၏ မျက်နှာများအား ခွဲခြားဖော်ထုတ်ရာတွင် တိကျမှန်ကန်ပြီး မှားယွင်းဖမ်းဆီးမှုများ ဖြစ်ပေါ်စေနိုင်သည်ကို သတိပြုပါ။

သင်သည် အလွန်အန္တရာယ်များသော အခြေအနေတွင်ရှိနေပါက နှာခေါင်းစည်းတပ်၍ ဦးထုပ်ဆောင်းခြင်း၊ ဘလူးတူ့စ်နှင့် WiFi ကို လတ်တလောတွင် အသုံးမပြုနေသည့်အခါ ပိတ်ထားခြင်းနှင့် အွန်လိုင်းတွင် ပို့စတင်ရန်အတွက် ဓာတ်ပုံရိုက်နေသူများကို ရှောင်ရှားခြင်းတို့ကို ပြုလုပ်သင့်သည်။