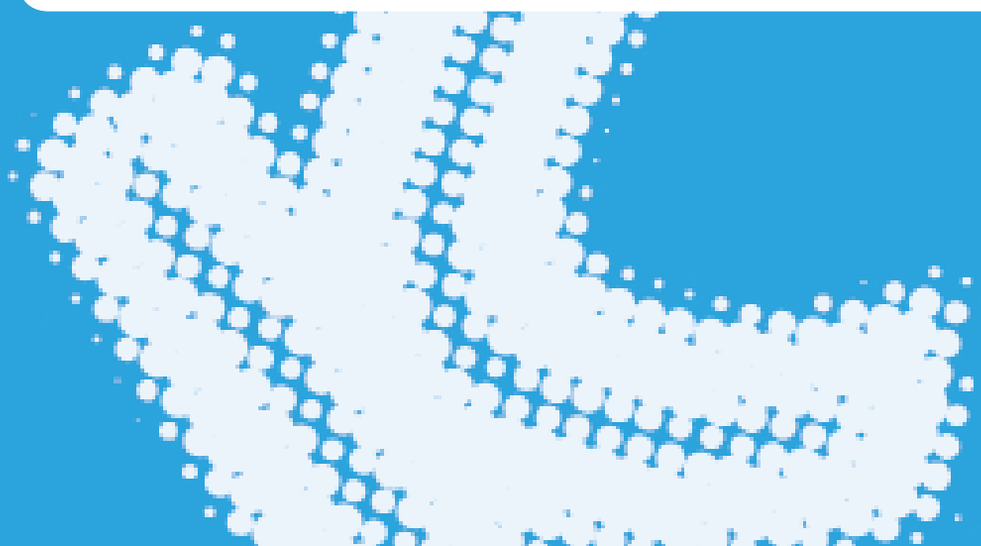
11. ALDIZKARIA. 2011

REVISTA Kontsumo ALDIZKARIA

Zuri gerta dakizuke



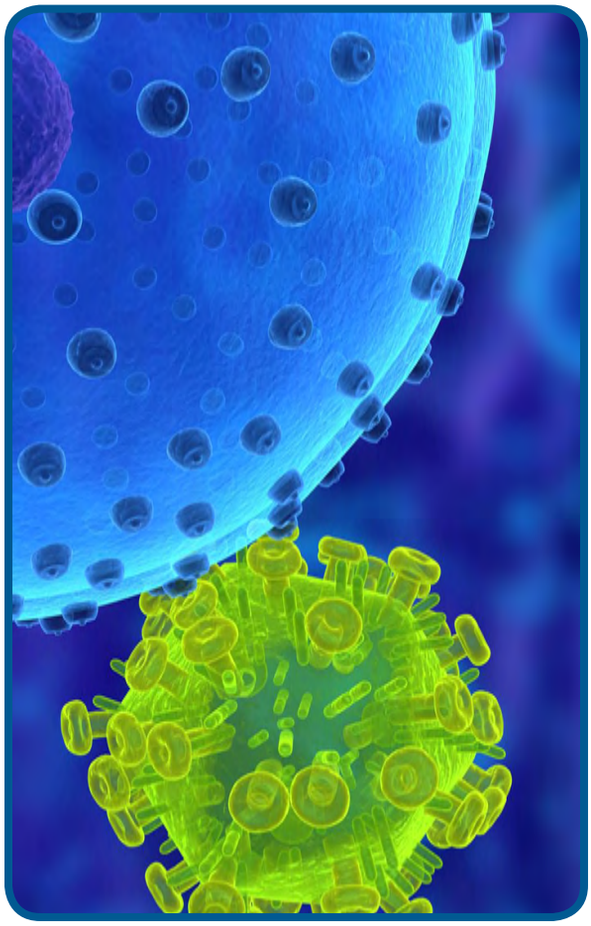
Zuri gerta dakizuke

Azken urteetan, hedatzeko gizarte-sareez baliatzen dira mehatxu informatikoak gero eta ugariagoak dira. Horren haritik, garrantzitsua da horri buruzko informazioa edukitzea, horien erabilera seguru bat egin ahal izateko.

Duela gutxi, Facebook kako gisa erabiltzen duten bi kode gaizto agertu dira.

Alde batetik, Asprox.N dugu, posta elektronikoaren bitartez ekipora iristen den troiarra. Erabiltzaileari iruzur egiten saiatzen da, bere Facebookeko kontua spam banatzen ari dela esanez, eta, arrazoi horrengatik eta bere segurtasunerako, bere pasahitzak aldatu egin direla. Word dokumentu faltsu bat eransten du, eta suposatzen da bertan erabiltzailearen pasahitz berria agertzen dela. Postari erantsitako artxiboak ohikoaren aldean desberdina den word dokumentu baten ikonoa agertzen du Facebook_details.exe deitua. Artxibo hori, benetan, “harra” da, eta behin exekutatzen denean, .doc artxibo bat deskargatzen du, eta horrek testu-prozesadorea exekutatzen du, eta erabiltzaileari sinetaraziz postari erantsitako jatorrizko artxiboa benetan ireki dela.

Troiarrak, behin exekutatu denean, beste fitxategi bat deskargatzen du. Horren funtzioa da portu erabilgarri guztiak irekitzea, eta hainbat hornitzaileren posta-zerbitzuetara konektatzea, horrela, albait pertsona kopuru handienari spam bidaltzen saiatzen da.



Bestalde, Lolbot.Q berehalako mezularitzako programen bitartez banatzen da, hala nola MSN edo Yahoo! bidez, eta link gaizto bat biltzen duen mezu bat erakusten du. Lotura horrek “harra” deskargatzen du, eta horren funtzioa da Facebookeko kontua bahitzea eta erabiltzeari bertan sartzea eragoztea. Gizarte-sarean sartzen saiatzen bada, mezu bat agertzen zaio kontua eten egin dela esateko, eta berriz ere aktibatzeko inkesta bat bete behar duela, eta hainbat gadget irabazteko aukera eskaintzen dio, hala nola iPad bat edo ordenagailu eramangarri bat, bere parte-hartzea sustatzeko.

Zuri gerta dakizuke

Hainbat galderari erantzun ondoren, sakelako telefono-zenbaki bat eskatzen da. Zenbaki horretan datu-mezuak jasotzen dira, eta astean 8,52 euroko gastua suposatzen dute. Izen-emate hori efektiboa egitean, biktimak pasahitz bat jaso beharko luke sakelako telefonoan, Facebookeko kontua berreskuratzeko.

Posta elektronikoa da ziber-delitugileen iruzur egiteko edo birusak banatzeko ahaleginen protagonista nagusia, eta, beraz, oso garrantzitsua da arrisku horiek saihesteko modua ezagutzea:

- Pasahitza berreskuratzeko mekanismoa modu seguruan konfiguratzea. Bi mekanismo daude: kontu alternatiboa eta galdera sekretua.
- Postan bidegabe sartzeak saihestea, pasahitz seguruak erabiliz, batez ere ordenagailu publikoetan, eta ziurtatu prozesuan zehar orrialdearen helbidea “https” moduan hasten dela.
- HTML mugatzea, horrelako postetan errazagoa delako kode gaiztoak izatea.
- Antispam iragazkia erabiltzea. Iragazki horrek sarrera erretiluan mezu baztergarriak agertzea saihesten du.
- Kontuz erantsitako fitxategiekin. Bidaltzailea ezaguna bada ere, posta kutsatua egon daiteke. Exekutatu aurretik, antibirus eguneratu batekin aztertzea gomendatzen da.
- Mezu susmagarriak ezabatzea. Eta susmo txikiena baldin badago, bertan agertzen diren loturei ez jarraitzea.