

Lætt at stovna falska vangamynd

Ber til at stóla upp á vangamyndirnar á Facebook? Kendi bloggarin, Michael Arrington hefur gjørt eitt eksperiment fyri at vísa, at mann lættliga kann stovna eina vangamynd undir følskum navni á Facebook.

Arrington brúkti veruligu teldupostadressuna hjá Google-stjóranum Eric Smith fyri at stovna eina vangamynd við eini mynd av honum. Út frá teldupostadressuni byrjaði Facebook alt fyri eitt at viðmæla vinfólk til tann falska Eric Smith – bæði maðurin aftan fyri Youtube, Chad Hurley, og marknaðarstjórin á Facebook, Elliot Schrage søgdu ja til vinarumbønina frá følsku vangamyndini hjá Eric Smith. Hareftir kom ein riðil av vinarumbønum til “Eric Smith”.

Tað, sum hefur serliga týðning, er teldupostadressan. Tá tú stovnar eina konto hjá Facebook, verður tú biðin um at játta teldupostadressuna við at reagera upp á ein

teldupost, sum verður sendur til teldupostadressuna. Tað er tískil bara veruligi eigarin av adressuni, ið kann síggja teldupostin.

Trupulleikin er tann, at hóast tú ikki reagerar upp á teldupostin frá Facebook, ber framvegis til at brúka tær flestu funktiónirnar á Facebook undir nýggju kontoini, senda vinarumbønir og gera stóðudagfóringar.

Hetta merkir, at tú kanst stovna eina falska vangamynd undir navninum hjá einum øðrum persóni og teldupostadressu, so leingi hesin persónurin ikki frammanundan hefur upplýst teldupostadressuna í samband við stovning av eini aðrari Facebook vangamynd.

Ein møguleiki at tryggja seg móti hesum svikinum er tí at leggja allar teldupostadressur, sum mann hefur, afturat aktivu vangamyndini, sum mann hefur á Facebook.

Kelda: channelworld.dk

6 góð ráð

Ynskir tú at sleppa undan, at tín Facebook vangamynd verður hakkað, at spamleinkjur verða send til tíni online-vinfólk, ella at allar applikatióir fylgja við í, hvat tú gert á sosiala miðlinum? Her eru seks góð ráð fyri at gera Facebook vangamyndina tryggari

1) Tak einans ímóti vinarumbønum frá fólki, tú kennir.

Jú færri fólk hava atgongd til tína vangamynd jú betri. Syrgir tú fyri, at einans vinfólk síggja tínar upplýsingar, myndir, stóðudagfóringar og so framvegis, ert tú væl tryggjaður. Til ber at gera innstillingar á Facebook, soleiðis at bert vinfólkini síggja tínar upplýsingar og eingin annar.

2) Bert tú á vegginum.

Mest vanligi mátin at spreidda malware á Facebook er at hakka eina konto og koyra falskar leinkjur á veggirnar hjá vinfólkunum. Innstilla veggina á Facebook soleiðis, at tað einans er tú, ið kann leggja nakað út á veggina.

3) Kryptering

Undir “Sikkerhed” í kontoinnstillingunum ber til at aktivera “Sikker browsing”, so at alt, tú gert á netinum, verður krypterað og til ber ikki at fylgja við í tí, tú gert online.

4) Ansa eftir applikatiónum

Tað finnst ein rúgva av applikatiónum, hvørs einasta endamál er at spamma tín vegg á Facebook. Eingin applikatión vísir, til dømis hvør fylgir tær mest á Facebook. Hesar applikatióirnar eru allar falskar – lat vera við at brúka tær.

5) Fleiri møguleikar við myndum

Um tú eitt nú hefur myndir liggjandi á Facebook, har tú til dømis ert í veitslu og stendur við eini øl í hondini, kanst tú velja, at tað einans eru ávís vinfólk, sum kunnu síggja myndirnar.

6) Brúka vit og skil

Facebook ger nógv fyri at tú kanst ferðast trygt á sosiala miðlinum, og tað er ikki heilt lætt at hakka og misbrúka eina vangamynd í dag. Tað krevur í stuttum, at TÚ gert onkran feil. Gert tú ikki tað, kanst tú ferðast rættiliga trygt á Facebook.