

ZIBERIRUZURREN SOFISTIKAZIOA

Adimen Artifizialarekin, erasoak eraldatzen ari dira: testu pertsonalizatuagoak idazten dira, identitatea ordezteko

Gabonetako ospakizunen etorrerarekin, erosketa fisikoak zein internet bidezkoak ikaragarri hazten dira. Deloitte egindako ikerketa baten arabera, iazko kanpainan egindako erosketen %25 Internet bidez egin ziren. Baina Adimen Artifizialaren alde ilunaren gorakadaren ondorioz, gero eta neurri gehiago hartu behar dira horrelako erosketak egiterako orduan.

«Adimen Artifizialak iraultza dakar arlo askotan, eta ziberiruzurren munduan ere eragina du, noski. Erasoa sofistikatuagoak dira, erasoak egiten dituztenek testu pertsonalizatuagoa idatz baitezakete, nortasuna ordezteko eta ingelesez *phishing* izenez ezagutzen dena egiteko, gaizkile berriak sartzea errazten duten hizkuntza berrietan birus gehiago sortzeko, dirua teknika berriein eskatzeko, hala nola hipertrukatzea (*deep fake* ingelesez) —teknika horiek irudiak, bideoklipak eta audioak konbinatzen, ordezen eta gainjartzen dituzte, benetakoak diruditen multimedia fitxategi faltsuak sortzeko—, edo beren eraso-estrategiak denbora errealean ahalik eta ondoen egokitzeke», ohartarazi du Laia Subirats Unibersitat Oberta de Catalunya (UOC) Informatika, Multimedia eta Telekomunikazio Ikasketetako irakasleak.

Zibersegurtasunaren munduan lan egiten duten espainiar Estatuko INCIBE bezalako institutuek oinarritzko aholku batzuk ematen dituzte erosterrako orduan, hala nola, posta

elektroniko, SMS edo WhatsApp bidez eskaintzen diren “sariekin” kontuz ibiltzea; erosi nahi den webgunearen informazioa bilatzea; ordaintzeko aukera seguru batzuk daudela egiaztatzea, edo banku-txartelen mugimenduen jarraipena egitea.

EAEn, Basque Cybersecurity Centre delakoa ipini dute martxan, Nafarroan ere Navarra Cybersecurity Center delakoa lehen urratsak egiten ari da. Eta nazioartean, National Cybersecurity Alliancek, adibidez, tresna erabilgarriak eskaintzen ditu, hala nola softwarearen eguneratze automatikoak aktibatzea edo wifi sare publiko batera konektatuta zaudenean erosketak egitea saihestea.

DATU ESKAERAK, QR KODEAK...

Erosketez gain, herritarrek ere erne egon behar dute, Adimen Artifizialarekin garatutako ziberiruzurren biktima ez izateko. Ildo horretan, Subiratsek gogorarazi du espainiar Estatuan dagoeneko badirela hala-koak jasan dituzten pertsonak: «Zibersegurtasuneko Institutu Nazionalak (INCIBE) ohartarazi zuen ziberdelitugileek Zerga Agentziaren itxura hartzen zutela, isunekin mehatxatzen zuen jakinarazpen bat bidaltzen zutela, kode maltzurra zuten artxiboak deskargatzera behartzen zutela eta erabiltzen ari zen gailua infektatzen zutela», gogoratu du irakasleak.

Badira beste kasu berriago batzuk ere: ziberdelitugileek X sareko (garai bateko Twitter) erabiltzaileek publikoki laguntza eskatzen dutela baliatu izan dute iruzur egiteko, edo

TEKNOLOGIA / GAUR8

Ikerketa desberdinek argi erakusten dute delitu informatikoen kopurua gora egiten ari dela nabarmen urtetik urtera. Eta Adimen Artifizialak zaildu egin dezake iruzurak detektatzeko lana. Internet bidezko erosketak ugarituko diren egunotan, komeni da gaur egungo joera nagusien azterketa bat egitea.

Gabon garaian asko ugarituko dira internet bidezko erosketak.
GETTY IMAGES

QR kodeak dituzten iruzurak antzeman dira tabernetan edo jatetxeetan (*qrishing* izenez ezagutzen dena). «Horregatik da hain garrantzitsua agentzia desberdinen zibersegurtasuneko joerak, albisteak eta gomendioak jarraitzea eta herritar guztiek jardunbide egokiak erabiltzea», azpimarratzen du Subiratsek.

Baina herritarrak ez dira erne egon behar duten bakarrak, adituak gogorarazi duenez, Adimen Artifizialarekin egindako zibereraso askoren jomugan erakundeak baitaude. Subiratsen arabera, kaltebertasunak detektatu ahal izateko, ziberiruzurak prebenitzeko eta detektatzeko politikak izan behar dituzte, hala nola baliabideen eta trafikoaren monitorizazioa, anomalien detekzioa, auditoriak egitea, softwarea maiz eguneratzea edo pirateatze etikoa sustatzea (*ethical hacking* ingelesez). «Zibererasoei aurre egiteko, paradoxikoki oso baliagarria da Adimen Artifizialaren azken teknikak erabiltzea», azaldu du espezialistak.

Espainiar Estatuan, aurreko urtean baino % 22,7 ziberdeli-



Adimen Artifizialak ziberiruzurren munduan ere eragina du. Erasoak sofistikatuagoak dira, testu pertsonalizatuagoak idatz daitezke, nortasuna ordezteko adibidez

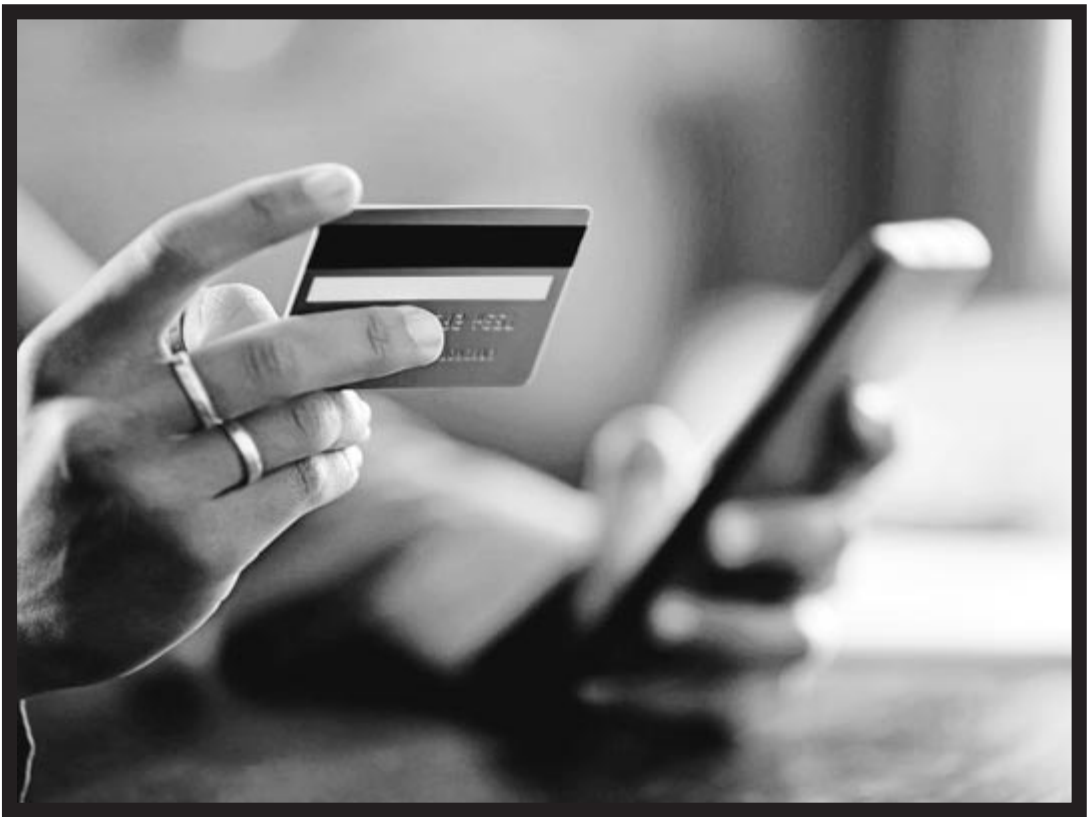
Espainiar Estatuan aurreko urtean baino % 22,7 ziberdelitu gehiago izan dira 2022an, eta ia 375.000 delitu informatiko izan dira, barne ministerioaren txostenaren arabera

tu gehiago izan dira, eta ia 375.000 delitu informatiko izan dira. Halaxe dio barne ministerio espainolak 2022ko “ziberkriminalitateari” buruz egindako txostenak. Eta ikerketak argi erakusten du joera goranzkoa dela nabarmen: 2018an 160.729 izan ziren, 2019an 218.302, 2020an 287.963, 2021ean 305.477 eta 2022an 374.737.

«Erasoen bolumen horrekin, ezinbestekoa da enpresek zibersegurtasunean adituak diren profesionalengan inbertitzea beren burua babesteko, eta langile guztiak trebatzea erakundean segurtasun-kultura ona har dezaten», ohartarazi du UOC-eko irakasleak.

Gainera, eta pentsa litekeenaren kontra, ziberdelituen biktimak ez dira adineko pertsonak soilik izaten, aipatutako txostenaren arabera. Datuak tentuz hartu behar diren arren, salaketa ipini zuten pertsonen kopuru handiena 26-40 urte artekoa zen (81.832). 51-65 adin tartean kopurua 72.520koa izan zen –egia da seguruena erabiltzaile kopurua txikiagoa izan litekeela tarte horretan–.

Ildo horretan, Subiratsek gogorarazi du 2022ko irailean European Union Agency for Cybersecurity (ENISA) erakundeak enpresek izan beharko luketen zibersegurtasun-profilen zerrenda bat argitaratu zuela. Enpresa txiki eta ertainen kasuan, PIMEC patronalak protokolo, zerbitzu, aseguru eta zibersegurtasuneko tresnei buruzko gomendioak ere ematen ditu. «Funtsezkoa da erregulazioaldaketekin eguneratuta egotea, bereziki kritikotzat jotzen diren sektoreetako erakundeak, osasun-sektorea adibidez», amaitu du irakasleak.



Datu finantzarioak webgune fidagarrietan bakarrik sartu behar dira. GETTY IMAGES

INTERNET BIDEZ EROSKETAK EGITERAKOAN GOGORATU BEHAR DIREN BOST GOMENDIO

Gabon garaia datorrenez eta internet bidezko erosketak ugartu egingo direla jakinda, komeni da INCIBE institutuak plazaratzen dituen bost gomendio nagusiak kontuan hartzea.

Lehenik eta behin, kontuz ibili posta elektronikoko, SMS, mezularitza-aplikazio (Telegram edo WhatsApp) edo sare sozial (Instagram edo X) bidez jasotzen diren kupoiekin, zozketekin eta Gabonetako sariekin. Egun hauetan, iruzurra diren mezuak ugartzen dira, erabiltzaileak ustezko zozketa, sari eta abarretan parte hartzera gonbidatuz. Zibergaizkileek erabiltzaileen datu pertsonalak eta finantzarioak lortzeko erabiltzen duten teknika besterik ez da.

Bigarrenik, datu pertsonalak eta bankuko datuak eman aurretik, egiaztatu datuak sartzeko ataria beti protokolo seguru baten bidez zifratuta dagoela. Fidagarriak diren dende segurtasuna eskainiko dute beti HTTPS protokoloa erabiliz egiten diren transakzioetan. Hala ez bada, baztertu webgune horretan erostea eta bilatu beste aukera bat.

Hirugarren gomendioa: informa zaitez apur bat erosketak egin behar duzun webguneari eta saltzen duen konpainiari

buruz. Bilatu oinarritzko informazioa, helbide fisikorik baduen, telefonoa, arduradunak, IFZa eta, beharrezkoa bada, deitu enpresari egiazkotasuna egiaztatzeko.

Laugarrena: ziurtatu online dendaren barruan ordaintzeko hainbat metodo daudela. Adituek beti gomendatzen dute ordainketa metodo seguruak erabiltzea, hala nola Visa, MasterCard, Apple Pay edo PayPal, gaur egun ospe ona duten webguneetan horrelako transakzioak egiteko eskaintzen ari diren bide nagusiak. Beste aukera on bat aurreordainketako txartelak edo diru-zorro birtualak erabiltzea da, bankuek bezeroei eskaintzen dizkietenak.

Eta azkenik, gogoratu txartelaren mugimenduen jarraipena egin behar dela. Interneten erosketak asko edo gutxi egin, egiaztatu egin dituzun mugimendu guztiak zuzenak direla eta ez dagoela ezer arrarorik. Halakorik balego, galdetu nondik datozen, eta identifikatzen ez baduzu, hitz egin zure banketxearekin, garaiz egin daitezkeen iruzurrak identifikatzeko.

Azken batean, zentzuz jokatzeko eskatzen dena, eta ez erosketen kasuan bakarrik. Beharrezkoa ez den daturik ez ematea eta fidagarriak ez diren loturak ez klikatzeko, horra hor bi gako nagusiak.