Consumer Watch

Digital Consumer ဥပဒေ

စာရေးသူတို့ တော်တော်များများဟာ ငွေကြေးဆိုင်ရာ စာရင်းဇယားတွေ၊ ကျန်းမာရေးဆိုင်ရာ အချက်အလက်တွေ၊ စာရွက်စာတမ်းတွေ၊ social network ဆိုင်ရာ အချက်အလက်တွေကို web အပေါ်မှာ တင်ထားလေ့ရှိ ပါတယ်။ ဒါပေမဲ့ ဒီအချက်အလက်တွေကို အလွဲသုံးစားမလုပ်စေရပါဘူး ဆိုတဲ့ အာမခံက နည်းပါးပါတယ်။

အဲဒီ data တွေဟာ ပျောက်သွားနိုင်ပြီး အခိုးလည်း ခံရနိုင်ပါတယ်။ ဒါကြောင့် web အပေါ်မှာ အချက်အလက်တွေ သိမ်းထားတတ်သူတွေ၊ digital data ၊ digital content တွေနဲ့ အလုပ်လုပ်သူတွေအတွက် digital အချက်အလက်ဆိုင်ရာတွေအတွက် လုံခြုံရေးဥပဒေ တစ်ရပ်ရှိရမယ့်အပြင်မှာ ဥပဒေကိုလိုက်နာအောင် ဖော်ဆောင်ပေးမယ့် အဖွဲ့အစည်းတစ်ခုလည်း လိုအပ်နေပါတယ်။ ဒီဥပဒေဖြစ်ပေါ်လာဖို့အတွက် ဆွေးနွေးထားတာတွေ ကို *(find.pcworld.com/ 72738)* မှာ အသေးစိတ် ဖတ်နိုင်ပါတယ်။

Internet ကုမ္ပဏီတွေဟာ သုံးစွဲသူတွေဆီက အချက်အလက်တွေကို ကောက်ခံတာ၊ သိမ်းဆည်းတာ၊ ပုံစံပြောင်းပြီး တခြားနေရာမှာ သုံးစွဲတာ၊ ကြော်ငြာကိစ္စတွေမှာ သုံးစွဲတာ၊ third-party အဖွဲ့အစည်းတွေမှာ သုံးနိုင်ဖို့ ပေးလိုက်တာ စတာတွေဟာ တရားဝင်ရဲ့လား၊ လုပ်ခွင့်ရှိရဲ့လား။ လုပ်ပိုင်ခွင့်ရော တောင်းဖို့လိုအပ်ပါသလား၊ ဆိုတာတွေကို ပွင့်ပွင့်လင်းလင်း သိရှိအောင် လုပ်ထားဖို့ လိုပါတယ်။ အများအားဖြင့် internet ကုမ္ပဏီတွေဟာ data တွေကို ပြန်လည်ရောင်းချတဲ့ ကိစ္စတွေ ပါရှိနေတဲ့အတွက် သူတို့ အကျိုးအမြတ်အတွက် တခြားသူတွေရဲ့လုံခြုံရေးကို ချိုးဖောက်စေမှာ လားဆိုတာတွေကိုပါ စဉ်းစားဖို့ လိုအပ်နေပါတယ်။

ဒီလို website တွေကို သုံးမယ်ဆိုရင် သုံးစွဲသူတွေက အချက်အလက်တွေပေးမယ်၊ မပေးဘူးဆိုတာ ရွေးချယ်ခွင့်ရှိပါတယ်။ ဒီလိုလုပ်၊ မလုပ်ဆိုတာကလည်း Privacy Policy ရဲ့ တစ်နေရာမှာ မြုပ်နေလေ့ရှိပါတယ်။ ဒီလို အချက်အလက်တွေရယူတယ်ဆိုတာက ဥပဒေ အကြောင်း အရလည်း ဘောင်ဝင်၊ မဝင်ဆိုတာလည်း အများကြီး စဉ်းစားရပါသေးတယ်။

အသုံးပြုသူတွေရဲ့ အချက်အလက်တွေကို online အပေါ်က storage တွေမှာ သိမ်းထားတယ်ဆိုရင် ဒီအဖွဲ့အစည်းတွေက ဒီဝန်ဆောင်မှုတွေ အတွက် ဝန်ဆောင်ခအကျိုးအမြတ်ရပါတယ်။ ဒါပေမဲ့ နောက်ကွယ်မှာတော့ ဒီလိုရတဲ့ ဝန်ဆောင်ခအပြင်မှာ ဒီကုမ္ပဏီတွေက အချက်အလက်တွေကို ဘယ်သူ့အချက်အလက်တွေမှန်းမသိအောင် ပြုပြင်ပြောင်းလဲလိုက်ပြီး၊ ကြော်ငြာကုမ္ပဏီတွေ၊ internet အပေါ်မှာ web marketing ကုမ္ပဏီ ကုမ္ပဏီတွေကို ငွေကြေးနဲ့ရောင်းချတတ်ကြတယ်။

ဘယ်လိုပဲဖြစ်ဖြစ် စာရေးသူ သတင်းအချက်အလက်တွေဟာ တန်ဖိုးရှိပြီး အရေးကြီးပါတယ်။ ဒီအချက်အလက်တွေကို ပိုင်ဆိုင်တာဟာ အပြင်မှာရှိတဲ့ ပစ္စည်းဥစ္စာတွေကို ပိုင်ဆိုင်သလိုပဲ ဖြစ်ပါတယ်။ အလွဲသုံးစားအလုပ်ခံရရင်၊ အခိုးခံရရင် တရားစွဲဆိုခွင့်၊ နစ်နာမှုအတွက် လျော်ကြေးတောင်းခွင့်တွေတော့ ရရှိသင့်ပါတယ်။ အခိုးခံရပြီးတဲ့နောက် မြိမ်းခြောက်မှုတွေခံရရင် ဘယ်လိုလုပ်ကြပါလဲ။ လျှို့ဝှက်ချက်တွေပေါက်ကြားကုန်ရင်လည်း ဒုက္ခရောက်နိုင်ပါတယ်။ ပြိုင်ဘက်တွေဆီကို ရောက်သွားရင်လည်း ယှဉ်ပြိုင်မှုမှာ နောက်ကျကျန်နိုင်ပါတယ်။

Mega Upload မှာဖြစ်ခဲ့တဲ့ ကိစ္စတစ်ခုကို ပြန်လေ့လာကြည့်မယ်ဆိုရင် တကယ်လို့ ကုမ္ပဏီတစ်ခုက ဥပဒေပိုင်းအရ ချိုးဖောက်မှုတွေဖြစ်

လာတော့ site ကို သုံးမရအောင် ပိတ်လိုက်မှာ ဖြစ်ပြီး၊ သုံးစွဲသူတွေရဲ့ file တွေဟာ တရားဝင်ပါတယ်ဆိုတဲ့တိုင်အောင် အဲဒီ file တွေကို စုံစမ်း စစ်ဆေးရေးအမဲ့ဆီကို ပွဲပြောင်းပေးထားရမှာဖြစ်ပါတယ်။ သက်သေအနေနဲ့ စစ်ဆေးပြီး မှန်ကန်တယ်ဆိုမှ သုံးစွဲသူတွေဆီသို့ ပြန်ပေးမှာ ဖြစ်ပါတယ်။

ဘယ် internet ကုမ္ပဏီမဆို data တစ်ခုကို သိမ်းထားပေးတယ်ဆိုရင် ထိုကဲ့သင့်တဲ့ security level တစ်ခုနဲ့ ကာကွယ်ပေးထားရမှာ ဖြစ်ပါတယ်။ အဲဒီ data security ဆိုင်ရာ ဥပဒေဟာ အမေရိကန်ပြည်ထောင်စုရဲ့ ပြည်နယ်ပေါင်း ၄၅ ခုမှာ အတည်ပြုပြဋ္ဌာန်းပြီးဖြစ်ပါတယ်။ Fealeral Trade Commission ကလည်း data-security ဆိုင်ရာညွှန်ကြားချက်တွေ ချမှတ်ပြီးဖြစ်ပါတယ်။ လုံခြုံရေးဆိုင်ရာကိစ္စရပ်တွေ ကိုင်တွယ်ရာမှာ အမြဲ upgrade လုပ်နေဖို့ လိုအပ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ နေ့စဉ်ဒုံအမျှ hacking နည်းတွေ တိုးတက်လာတာကြောင့်ပါ။

မကြာခင်အစိုးရက D order ဆိုတဲ့ ဥပဒေတစ်ရပ်ထုတ်ပြန်ခဲ့တယ်။ ဒါဟာ Stored Communications Act က အပိုဒ် ၂၇၀၃ အပိုဒ်ခွဲ D အရ ပြဋ္ဌာန်းထားတဲ့ဥပဒေဖြစ်တယ်။ အဲဒီဥပဒေအရ တရားရုံးက အဖိန့်တစ်ခုထုတ်ပြီး ISP တစ်ခုမှ သုံးစွဲသူတွေရဲ့ email address တွေ၊ IP address တွေအပါအဝင် သူတို့နဲ့ အပြန်အလှန်ဆက်သွယ်နေတဲ့ အချက်အလက်တွေကို ကောင်းဆိုခွင့်ရှိပါတယ်။ ဒါတင်မက သုံးစွဲသူတွေ ကြည့်ရှုခဲ့တဲ့ webpage တွေကိုလည်း ရယူနိုင်တဲ့အပြင် ဘယ်နေရာမှာ သုံးစွဲနေတယ်၊ ဘယ်ကို phone ခေါ်ဆိုမှုတွေပြုလုပ်ခဲ့တယ်၊ စတဲ့အချက် အလက်အသေးစိတ်တွေကိုပါ ရယူပိုင်ခွင့်ရှိတယ်။

အနှစ်ချုပ်အားဖြင့် အဲဒီ D order ဥပဒေကို ဝေဖန်ရရင် သုံးစွဲသူတွေ ရဲ့ internet အသုံးချမှုတွေအပြင် GPS တည်နေရာတွေကို ဥပဒေကြောင်းအရ အပြည့်အဝပိုင်ဆိုင်ခွင့်ရှိတဲ့ ရာဇဖွဲ့ရမ်းပုံစံတစ်ခုဖြစ်တယ်။ ဒီနည်းနဲ့ မူခင်းတစ်ခုဖြစ်ပေါ်ခဲ့ရင် သက်သေခံချက်တွေ ရရှိနိုင်မှာ ဖြစ်ပါတယ်။

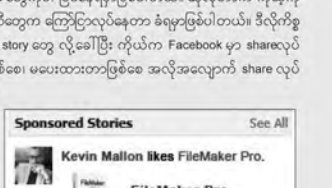
ဒီလို ဥပဒေပေါ်လာတာဟာ ဥပဒေချိုးဖောက်သူတွေ၊ ချိုးဖောက်မယ်လို့ သံသယရှိသူတွေကို ဧောင့်ကြည့်နိုင်တဲ့ အကူအညီတစ်ခုဖြစ်လာပေ မယ့်လည်း သာမန်နိုင်ငံသားတွေအတွက်တော့ ကိုယ်ရေးကိုယ်တာ ကိန္ဒတွေမှာ လုံခြုံမှုမရှိနိုင်တော့ကြောင်း ခံစားလာရတယ်။ အမေရိကန်ပြည်ထောင်စုရဲ့ သမိုင်းတစ်လျှောက်မှာ ဒီလိုလုပ်ဆောင်မှုတွေ များစွာရှိခဲ့တယ်။ ဒါကြောင့်လည်း digital ခေတ်ရောက်လာတဲ့အခါမှာလည်း အလွှာပေးမှာမဟုတ်ဘဲ တင်းကြပ်မှုတွေ ဆက်လက်ရှိနေဦးမှာ ဖြစ်ပါတယ်။

တစ်ကမ္ဘာလုံးရှိ ကုမ္ပဏီပေါင်းများစွာက သူတို့ထံမှ အချက်အလက်တွေပျောက်ဆုံးကြောင်း၊ အစိုးခံရကြောင်း သတင်းပို့အကြောင်း ကြားမှုတွေရှိလာပါတယ်။ The Privacy Cleaninghouse က ၂၀၀၅ ခုနှစ် ကတည်းက ယခုအချိန်အထိ အရေးကြီးအချက်အလက်ပေါင်း သန်း ၅၀၀ ကျော် ချိုးဖောက်ခံခဲ့ရကြောင်း၊ ၂၀၁၁ တစ်နှစ်တည်းမှာပဲ ၂၂.၄ သန်းမျှရှိတဲ့ အကြောင်းအရာတွေ ချိုးဖောက်ခံခဲ့ရတယ်လို့ ပြောကြားခဲ့ တယ်။ ဒီနှစ်နှစ်မှတွေအတွက် ဘယ်လိုဘယ်ပုံ စီမံရမယ်ဆိုတာကလည်း ကြန့်ကြာနေဦးမှာ ဖြစ်တယ်။

Facebook မှာ Like မလုပ်ခင် စဉ်းစားပါ

Facebook သုံးနေရင်း အကြောင်းအရာတစ်ခုခုကို ကြိုက်နှစ်သက်ခဲ့ရင် Like button ကိုနှိပ်ပြီး ထောက်ခံအားပေးမှုတွေပြုလုပ်လေ့ရှိပါတယ်။ ဒီလိုပါပဲ မိမိကြိုက်နှစ်သက်တဲ့ ကုန်ပစ္စည်းတစ်ခု၊ ကုမ္ပဏီတစ်ခုဆိုရင် လည်း Like နှိပ်ပြီး အားပေးလေ့ရှိကြပါတယ်။ လူတွေမသိကြတာက ဒီလို Like နှိပ်ပြီးတဲ့ နောက် ကွယ်ကဖြစ်ရပ်တွေ ဖြစ်ပါတယ်။

ကုမ္ပဏီတစ်ခုရဲ့ page ကို Like လုပ်ပြီးရင် သူ့ရဲ့ location တွေ၊ product တစ်ခု၊ ဝန်ဆောင်မှုတစ်ခု update လုပ်တာနဲ့ တင်လိုက်တဲ့ သတင်းအချက်အလက်တွေ စသဖြင့် ကိုယ့် wall အပေါ်မှာ ပေါ်လာမှာ ဖြစ်ပြီး ကိုယ့်မိတ်ဆွေတွေက အဲဒီ update တွေကိုပါ မြင်နေရမှာဖြစ်ပါတယ်။ ဆိုလိုတာက ကိုယ့်ကို ခုထုံးလုပ်ပြီး ကုမ္ပဏီတွေက ကြော်ငြာလုပ်နေတာ ခံရမှာဖြစ်ပါတယ်။ ဒီလိုကိစ္စတွေကို sponsored story တွေ လို့ခေါ်ပြီး ကိုယ်က Facebook မှာ shareလုပ်ခွင့်ပေးထားတာဖြစ်ခဲ့ရ၊ မပေးထားတာဖြစ်စေ အလိုအလျောက် share လုပ်သွားမှာဖြစ်တယ်။



Facebook ရဲ့ video တစ်ခုမှာ product manager တစ်ယောက်က အဲဒီ story တွေဟာ ကိုယ့်ရဲ့ ခွင့်ပြုချက်နဲ့ပဲ ကိုယ့်မိတ်ဆွေတွေဆီရောက်သွားမှာ ဖြစ်တယ်လို့ ရှင်းလင်းခဲ့ပါတယ်။ ဒါပေမဲ့ ကိုယ်က recommend လုပ်ပြီး ကိုယ့်မိတ်ဆွေတွေသိစေတာနဲ့ Facebook ကနေ ကိုယ့်ကိုယ်စားဝင်လိုက်တာနဲ့ ဘာများကွာခြားမှုရှိပါသလဲ။

Sponsored Story တွေဟာ သူတို့ရဲ့ feed ထဲမှာပဲရှိလို့ မကြိုက်ရင် ignore လုပ်တာဖြစ်စေ၊ ဖျက်ပစ်တာဖြစ်စေ လုပ်နိုင်ပါတယ်။ ဒါပေမဲ့အခုအချိန်မှာတော့ Facebook ဟာ feed တွေကို user တွေရဲ့ new feed အနေနဲ့ထည့်ပေးနေပြီဖြစ်ပါတယ်။ Facebook ကနေ ဒီလိုမလုပ်အောင်တားမို့ မဖြစ်နိုင်သေးပါဘူး။ ဒါကြောင့်ပဲ ကိုယ်ကိုယ်တိုင်ပဲ စနစ်တကျ သတိရှိရှိသုံးဖို့ လိုအပ်ပါတယ်။ Like button တစ်ခုကို မနှိပ်ခင်မှာ ဖြစ်ခြင်း၊ ဆိုင်တစ်ခု ၊ ဒါမှမဟုတ် စားသောက်ဆိုင်တစ်ဆိုင်မှာ check-in မဝင်ခင်မှာဖြစ်ဖြစ်၊ product ၊ ဒါမှမဟုတ် ဝန်ဆောင်မှုတစ်ခုအကြောင်း ကို update မလုပ်ခင်မှာဖြစ်ဖြစ်၊ ကိုယ့်လူပ်ရှားမှု၊ လုပ်ကိုင်နိုင်မှုတွေကို track လုပ်နိုင်တဲ့ app တစ်ခု install မလုပ်ခင်မှာဖြစ်ဖြစ် စဉ်းစားသင့်ပါတယ်။ ကိုယ်ကိုယ်တိုင် ဒီ product ၊ ဒါမှမဟုတ် ဝန်ဆောင်မှုတစ်ခုကို ကိုယ့်မိတ်ဆွေ သူငယ်ချင်းတွေကို အမှန်တကယ်ပဲ သိစေချင်ရဲ့လား ဆိုတာပဲ ဖြစ်ပါတယ်။ တကယ်လို့ ကိုယ်တိုင်လည်း မကြိုက်၊ တခြားသူတွေကိုလည်း မညွှန်လိုသူးဆိုရင်တော့ ကိုယ့်ကိုခုတုံးလုပ်ပြီး ကြော်ငြာသူတွေကို ဆက်မလုပ်နိုင်အောင် Like button တွေကိုတွေ့တိုင်း မနှိပ်မိဖို့ လိုအပ်ပါတယ်။

ကောင်းမြတ်ထွန်း