NEWSLETTER 1

NORBERAREN GAILUEN SEGURTASUNA: ORDENAGAILUA, TABLETA ETA TELEFONO MUGIKORRA

Interneteko segurtasunaren gaia lau zatitan bana daiteke: gailuen eta etxeko sarearen babesa, pasahitzak, nabigatzaileak eta wifi sareetako nabigazioa.

Kategoria horietako bakoitzerako, gutxieneko segurtasun-maila bat lortzeko egin behar den guztia ikusiko dugu, webgunearen eta sarearen bidez transferitutako datu guztiak eta sistema erabat babestuta egon arte.

1) Ordenagailu, tableta edo telefono mugikorren segurtasuna

Antibirusik instalatuta al dago? Antibirusa automatikoki eguneratzen da egunero?

Oraindik birusen aurkako programarik instalatu ez baduzu edo eguneratzen ez den programa iraungi bat baduzu, neurriak hartu behar dituzu.

Desinstalatu zure egungo antibirusa eta deskargatu gomendatutako doako birusen aurkako programetako bat. Antibirus bat mundu guztiak ulertzeko moduan epaitzeko, gutxienez 6 parametro hartu behar ditugu kontuan edozein erabaki hartu aurretik. Izan ere, antibirus on bat:

- PCa ez da gehiegi mantsotu behar eta RAM memorian arina izan behar du.

- Birusak geldiarazi behar dituzu jardun ahal izan aurretik (eskaneatze aktibo egoiliarra).

- Ez du positibo faltsu gehiegi detektatu behar, mehatxurik ez dagoen lekuetan ikusiz.

- Eskaneatze automatikoak edo eskaneatze automatikoak ez du denbora gehiegi behar: SSD moderno bat 2 ordu baino gutxiagoan erabat eskaneatu behar da.

- Automatikoki eguneratu behar da, infekzio berriak berehala gelditu ahal izateko eta sistemaren bizi-zatietara iristea saihesteko.

- Aurkitu gabeko malwarea blokeatzeko gai izan behar du (0-day mehatxuak), eta zenbait osagairen portaera susmagarriak soilik detektatu behar du mehatxua.

Parametro horiez gain, horiek guztiak oso garrantzitsuak dira antibirusa denean, kontuan hartu behar dira, halaber, erabiltzeko erraztasuna, erabiltzaile-interfazea, erabilgarritasun-arazoak eta bugak, erroreak eta bateraezintasunak.

- Suebaki bat instalatuta al dago?

Windows 7 baduzu eta etxean router batekin Interneten nabigatzen baduzu, ez duzu suebaki-programarik behar. Behar izanez gero, doako suebaki bat deskarga dezakezu zure sarea babesteko eta intrusioak blokeatzeko.

-Windows (edo Mac) eguneratuta dago eta automatikoki eta erregulartasunez eguneratzen da?

Pertsona askok Windows eguneratzen dute Microsoftek astero banatzen dituen adabakiekin. Eguneratze horiek segurtasun-adabakiak dira beti, asmo txarreko erabiltzaileei PCetan kanpotik sartzea eta kontrola hartzea ahalbidetzen dieten azken zuloak estaltzen dituztenak.

Egiaztatu Windows Update zerbitzua aktibo dagoela Kontrol Panelean.

Mac-en erabiltzaileek ere ez dituzte gutxietsi behar segurtasun-eguneratzeak.

- Ezarri al duzu zure datu, dokumentu eta argazkietarako segurtasun-kopien planik?

Sortzen dituzun eta zure ordenagailuan gordetzen dituzun fitxategiak galtzen ez dituzula ziurtatzeko, planifikatu segurtasun-kopia automatiko bat segurtasun-kopia bikoitza izateko.

Segurtasun-kopia bat egiteko datu gehiegi ez baduzu, askoz errazagoa eta azkarragoa izan daiteke sareko segurtasun-kopia bat egitea hodeiko biltegiratze-zerbitzuetan, hala nola Dropbox eta Skydrive zerbitzuetan.

-Eguneratuta al dituzu ordenagailuan instalatutako programak?

Windowsen kasuan bezala, askotan programetarako segurtasun-eguneratzeak argitaratzen dira.

Nahi dutenentzat, ordenagailuan instalatutako programak eta softwarea automatikoki eguneratzeko moduak daude.

- Programak deskargatzen direnean, instalazio-prozeduran kontuz ibiltzen al da "gomendatutako" beste programa batzuk ere ez instalatzeko?

Zoritxarrez, doako programa askok babesleak dituzte, "Crapware" izenekoa, automatikoki instalatzen diren eskatu gabeko programak.

2) Nabigatzailearen segurtasuna

Ordenagailua, tableta edo telefono mugikorra birusen eta kanpoko intrusioen aurka babestuta egoteak ez du bermatzen nabigazioak segurua eta pribatua izaten jarraituko duenik. Beharbada jende askori ez zaio axola pribatutasuna, baina segurtasuna funtsezkoa da oraindik.

Erabiltzen duzun nabigatzailea edozein dela ere, azken bertsiora eguneratuta egon behar du eta eguneratze automatikoak aktibatuta. Eguneratze automatikoak dituzten nabigatzaileak, zalantzarik gabe, Chrome, Firefox, Opera eta Microsoft Edge dira**.**

- Pasahitz batekin gune batera konektatzen zarenean, beti egiaztatzen duzu helbidea https bidez hasten dela?

HTPPS konexio enkriptatuaren protokoloa da, eta http normaletik bereizten da https helarazitako edozein datu enkriptatuta dagoela. Horrek esan nahi du https-en idazten dena edonork irakur dezakeela, baita gune horretako operadoreek ere.

https Everywhere nabigatzailearen luzapenak gune seguruak nabarmentzen ditu eta eskuragarri dagoenean beti httpsn egongo dela ziurtatzen du (ikus artikulua https webgunean, banku-guneetan, online dendetan, Facebooken, konexio seguru batekin).

-Ba al dakizu begiz ezagutzen klikekin kontuz ibili behar den leku arriskutsuak?

Oraindik ezin baduzu leku on bat eta txarra begiz bereizi, eta beti paranoikoa edo gaizki hitz egiten baduzu ezagunena ez den beste edozein lekurekin, orduan WOT bezalako luzapen batzuk instalatu ditzakezu, esteka arriskutsuetan eta leku susmagarrietan klik ez egiteko.

- Zuk bakarrik erabiltzen ez duzun ordenagailu batetik leku batera konektatzen zarenean, beti ixten duzu saioa?

Gogoratu beti ordenagailu publiko batean edo beste pertsona batzuekin (familiako kideak barne) partekatutako ordenagailu batean erabiltzen dituzun kontu guztien saioa itxi behar duzula.

- Ezagutzen dituzu iruzurren oinarriak?

Interneteko phishing, malware eta beste arrisku batzuk zer diren eta horietatik urrun mantentzeko zer den garrantzitsua jakitea.

- Zure nabigatzailea linean arakatzetik babesten duzu?

Azaldu den bezala, webguneek linean ez arakatzeak datu-bilketa blokeatzea esan nahi du. Hori posible da zure nabigatzailean instalatu ditzakezun luzapen batzuen bidez.

Interneteko babes- eta pribatutasun-mailarik handiena nabigazio anonimoa da. Erabat anonimoa nabigatzea ez da mundu guztiarentzat baliagarria eta ezin da egoera guztietan egin. Erabilgarria izan daiteke legez kanpoko zerbait egiten ari zarenean (baina bueno, torrents deskargatzea bezala), zure kokapen geografikoa partekatu nahi ez duzunean edo zure IP helbidea faltsutu nahi duzunean blokeatutako guneetara sartzeko.

Interneten modu anonimoan hainbat modutan nabigatu dezakezun arren, online pribatutasuna TOR nabigatzailearekin soilik dago bermatuta.

3) Online erabiltzen diren pasahitzen segurtasuna

- Pasahitz zailak erabiltzen dituzu?

Internauten akatsik ohikoenetako bat pasahitz sinpleak edo beren bizitza pertsonaleko gertaera edo gertaerei erreferentzia egiten dietenak erabiltzea da. Deskubritu ezin diren pasahitzak aukeratu behar dira beti, eta, batez ere, webgune guztietarako pasahitz indartsu bat sortu behar da, inori asmatzeko aukerarik eman gabe (inoiz ez erabili zure jaiotze-data, zure talde gogokoena edo zure emaztearen edo txakurraren izena).

- Gauza bakoitzerako pasahitz bat erabiltzen duzu?

Inoiz ez da berrerabili behar posta elektronikoaren eta pasahitzaren konbinazio bera hainbat zerbitzutan; izan ere, pirata informatiko batek posta elektronikoko kontu horretan sartzea lortzen badu, kontu pertsonal guztiak urratu ahal izango ditu zailtasunik gabe.

Web kontuen pasahitzak sortzeko eta kudeatzeko programa bat erabiltzen du.

Ahal denean (Dropbox, Google, Gmail eta Facebook), bi faktoreren autentifikazioa erabil daiteke.

Babes handiagoa izateko, egiaztatu aplikazioen baimenak Facebooken eta Twitterren.

4) Sareetan segurtasuna

- Zure etxeko WiFi sarea WPA2 gako batekin babestuta dago?

Hala ez bada, edo WPA2 zer den ez badakizu, jakin behar duzu WPA Wi-Fi Protected Access siglak direla, eta Wi-Fi Protected Access II (WPA2) eta Wi-Fi Protected Access III (WPA3) Wi-Fi Alliancek sare informatikoak babesteko garatutako hiru segurtasun-protokolo eta ziurtapen-programak direla.

- Jabetzen zara Wi-Fi sare ireki batera konektatzen zarenean, egiten duzun guztia zure ordenagailutik kanpo ikusten dela?

Wifi sare publiko batean Interneteko pasahitzen segurtasuna babesten duen gauza bakarra bigarren puntuko lehen galderan aipatutako https protokoloa da.

- Egiaztatu dituzu zure ordenagailuko karpeta partekatuak?

Frogatu denez, ordenagailuak hackeatzea eta beste ordenagailu batzuetako karpetak partekatzea oso erraza da. Askotan, eragiketak arrakasta izaten du, jendeak ahaztu egiten baitu karpetak edo ordenagailuko disko gogor guztia bateratzea. Ordenagailu bat anonimotasun osoz erabiltzeko eta inolako arrastorik utzi gabe sarera konektatzeko, Linux sistema anonimo eta pribatu bat erabil daiteke, Tails izenekoa.

Segurtasuna garrantzitsua da guztiontzat, eskarmentu handiko teknikariarengandik hasi eta analfabeto informatikoraino. Hartzen duzun arreta-maila zure esku dago, baina kontuan izan gaur egun lineako segurtasuna zure etxeko segurtasuna bezain garrantzitsua dela (gehiago ez bada).

This project has been funded with support from the European Commission. This document reflects the views only of the project partners, and the Commission cannot be held responsible for any use which may be made of the information contained therein.