EDUKI DESEGOKIA n. 2

Zein dira ezagutu behar diren eta kontuz ibili behar diren Interneteko arriskuak?

Ezagutu behar diren, kontuz ibili behar diren eta beharrezkoa denean aurre egin behar zaien Interneteko arriskuak 9 kategoria handitan laburbil daitezke.

1) Bere ordenagailua infektatzeko prest dauden malwarea eta birusak dituzten guneak

Interneten nabigatzean, oso erraza da esteka okerrean klik egitea eta ordenagailuan malwarea kargatzen duen gune bat irekitzea. Zorionez, zure PCan antibirus eguneratu bat instalatuta baduzu, birus hori ia beti geldituko da kalteren bat eragin baino lehen. Birusak akats batengatik pasatzen uzten duen antibirusaz gain, arriskurik handiena da ez konturatzea bere ordenagailuaren funtzionamendua edo datuen osotasuna arriskuan jar lezakeen infekzio bat izateko arriskua izan duela. Hain zuzen ere, pertsona askoren arreta faltagatik, azken urtean Cryptlocker bezalako ransomware birusak zabaldu dira, artxibo pertsonalak zifratu eta erreskate bat eskatzen dutenak.

Badakigu zein gune diren arriskutsuak, normalean pirateriarekin, streaming guneekin, helduentzako edukiekin, hitzorduekin eta legez kanpoko materialarekin zerikusia dutenak. Ezin baduzu saihestu horrelako guneak bisitatzea, kontuz ibili non egiten duzun klik, birusa edozein lekutan ezkuta baitaiteke. Nahikoa da okerreko "deskarga" botoian klik egitea malware bat instalatzen amaitzeko. Eta ez ahaztu zure ordenagailua infektatuta dagoela esaten dizuten publizitate-banner horiek, benetan infektatuta ez dagoenean.

Zalantzarik izanez gero, esteka arriskutsuak eta gune susmagarriak ezagutzeko eta saihesteko tresnak daude. Birusak dituzten guneak ezagutzeko eta saihesteko funtsezko faktore bat nabigatzaile eguneratu eta babestu bat erabiltzea da, orain arte aurkitutako akats guztien aurka.

Malwarea izan dezaketen gunerik arriskutsuenen artean daude, zalantzarik gabe, helduentzako guneak, edozein motatako pirateria guneak, ia torrents gune guztiak (pirateriarekin ere bai), legez kanpoko deskargak (filmak eta musika) eta crack guneak.

Egokiena da, horrelako leku bat bisitatu behar baduzu, onena sandbox bat erabiliz nabigatzea izatea. Windows 10 eta Windows 11 sistemetan mahaigain birtualeko funtzio bat erabil daiteke. Segurtasun-tresna izateaz gain, ordenagailuan gauzak egiteko modu bikaina da, erregistratuta geratu gabe edo gogoan izan gabe, web nabigatzaileen modu ezezagun gisa. Tresna horrek Sandbox du izena, eta ordenagailuaren gune gisa pentsatuta dago. Bertan, egiten den guztiak ez du eraginik sisteman, eta itxi eta berehala ezabatzen da. SandBoxak erabili eta botatzeko makina birtual bat bezala funtzionatzen du, nahi den guztia segurtasunez exekutatu dezakeena; birus edo malware bat ireki daiteke PCa kaltetuko duen edo ekipoaren datuak lapurtuko dituen kezkatu gabe.

2) Online pribatutasuna beti arriskuan

Argi dago Internet modu parte-hartzailean erabili nahi baduzu, hau da, foroetan, sare sozialetan eta txatetan sartuta, pribatutasunaren zati bat sakrifikatu behar duzula. Facebook bezalako guneetan, benetako izena ematera behartuta dago; beste gune batzuetan, berriz, posta elektronikoko helbide bat utzi behar da, nahi izanez gero, jabea arakatzeko. Funtsean, Interneten erabilera normalean, anonimotasuna ezin da existitu, eta norbaitek nor garen jakiteko interesa balu eta hackeatzeko trebetasun eta talentu egokiak balitu, teorikoki dena jakin ahal izango luke guri buruz.

Lineako pribatutasuna babesteak, ordea, ez du esan nahi hacker batek gure bizitzak zelatatzea eragoztea, jazarle batek jazartzen ez bagaitu edo legez kanpokoak diren eta ezkutatu behar diren gauzak egiten ez baditugu, esan dezagun litekeena dela inork denbora galtzea gure bizitzak hackatzen. Lineako pribatutasunak, aldiz, informazio sentikor jakin bat pribatuan mantentzea esan nahi du, hala nola gure kreditu-txartelen zenbakiak, gure pasahitzak, une bakoitzean non gauden, Interneten zer bilatzen dugun, etab.

3) Segurtasun gabeko orrialdeak

Hau arrisku faktore bat da, jende gehienak ez ikusiarena egiten jarraitzen duena.

Webguneak ez dira denak berdinak eta gune seguruetan banatzen dira, non transmititzen den informazioa enkriptatuta dagoen eta kanpotik ezin den atzeman, eta argi transmititzen duten gune normaletan. Navigaweb.net enkriptatu gabeko gunea da gaur egun, baina horrek ez du esan nahi segurua ez denik, baizik eta sartzeko pasahitzik behar ez denez, ez duela informazioa babestu behar. Pasahitz bat sartu behar den gune guztiek enkriptatuta egon behar dute, eta Interneteko helbideko giltzarrapoak eta https aurrizkiak ezagut dezakete babes hori, http izan beharrean. Gune bat httpsn dagoenean eta ziurtagiri-akatsik ez duenean, orduan bidaltzen dugun informazio guztia, sarbide-pasahitzak, kreditu-txartelen edo banku-kontuen zenbakiak barne, ez da Interneten ikusten inorentzat, ezta informazio hori bidaltzen dugun guneko operadorearentzat ere. Zer esanik ez http eta https gabeko gune guztietan ez da informazio pertsonalik partekatu behar.

Oraindik erabiltzen ari bazara posta elektronikoko zerbitzu bat https gabe edo online banku zerbitzu bat hain azalekoa, erabat berehala aldatu.

4) Phishing

Leku arriskutsuen artean, oro har, kategoria berezi bat maula guneena da, hala nola, ezezagunak eta ez gomendatuak diren erosketa guneak edo, are okerrago, leku ospetsuen berdin-berdinak diruditen eta kontuetako pasahitzak lapurtzeko sortzen diren toki faltsuak.

Banku-guneen edo erosketa-guneen kopiak egitea da hackerrek web kontuetako pasahitzak lapurtzeko erabiltzen duten teknika ohikoenetako bat, eta Phishing du izena. Phishingak beti funtzionatzen du mezu bat bidaliz posta elektronikoz, Facebook, SMS, Whatsapp, etab. Teknika honetan ez erortzeko modurik onena pasahitzak lapurtzeko aitzakia gisa erabiltzea da. Horrelako tranpetan erortzea saihesteko modurik onena pasahitzak eta datu garrantzitsuak inoiz ez idaztea da (ezta posta elektronikoz ere), kontuen webgune ofizialetan izan ezik, horiek nabigatzailearen goiko aldean idatzitako helbideak eta giltzarrapo berdedun httpsak ezagut baititzakete.

Egokiena Microsoft Outlook bezalako posta elektronikoko bezero bat erabiltzea eta mezu horiek blokeatzeko spam iragazki bat erabiltzea litzateke.

5) Spam

Spamaren arriskua duela urte batzuk baino askoz txikiagoa da gaur egun.

Spama zabor mezu, publizitate, phishing eta birus edo alferrikako komunikazioen kategoria osoa izango litzateke. Zorionez, gaur egungo posta elektronikoko zerbitzu nagusiek, hala nola Gmailek eta Outlook.com-ek, spam iragazki eraginkor bat dute, posta elektronikoen harrera arautzen duena.

6) Informazio eza

Spam kategorian sar daitekeen arren, Interneteko desinformazioa benetako arrisku bihurtu da azken urtean, albiste faltsuak bulo-guneetatik zabaldu direlako, eta albiste horiek ezagutzen ikasi behar dugu, Interneten edo Facebooken irakurtzen duten edozer gauza sinistu ezin izateko.

7) Online bidezko hitzorduak

Hori da Interneteko arriskurik larrienetako bat gazteentzat.

Gaizki ematen du esatea, baina aita arduratsu batek egiaztatu behar du ea bere seme-alabek arrotzekin txiokatzen duten Internet bidez, zirkunstantziak edozein direla ere. Ezezagun batekin txateatu daiteke online joko batean, noizbehinkako hitzorduen gune batean, sare sozial batean, foro batean eta beste edozein txat-aretotan. Sexu-arrazoiengatik, hitzorduengatik edo jolas-arrazoi hutsengatik, garrantzitsua da informazio pertsonal gehiegi ez ematea: ez esan zure benetako adina, ez esan non bizi zaren, ez esan zein ikastetxetara zoazen, ez eman senideen edo lagunen benetako izenik eta ez eman zure telefono-zenbakirik. Online harrapariak oso onak dira mutil arrunten itxura hartzen, eta badakite nerabeen ahuleziak esplotatzen, psikologo onenek ere ez bezala, kasu larrienetan, pedofilia gaixotasun izugarri horrek eraginda.

8) Cyberbullying

Arrotzekin txateatzea arriskutsua izan daiteke, inoiz ez baita jakiten nor dagoen teklatuaren atzean, baina txateatzea edo pertsona ezagunekin mezuak bidaltzea ere arriskutsua izan daiteke. Ziberjazarpenak horrela funtzionatzen du, gutxi gorabehera: eskolan edo zure lagunei iseka egiten badizute, horietako batek bideo bat edo argazki bat argitaratu dezake Facebooken edo biktima lotsarazi dezakeen beste sare sozial batzuetan.

Ziberjazarpenaren beste kasu bat biktima asko iraintzen duten mezu anonimoetatik etor daiteke, baita mehatxuekin ere.

Benetako jazarpenarekin alderatuta, ziberjazarpenaren abantaila da ez dagoela kontrolik eta nahi duena esan dezakeela biktimari aurpegira begiratu gabe, edo are modu anonimoan, teklatuaren atzean ezkutatuta. Kasu batean zein bestean, ez litzateke hain zaila izango, maila teknikoan behintzat. Hala ere, askoz ere zailagoa da maila psikologikoan defendatzea, eta horrek aita edo aditu baten laguntza eska dezake.

Hasteko, ordea, aurrerapauso bikaina litzateke kontua Ask.fm-n ezabatzea, hau da, online ziberjazarpenari gehien eskaintzen zaion guneetako batean.

9) Segurtasun informatikoaren inguruko jakintza falta

Segurtasun informatikoaren erabateko ezjakintasuna

Arrisku nabarmena da, hain zabaldua, non harritu egiten baikara.

Posible al da gaur egun ere munduko pasahitzik ohikoena 123456 izatea?

Jendeak uste al du, ezkutatzeko ezer ez izateagatik, hacker batek ere ez duela bere kontua lapurtuko?

Nola liteke jendeak webgune guztietarako pasahitz bera erabiltzen jarraitzea?

Eta oraindik ba al dago bere pasahitzak, agian denak ezberdinak eta gogoratzeko zailak, edonork irakur dezakeen paper batean idazten dituenik?

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.