AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Rekomandime Për Sigurinë Në Internet

per shitje dhe blerje online (Qytetaret dhe Bizneset)

31/03/2020

Autoriteti Kombetar per Certifikim Eletrokin dhe Sigurine Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Hyrje

Këshilla për sigurinë në internet kur bleni dhe shisni në internet:

Përhapja e Covid-19 ka çuar në një rritje të tregtisë elektronike ndërsa njerëzit kerkojne në internet për të blerë ndonjë gjë nga librat në sende ushqimore. Një anë pozitive për këtë është rritja e transformimit dixhital, veçanërisht e bizneseve të vogla, të cilët duhet të kenë praninë e internetit për të mbijetuar.
SME-të (small and medium-size enterprise business), bizneset e vogla dhe të mesme përbëjnë 99% të bizneseve evropiane dhe ndërsa 77% e SME-ve kanë një faqe në internet, vetëm 17% janë duke shitur në internet (Indeksi i Ekonomisë Dixhitale dhe Shoqërisë (DESI) 2019). Në të njëjtën kohë, 41% e evropianëve janë të shqetësuar për sigurinë e pagesave në internet (qëndrimet e Eurobarometer evropianët ndaj sigurisë kibernetike - Janar 2020).

SME-të krijojnë biznes online, sepse mbijetesa e tyre varet nga kjo. Qytetarët blejnë në internet sepse duan të mbrojnë sigurinë e tyre. Si NVM ashtu edhe konsumatori po kërkojnë të përmbushin shpejt nevojat e tyre. Ata shpesh nuk duan të zbatojnë zgjidhje të gjata të sigurisë në internet dhe për të ndihmuar, Agjensia e BE-së për Siguria e Kibernetikës ka zhvilluar 10 këshilla për NVM-të dhe qytetarët për të qëndruar të sigurt kur blejnë dhe shesin në internet.

Rekomandime për blerje online nga qytetarët dhe bizneset

Rekomandime për qytetarët (blerje online)

- **Lidhje e sigurt**: Kushtojini vëmendje vulës së sigurisë së secilës faqe në internet që po kërkoni duke kërkuar praninë e kutisë së vogël jeshile në shiritin e adresave. Kjo do të thotë në përgjithësi që lidhja juaj të vendoset mbi një kanal të sigurt.
- **Shikoni për emailet e phishing të Covid-19 dhe faqet e internetit të rreme**: ka pasur një rritje në regjistrimin e domeIneve, të cilat përmbajnë fjalën "Corona", e cila përdoret nga kriminelët në internet për të ofruar mashtrime. Jini dyshues për ndonjë e-mail që kërkoni të kontrolloni ose rinovoni kredencialet edhe nëse duket se vjen nga një burim i besueshëm. Në të gjitha rastet, përpiquni të verifikoni vërtetësinë e kërkesës përmes mjeteve të tjera, mos klikoni në lidhje të dyshimta ose të hapni ndonjë bashkëngjitje të dyshimtë. Kujdes që postat elektronike që pretendojnë të jenë një faturë për një blerje që në fakt nuk ishte bërë.
- **Mashtrimi i pagesave**: Kontrolloni rregullisht llogaritë tuaja në internet dhe deklaratat tuaja bankare dhe raportoni çdo aktivitet të dyshimtë në bankën tuaj. Nëse mendoni se keni qenë viktimë e një sulmi, kontaktoni bankën tuaj. Nëse është e mundur, aktivizoni vërtetimin me dy faktorë sigurie (double Auth) për pagesa.

- **Sistemet të jenë azhurnuara** - sigurohuni që sistemi juaj (sistemi operativ dhe aplikacionet e përdorura) të jenë të azhurnuar, si dhe të siguroheni që antivirusi dhe antimalware juaj janë instaluar dhe azhurnuar plotësisht.

- **Mbroni privatësinë tuaj** - Mendoni dy herë kur kërkohen të dhëna dhe lexoni politikat e privatësisë. Nëse keni nevojë të krijoni një llogari me një furnizues, përdorni fjalëkalime të vështira që nuk mund të parashikohen lehtësisht dhe përdorni një menaxhim të fjalëkalimeve. Shmangni ndarjen e informacionit personal me persona që nuk i njihni në mediat sociale. Konsideroni të përdorni tools-sa private, të tilla si mjete për përcjelljen dhe mesazheve të sigurta, për mbrojtjen tuaj në internet dhe celular.

Rekomandime biznesin (shitja online)

- S**iguroni faqen tuaj te internetit për klientët**: - është thelbësore që ju të keni sigurinë e duhur për të mbrojtur ndërmarrjen tuaj, por edhe klientët tuaj, për shembull përdorni lidhjet ***https*** dhe mundësoni vërtetimin e 2 faktorëve të autorizimit kur është e mundur. Për më tepër është e rëndësishme të testoni sigurinë e faqes në internet dhe të siguroni mbështetje adekuate për klientët në rast problemi.
- **Mbroni asetet tuaja**: Ashtu si çdo aset tjetër i biznesit, informacioni duhet të menaxhohet dhe mbrohet strategjikisht. Siguria e informacionit është mbrojtja e informacionit brenda një biznesi, përfshirë sistemet dhe pajisjet e përdorura për të ruajtur, përpunuar dhe transmetuar këtë informacion. Sigurohuni që të jetë krijuar një politikë sigurie, së bashku me të gjitha masat e nevojshme teknike dhe organizative të sigurisë.
- **Ruani fjalëkalimet me siguri**: Nëse klientët duhet të krijojnë llogari për të blerë nga faqja juaj e internetit, atëherë sigurohuni që të gjitha fjalëkalimet të ruhen në mënyrë të sigurt. Sigurohuni që të dhënat e klientit tuaj të mbrohen sipas rregullave të industrisë. Kur është e mundur, sigurohuni që të dhënat e ndjeshme të mos jenë të lexueshme, zgjidhje të tilla si Salted HASH mund të zbatohen.

- **Siguroni respektimin e kërkesave për mbrojtjen e të dhënave**: Kur përpunoni të dhënat personale të klientëve, sigurohuni që të respektoni kornizën ligjore për mbrojtjen e të dhënave.
- **Monitoroni dhe parandaloni incidentet** - Bëni një politikë të reagimit ndaj incidenteve të sigurisë dhe sigurohuni që të merren masa për parandalimin, monitorimin dhe reagimin ndaj incidenteve të sigurisë, përfshirë shkeljet e të dhënave personale.

Link

a) https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online/