



2026KO IRAILA

Enfoka-Trends

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

"Bankuaren" dei bat, mezularitzako SMS bat edo ustezko legezko betebeharraren bat kobrantza bat, iruzurgileek ez dituzte multinazional bat eta saltoki txiki bat bereizten.

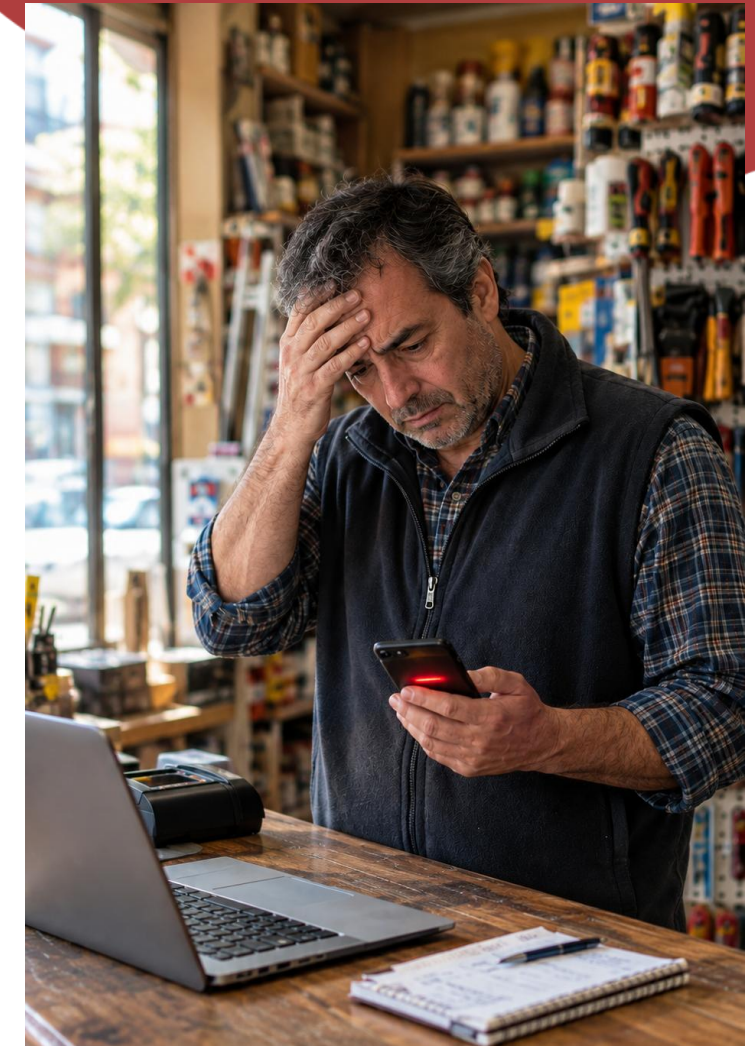
Zergatik da zure negozioa helburu erakargarria?

Zure denda ia bakarrik eramaten baduzu, erabakia, sinadura eta ordainketa pertsona beraren esku egongo dira. Ez dago zalantzarik duen administrazio-sailik, ezta posta berrikusten duen informatikako langilerik ere. Gainera, deiak hartzen ditu bidaltzen dituen bitartean, mugikorra aztertzen du bezeroen bisiten artean eta fakturak ordaintzen ditu presaka. Gaizkileek badakite hori, eta kanpaina masibo eta automatizatuak egiten dituzte, norbaitek noiz edo noiz despisteren bat noiz izango zain.

Online iruzurrak arraste-arrantza gisa funtzionatzen du. Milaka mezu bidaltzen dira, ia berdinak, eta nahikoa da batzuek aurrera egitea. Horrek bereziki kolpatzen ditu Langile Autonomoen Araubide Bereziaren (LAAB) eta ETEen mendeko pertsonak, segurtasun-neurri gutxiago dituztelako eta klik bakar batek jarduera geldiarazi edo ordainketak desbideratu ditzakeelako.

Nola aurreratu?

Prebentzioa ohitura bat da. Hilean hamar minutu eman kontuaren mugimenduak, bankuko abisuak eta profilak bere izenarekin aztertzen. Kontsulta itzazu INCIBEn (Zibersegurtasun Institutu Nazionala) abisuak, iruzurrek mozerroa aldatzen baitute hilero. Eta ados egon zaitez negozioan laguntzen dizunarekin, izan enplegatua edo senidea, ez dela ez ordainketarik ez koderik ematen egiaztapenik gabe.



Adimen artifizialarekin sortutako irudia

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

ENFOKA-TRENDS 2026ko IRAILA

Ezagutu behar dituzun bost iruzurrak

1. «Bankukoa naiz»: telefono bidezko ordezkapena

Nola funtzionatzen duen. Norbaitek deitzen dio esanez bere bankukoa dela eta mugimendu susmagarri bat dagoela eta «bertan behera utzi» behar dela. Pantailan agertzen den zenbakia aldatzen duen teknika da *spoofing*, bankuarena dirudiena. Are gehiago, zenbakia webgune ofizialaren zenbakiarekin bat datorrela egiaztatzeke eska diezaioke.

Adibidea. Ile-apaindegi batek «segurtasun-sailaren» dei bat jasotzen du, eta SMS bidez jasotako kode bat berresteko eskatzen dio, «transferentzia bat blokeatzeko». Kode hori, egia esan, zure kontua husteko baimena da.

Alerta-seinaleak. Gaizkileek bankuko langileen itxura hartzen dute pasahitzak, sarbide-kodeak edo kontu-zenbakiak eskatzeko. Urgentzia ere aplikatzen dute, pentsatzeko astirik izan ez dezan.

Ondorioak. Negozioaren kontuko eta, batzuetan, langileen kontuko dirua galtzea.

2. Posta, SMS eta WhatsApp bidezko phishinga

Nola funtzionatzen duen. Phishing-a mezu faltsu bat da, banku bat, Administrazioa edo beste enpresa bat imitatzen duena esteka bat sakatzeko edo gakoak emateko. SMS bidez smishing deitzen da.

Adibidea. Gizarte Segurantzaren Diruzaintza Nagusiak SMS faltsu baten berri eman zien autonomoei, zergak itzuliko zituztela agindu baitzien. Iruzur-seinale bat zen itzulketak Zerga Agentziari dagozkiola, ez Diruzaintzari. Negozioetarako oso kaltegarria den aldaera bat faktura batean kontua aldatzea da. Erasotzaileak enpresa hornitzaile baten fakturaren kontu-zenbakia aldatzen du ordainketa desbideratzeko.

Alerta-seinaleak. Webgune ofizialarekin bat ez datozen estekak, agur generikoak, gakoak edo kodeak eskatzea, eta berehalako edo ezohiko ordainketak.

Ondorioak. Kredentzialak lapurtzea, ordainketa desbideratuak egitea eta zure posta edo bankura sartzea.



Adimen artifizialarekin sortutako irudia

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

ENFOKA-TRENDS 2026ko IRAILA

3. Webgune faltsuak eta denda faltsuak sare sozialetan

Nola funtzionatzen duen. Arazoaren bi alde daude. Lehenengoa sareetan iragartzen diren denda faltsuena da. Bigarrena bere negozioa ordezkatzeko da. Sare sozialetan, gaizkileek enpresaren ia profil bera sortzen dute, eta izenak ez du aldaketa handirik, enpresaren itxura egiteko. Profil horrekin, jarraitzaileak engaina ditzakete, beren izenpean egindako iruzur batean eror daitezten. Tokiko denda txiki gisa aurkezten diren denda faltsuak salatu ditu.

Adibidea. Loradenda batek bere logoa duen klon profil batek zozketa bat iragartzen duela ikusiko du, eta bezeroei «bidalketa-gastuak» eskatuko dizkie.

Alerta-seinaleak. Bezeroek hasi ez dituzun marketin-ekintzei buruz galdetzen dizute, edo zure izenean argitalpen gutxi dituzten kontuak agertzen dira sare sozialetan.

Ondorioak. Zure izen onari egindako kaltea, zuri eskatzen dizuten bezero iruzurtiak eta konfiantza galtzea.

4. Euskarri-teknikari faltsuak

Nola funtzionatzen duen Deitu egiten dizute edo pantailan abisu bat agertzen zaizu zure ordenagailua infektatuta dagoela esanez. Beren burua eskaintzen dute konpontzeko, eta gakoak edo urruneko kontrol-tresna bat instalatzeko eskatzen diote. Horrekin ekipoa bahitu, datuak lapurtu edo transakzioak egin ditzakete.

Adibidea. Saltoki bati blokeo-abisu bat agertuko zaio bere STaren pantailan, birusak infektatzeagatik, eta jakinaraziko zaio salmentak kudeatzeko softwarearen «euskarri informatikotik» dei bat jasoko duela, urruneko sarbide-programa bat instalatzeko eskatuko diote, eta, minutu batzuk geroago, kurtsoa online bankako profilagatik bakarrik mugituko da.

Alerta-seinaleak. Zuk eskatu ez duzun dei bat, kontakturako telefonoa duen birusaren abisua eta zerbait instalatzen tematzea.

Ondorioak. Dirua, esposizioan dauden bezeroen datuak eta blokeatutako ekipook galtzea.



Adimen artifizialarekin sortutako irudia

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

ENFOKA-TRENDS 2026ko IRAILA

5. Legezko betebeharrak edo kuota faltsuak

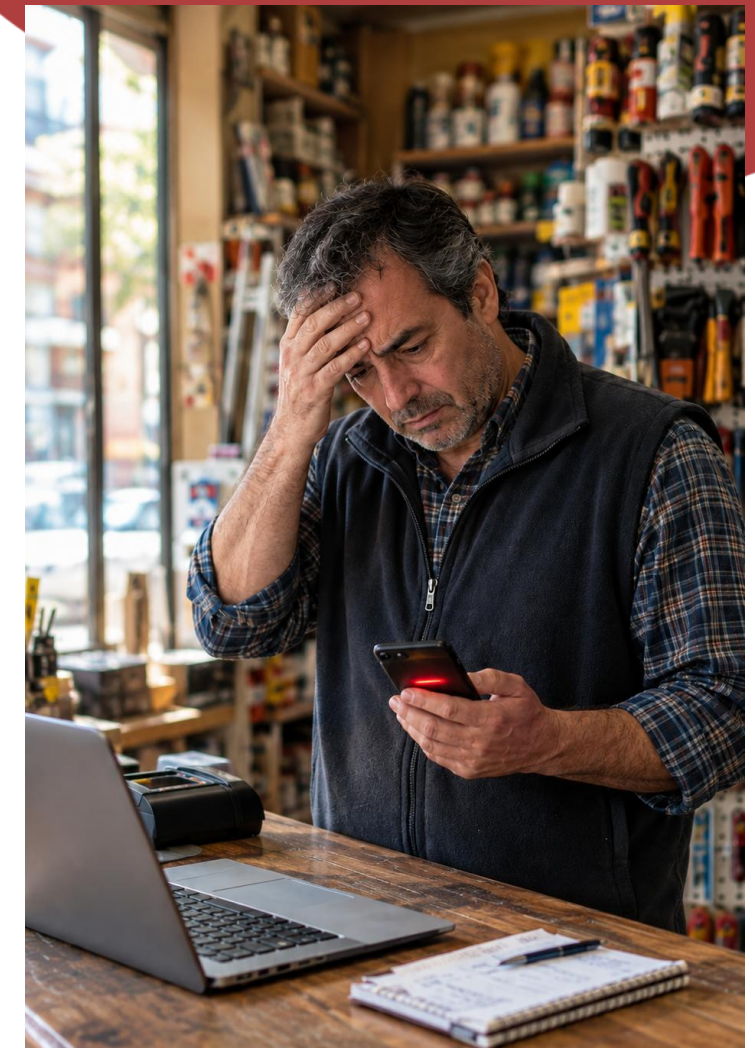
Nola funtzionatzeko duen. Erakunde ofizialtzat jotzen dira, hala nola Ogasuna, Gizarte Segurantzak edo erregistroak, eta «nahitaezko» ordainketa edo izapide bat eskatzen diote.

Adibidea. Denda irekita dagoela, SMS bat iritsiko zaizu, egiteke dagoen eguneratze bati buruz hitz egiteko, eta esteka bat sakatzera gonbidatuko zaitu. Estekaren domeinuak «atari», «seg» edo «sozial» hitzak barne hartzen ditu, itxura ofiziala emateko, eta orriak Diruzaintzako atariaren irudia erreproduzitzen du. Bertan, espedientearen ustezko erreferentzia bat eta «kuoten erregularizazioaren» kontzeptu bat agertzen dira, eta 38,74 euro erreklamatzeko zaizkio. Autonomoen eta Ekintzailearen arabera, kotizazioak doitzeko bezain sinesgarria da kopuru txiki bat, eta ez du egiaztatzerik gonbidatzen. Estekak ordainketa-pasabide faltsu batera darama, Importass aplikazioa imitatzen duena, eta bertan zure txartelaren datuak eskatzen dizkizute.

Alerta-seinaleak. Abisu faltsuek ortografia-akatsak, gaizki eraikitako esaldiak eta azkar jarduteko oso epe laburrak izaten dituzte. Gizarte Segurantzak ez du zorrak ordaintzeko eskatzen, ezta SMS bidez bidalitako esteken bidez datu pertsonalak eguneratzeko ere.

Ondorioak. Zure txartelaren datuak sartzen badituzu, baimendu ez dituzun karguak izan ditzakezu, eta datu horiekin iruzur egiteko beste saiakera batzuk jasan ditzakezu. Txartela eman baduzu, ez itxaron kargu bat agertu arte. Blokeatu berehala, zure bankura deitu eta frogak gorde salaketa jartzeko. INCIBEn 017 telefonora ere eska dezakezu laguntza.

Eragina izanez gero, hainbat egoera gerta daitezke: dirua zuzenean edo faktura faltsu baten bidez gal dezake. Gainera, erreklamatzeko eta salatzeke denbora behar da, eta hori ere kostatzen da. Zure ordenagailura, postara edo agendara sartuz gero, baliteke datu pertsonalen arrakala gertatu izana. Araudiak 72 orduko epea ezartzen du DBEAr jakinarazteko, horren berri izaten denetik zenbatzen hasita. Zure bezeroei iruzur egin diezaiekete zure izenean, eta zure deiak spam gisa markatu daitezke.



Adimen artifizialarekin sortutako irudia

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

ENFOKA-TRENDS 2026ko IRAILA

Zer diote datuek?

- **Zibersegurtasun-intzidenteak (INCIBE, 2025).** INCIBEn CERTek 122.223 gertakari kudeatu zituen 2025ean, 2024an baino % 26 gehiago. Online iruzurrak 45.445 kasu izan zituen, aurreko urtean baino % 19 gehiago, eta phishing-a izan zen teknikarik ohikoena, 25.133 kasurekin.
- **Eragindako enpresak.** Aurkitu dugun azken banakatze ofiziala 2024koa da: enpresei 31.540 gertakari egotzi zitzaizkien, guztizkoaren % 32,4. Kategoria horretan ETEak eta Langile Autonomoen Araubide Bereziko pertsonak sartzen dira.
- **Salatutako delituak (Barne Ministerioa, 2025).** 488.426 ziberdelitu erregistratu ziren, 2024an baino % 5,1 gehiago, hau da, kriminalitate osoaren % 19,8. Hamarretik ia bederatzi iruzur informatikoak izan ziren (429.677), eta % 4 gehitu ziren. Zifra horietan partikularrak eta enpresak sartzen dira.
- **Espainiako ETEen jabeak (Mastercard, 2024-2025eko inkesta).** % 23k bere negozioan iruzur baten biktima izan zela adierazi zuen, % 13k dirua galdu zuen eta % 7k bezeroak galdu zituen. Gainera, % 29k uste dute itxi egin beharko luketela zibereraso bat jasango balu.
- **Zibererasoak ETEei (Hiscox, 2025).** Txosten horren arabera, Espainiako enpresa txiki eta ertainen ia % 60k gutxienez zibereraso bat jasan zuen aurreko hamabi hilabeteetan.
- **Txikizkako merkataritza.** Check Point Software-ren arabera, % 178 igo dira ransomware-intzidentziak eta datu-filtrazioak Espainiako txikizkako merkataritzan 2024an. Txosten honetako iruzurrak ez bezalako eraso mota bat da, baina presioa norantz doan adierazten du.

Zenbaki ofizialek salatzen edo jakinarazten dena baino ez dute islatzen. Arrazoizkoa da errealitatea are handiagoa dela pentsatzea.



Adimen artifizialarekin sortutako irudia

Iruzur digitalak: nola ezagutu, babestu eta garaiz jokatu

ENFOKA-TRENDS 2026ko IRAILA

Nola babestu: neurri errazak eta merkeak

1. **Zintzilikatzeko eta deitzeko urrezko erregela.** Zure bankuaren edo teknikarien dei baten aurrean, eseki eta deitu zure txartelaren edo webgunearen telefono ofizialera. INCIBEk susmagarria iruditzen zaion dei oro beste bide batetik kontrastatzea gomendatzen du.
2. **Ez eman inoiz koderik edo gakorik,** ez telefonoz, ez mezuz. Zure bankuak ez dizkizu eskatuko.
3. **Postan, bankan, sareetan eta webgunean bi urratsetan egiaztatzea.** Defentsarik eraginkorrenetako bat da.
4. **Zerbitzu bakoitzerako pasahitz desberdinak,** pasahitzen kudeatzaile batekin, eroso bazeaz.
5. **Ez instalatu urruneko sarbideko programarik** pertsona ezezagunek eskatuta.
6. **Egiaztatu enpresa hornitzaileen kontu aldaketak lehendik duzun** telefono batera deituta, ez fakturara deituta.
7. **Alertak eta mugak bankuan,** eta kontu bereizi bat negoziarako.
8. **Fitxategien segurtasun-kopiak,** ordenagailutik kanpo gordeta.
9. **Zaindu zure marka,** bilatu zure izena sareetan noizean behin eta jakinarazi bezeroei zein diren zure profil ofizialak.

Inor ez dago despiste batetik salbu, baina ia iruzur horiek guztiek patroia bat partekatzen dute: premia, kode edo gako bat eskatzen dizute, eta espero ez zenuen dei edo mezu bat. Gelditzen, zintzilikatzen eta beste kanal batetik egiaztatzen ikasten badu, gehienak balaztatuko ditu.

Aste honetan ordu erdi eman egiaztapena aktibatzen bi urratsetan, zure bankuko alertak aztertzen eta 017 telefonoa zure mugikorrean gordetzen, doako linea konfidentziala da, egunero 8:00etatik 23:00etara enpresak eta profesionalak artatzen dituzte.



Adimen artifizialarekin sortutako irudia

Bibliografia

- **Carlos Olivera (LinkedIn, 2026)** *Las estafas digitales más comunes de este año.* 2026ko irailaren 28an hemendik eskuratua <https://www.linkedin.com/pulse/las-estafas-digitales-m%C3%A1s-comunes-de-este-a%C3%B1o-olivera-villanueva-cybre/>
- **INCIBE (2026)** *INCIBE detectó más de 122.000 incidentes de ciberseguridad en 2025.* 2026ko irailaren 28an hemendik eskuratua <https://www.incibe.es/incibe/sala-de-prensa/incibe-detecto-mas-de-122000-incidentes-de-ciberseguridad-en-2025>
- **itUser (2026)** *Los ciberataques en serie golpean a autónomos y pymes.* 2026ko irailaren 28an hemendik eskuratua <https://tecnologiaparatuempresa.ituser.es/seguridad/2026/03/los-ciberataques-en-serie-golpean-a-autonomos-y-pymes>
- **Lucía Fernandez (Libre Mercado, 2026)** *Las tiendas falsas se disparan: así operan las estafas que engañan a miles de usuarios en TikTok, Instagram y Facebook.* 2026ko irailaren 28an hemendik eskuratua <https://www.libertaddigital.com/libremercado/2026-04-14/las-tiendas-falsas-se-disparan-asi-operan-las-estafas-que-enganan-a-miles-de-usuarios-en-tiktok-instagram-y-facebook-7387416>
- **Guijarro Pique Asociados (2026)** *¿Qué puedo hacer si he sido víctima de phishing o una estafa bancaria?* 2026ko irailaren 28an hemendik eskuratua <https://www.guijarropique.com/phising-estafa-banco>
- **Sol Galindo (Autónomos y emprendedores 2025)** *Los ciberataques contra los pequeños comercios se triplicaron en 2024: el 28% accedió a pagar un rescate.* 2026ko irailaren 28an hemendik eskuratua <https://www.autonomosyemprendedor.es/articulo/todo-digital/ciberataques-pequenos-comercios-triplicaron-2024-28-accedio-pagar-rescate/20250220132209041096.html>