SMART Balkans

Civil Society for Shared Society in the Western Balkans

INSTITUTI LIBERAL PASHKO

Forcimi i Privatësisë dhe Sigurisë së të dhënave për nxënësit dhe të rinjtë në Baldushk

EPOKA DIGJITALE

Jetojmë në një kohë ku gjithçka ndodh online! Nga shkolla, tek argëtimi, komunikimi me miqtë apo ndjekja e lajmeve – gjithçka kalon përmes ekranit. Teknologjia është bërë pjesë e përditshmërisë sonë, që nga momenti kur zgjohemi dhe kontrollojmë telefonin, deri në orën e fundit kur shkëmbejmë mesazhe me miqtë.

A mund ta imagjinoni një ditë pa telefon, pa internet apo pa rrjete sociale? E vështirë, apo jo? Interneti dhe rrjetet sociale kanë ndryshuar mënyrën si mësojmë, si lidhemi me të tjerët dhe si shprehim veten. Me një klikim, mund të ndodhesh në çdo cep të globit.

Por, bashkë me mundësitë e pafundme që sjell teknologjia, vijnë edhe sfida të reja: ruajtja e privatësisë, sigurimi i informacionit personal dhe mbrojtja nga rreziqet online. Prandaj, është e rëndësishme të mësojmë si të përdorim internetin me zgjuarsi, me përgjegjësi dhe me vetëdije. Vetëm kështu, bota digjitale mund të mbetet një hapësirë e sigurt dhe pozitive për të gjithë.

ÇFARË ËSHTË PRIVATËSIA DHE SIGURIA E TË DHËNAVE?

A e keni menduar ndonjëherë kush mund të shohë mesazhet, fotot apo informacionin tuaj personal online?

Privatësia dhe siguria e të dhënave do të thotë të mbrojmë informacionin tonë personal kur përdorim internetin. Kjo përfshin gjërat si mesazhet, fotot, fjalëkalimet dhe informacionet që nuk duam t'i shohin të tjerët.

Në epokën digjitale, është e rëndësishme të mos lejojmë që dikush të përdorë informacionin tonë pa leje, të na mashtrojë apo të manipulojë atë që ndajnë të tjerët për ne. Kur e dimë si të kujdesemi për të dhënat tona, mund të përdorim internetin në mënyrë të sigurt dhe të shijojmë teknologjinë pa frikë.

FËMIJËT DHE TË RINJTË

- Të rinjtë janë një nga grupet më të ekspozuara në internet. Shpesh ata ndajnë informacione pa menduar për pasojat, duke u bërë viktima të keqpërdorimit të të dhënave, profilizimit të pashmangshëm nga platformat digjitale dhe sulmeve kibernetike, si cyberbullying dhe mashtrimet online. Mungesa e edukimit mbi privatësinë mund t'i vërë ata në rrezik të identitetit të vjedhur ose të manipulimit psikologjik.

PERSONAT E MOSHUAR

- Personat e moshuar shpesh nuk kanë edukim teknologjik të mjaftueshëm për të kuptuar mekanizmat e privatësisë dhe sigurisë së të dhënave. Ata mund të bien viktima të mashtrimeve financiare, keqpërdorimit të informacionit të tyre mjekësor dhe sulmeve kibernetik, duke humbur aksesin në financat e tyre ose duke u manipuluar nga individë të pandërgjegjshëm.

SULMET KIBERNETIKE: PHISHING, MALWARE, HACKING

🎣 **Phishing**

- **Çfarë është:** Kur dikush të dërgon një email ose mesazh që duket i vërtetë (nga banka, nga një lojë, apo nga një shok), por në të vërtetë është i rremë. Ata duan që ti të japësh fjalëkalimin, numrin e kartës apo informacione të tjera private.
- **Shembull:** Merr një email që thotë “Je fitues! Kliko këtu për t’u regjistruar” — por është mashtrim.
- **Si ta parandalosh:** Mos kliko linqe nga njerëz që nuk i njeh; pyet një prind ose mësues; kurrë mos jep fjalëkalimin tënd.

➢ **Si të mbrohemi? Përdorimi i antivirusëve, fjalëkalimeve të sigurta, autentifikimit me dy faktorë, dhe mos hapja e mesazheve nga burime të panjohura janë mënyra efektive për të zvogëluar rrezikun.**

SULMET KIBERNETIKE: PHISHING, MALWARE, HACKING

- 🦠 **Malware (një program i keq brenda kompjuterit)**

Çfarë është: Një program që futet fshehurazi në telefon ose kompjuter për të vjedhur të dhëna, për të shkatërruar skedarë, ose për të parë çfarë bën ti.

- **Shembull:** Ke shkarkuar një lojë nga një faqe të panjohur dhe papritmas telefoni yt fillon të ngadalesohet dhe shfaq reklama të shumta.

Si ta parandalosh: Shkarko lojëra vetëm nga dyqanet e njohura (App Store/Play Store); mos hap skedarë nga njerëz të panjohur; instalo një program antivirus dhe përditëso pajisjen.

- **Si të mbrohemi? Përdorimi i antivirusëve, fjalëkalimeve të sigurta, autentifikimit me dy faktorë, dhe mos hapja e mesazheve nga burime të panjohura janë mënyra efektive për të zvogëluar rrezikun.**

SULMET KIBERNETIKE: PHISHING, MALWARE, HACKING

- 🦹‍♂️ **Hacking (hyrja e paligjshme në sistemet e të tjerëve)**
- **Çfarë është:** Kur dikush hyn pa leje në kompjuterin, llogarinë ose rrjetin e një personi për të marrë informacion ose për të prishur punën.
- **Shembull:** Një person përpiqet të gjejë fjalëkalimin tënd dhe të hyjë në llogarinë tënde të email-it.

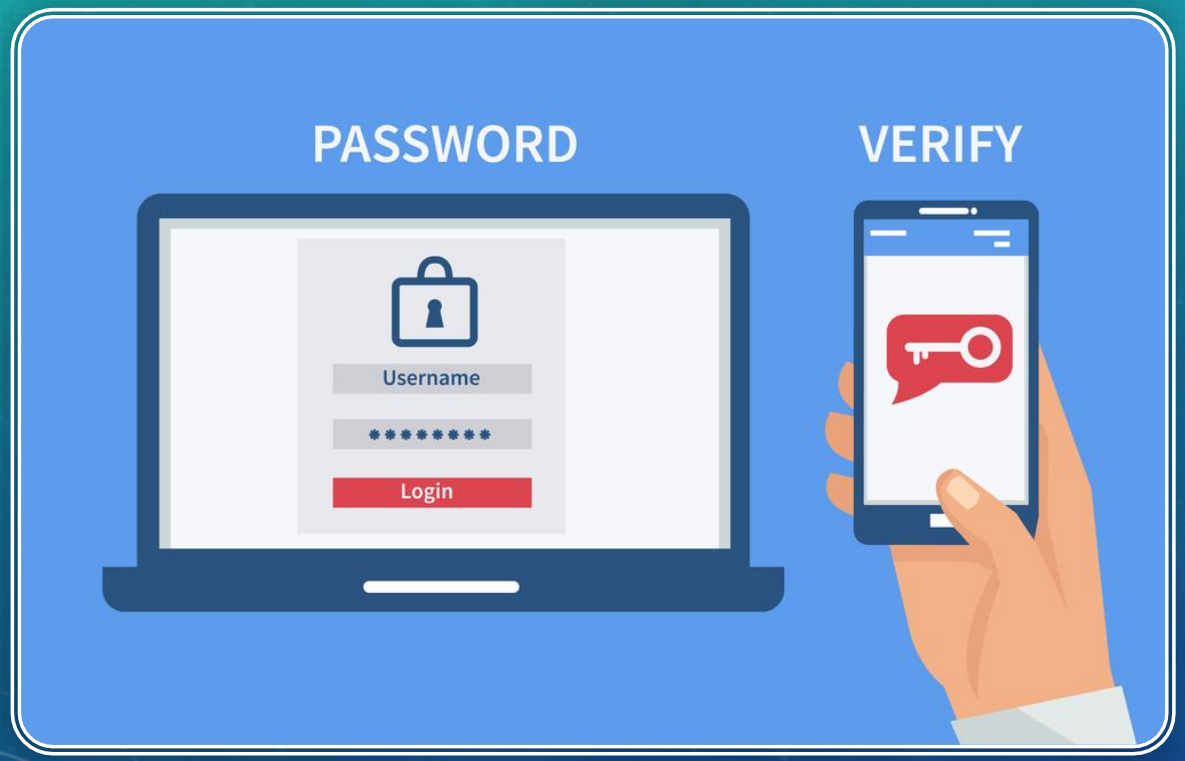
- **Si ta parandalosh:** Përdor fjalëkalime të forta; aktivizo verifikimin me dy hapa (2FA); mos përdor të njëjtin fjalëkalim për shumë llogari; mos lidhu me Wi-Fi publik pa VPN.

➢ **Si të mbrohemi? Përdorimi i antivirusëve, fjalëkalimeve të sigurta, autentifikimit me dy faktorë, dhe mos hapja e mesazheve nga burime të panjohura janë mënyra efektive për të zvogëluar rrezikun.**

SI MUND TË MBROHEMI?

- Mbrojtja e të dhënave personale është një proces që kërkon kujdes dhe vigjilencë të vazhdueshme. Në botën digjitale, ku informacionet qarkullojnë me shpejtësi, individët mund të minimizojnë rreziqet duke përdorur strategji të sigurta.
- Më poshtë janë masat kryesore të sigurisë që duhet të aplikojmë për të mbrojtur të dhënat tona.

1. PËRDORIMI I FJALËKALIMEVE TË SIGURTA DHE AUTENTIFIKIMI ME DY FAKTORË



Ky mekanizëm **shton një shtresë ekstra sigurie** duke kërkuar një kod shtesë për qasje, zakonisht të dërguar në telefon ose email.

- **Përfitimet:**
- Redukton mundësinë e vjedhjes së fjalëkalimit.
- Bën më të vështirë qasjen e paautorizuar edhe nëse dikush di fjalëkalimin tuaj.
- Shumica e platformave si **Google, Instagram, Facebook, Bankat Online** e mbështesin këtë veçori.

1

Test Scan
srtscanricoh@gmail.com

Manage your Google Account

Ricoh Testing *Default*
ricohtestingmac@gmail.com

Add another account

Sign out of all accounts

Privacy Policy • Terms of Service

2

Google Account

Search Googl

Home

Personal info

Data & privacy

Security

People & sharing

Payments & subscriptions

About

3

Signing in to Google

Password — Last changed May 10

Use your phone to sign in — Off

2-Step Verification — Off

2. RREGULLAT E SIGURISË NË INTERNET

➢ **Pse është e rëndësishme?**

- Sulmet kibernetike **përdorin dobësitë** në sistemet tona për të fituar akses në informacionet personale. Mbrojtja e pajisjeve tona është **thelbësore** për të reduktuar këto rreziqe.

➢ **Si të mbrohemi?**

- **Përditëso softuerët dhe aplikacionet** rregullisht për të shmangur dobësitë e sigurisë.
- **Mos hap email-e dhe mesazhe nga burime të panjohura** (mund të jenë sulme phishing).
- **Përdor VPN kur lidheni në rrjete publike** për të mbrojtur trafikun tuaj të internetit.
- **Instalo një antivirus cilësor** dhe aktivizo firewall-in në pajisjet tuaja.
- **Kujdes me shkarkimet online** – shmang skedarët që nuk kanë burim të besueshëm.
- **Verifikoni faqet ku vendosni të dhënat personale** – sigurohuni që janë të enkriptuara (https://).

Çfarë është VPN-ja (Virtual Private Network)?

VPN do të thotë **Rrjet Privat Virtual** — një mjet që ndihmon për **të mbrojtur privatësinë dhe sigurinë tuaj online.**

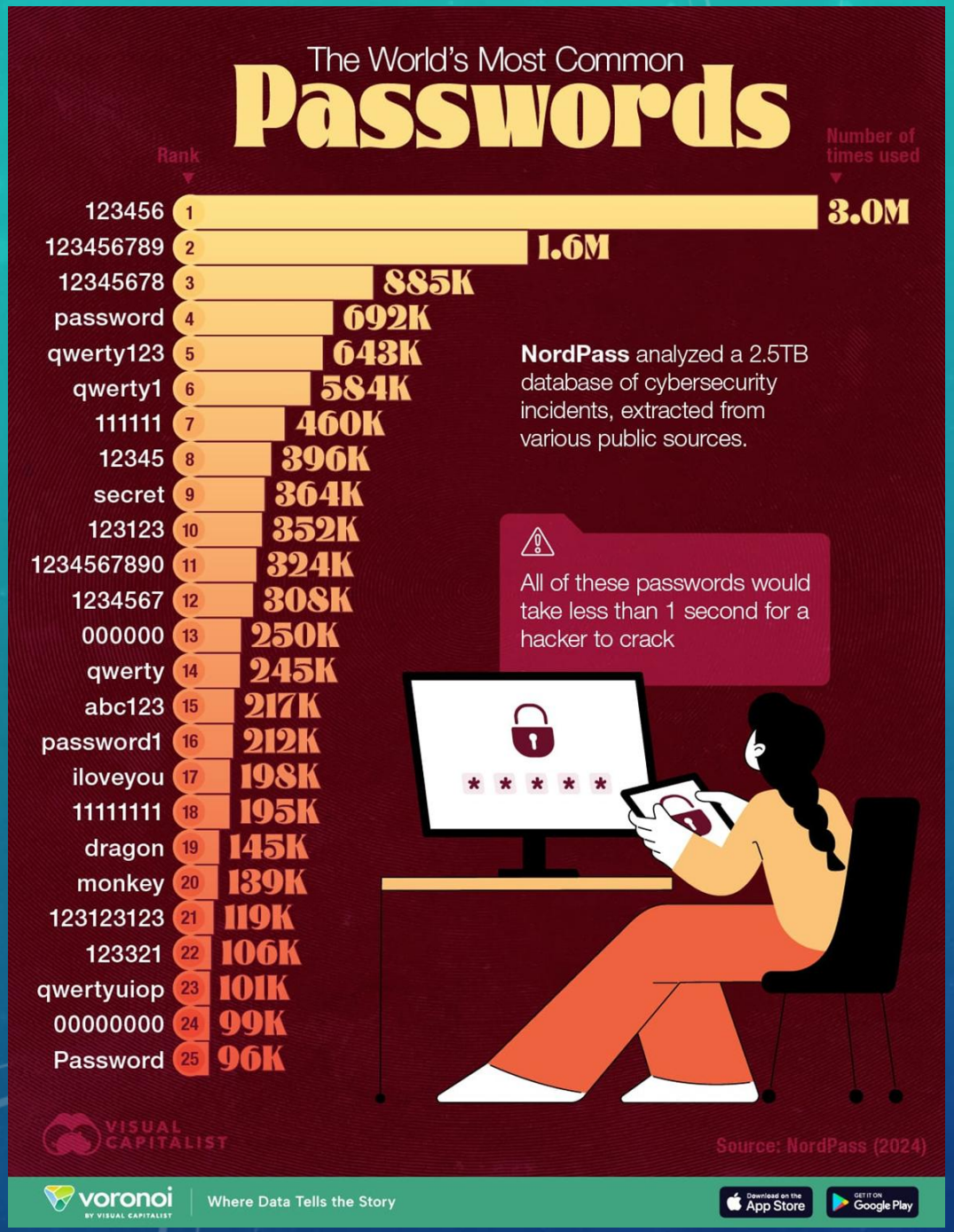
Ja si funksionon me fjalë të thjeshta

1. **Fsheh vendndodhjen tënde (location)**
Kur lidheni me një VPN, interneti mendon se jeni në një vend tjetër — p.sh. mund të jeni në Tiranë, por të duket sikur jeni në Berlin.

2. **Kodifikon (enkripton) lidhjen tuaj**
VPN "mbështjell" të gjitha të dhënat që dërgoni ose merrni në internet, në mënyrë që askush (as rrjeti publik, as hakerat) të mos i lexojë dot.

3. **Mbron të dhënat personale**
Kur përdorni Wi-Fi publik (në shkollë, kafene, aeroport), VPN ju mbron që dikush të mos ju vjedhë fjalëkalimet, kartat apo mesazhet.

4. **Ju ndihmon të kaloni kufizime online**
VPN përdoret edhe për të hyrë në faqe ose platforma që mund të jenë të bllokuara në një vend të caktuar.



Si të krijosh një password të fortë

1. Zgjidh **3-4 fjalë të rastësishme** që të pëlqejnë, pa lidhje me njëra-tjetrën (p.sh. *mollë, rrugë, kafe, re*).

2. Bashko i gjitha së bashku dhe shto **një numër** dhe **një simbol** dhe një shkronjë të madhe:
   Shembull: `molleRrugeKafe7!` — e lehtë për t'u mbajtur, por e fortë.

3. Për akoma më shumë siguri, përdor një ndryshim specifik për çdo faqe (p.sh. shto 2 shkronja të shkurtuara që të kujtojnë faqen: `molleRrugeKafe7!FB` për Facebook).

3. MENAXHIMI I PRIVATËSISË NË RRJETET SOCIALE

Kontrollo privatësinë

- Vendos që vetëm persona të besuar të shohin profilin dhe postimet e tua

Mo**s shpërndaj të dhëna personale**

- Mos ndaj adresën, vendndodhjen e drejtpërdrejtë apo numrin e telefonit.

Mos prano kërkesa miqësie nga të panjohur

- Shumë profile të rreme përdoren për mashtrim. **Mos kliko linke të dyshimta**
- Mund të të çojnë në faqe mashtruese ose të vjedhin informacionin tënd.

- **"Jo çdo 'like' është miqësi. Më e rëndësishme është siguria, jo numri i ndjekësve."**
- **"Ndajmë histori, jo të dhëna personale."**

Çfarë është vjedhja e identitetit?

- Dikush gjen fjalëkalimin tënd dhe hyn në email/rrjete sociale.
- Dikush përdor fotot dhe emrin tënd për të krijuar një profil të rremë.
- Dikush përdor të dhëna (nr. identiteti, adresë) për të hapur një kartë ose marrë kredi.
- Informacione të dorëzuara në faqe mashtruese (“phishing”) përdoren për të marrë qasje në llogaritë tua.

- **“Jo çdo ‘like’ është miqësi. Më e rëndësishme është siguria, jo numri i ndjekësve.”**
- **“Ndajmë histori, jo të dhëna personale.”**

Shenjat që mund të tregojnë vjedhje identiteti

- Paralajmërime nga banka për transaksione që ti nuk i ke bërë.
- Faturime ose letra për shërbime/llogari që ti nuk i njeh.
- Pamundësia për të hyrë në email ose rrjete sociale (fjalëkalimi është ndryshuar).
- Njerëz që i shohin profilin tënd si “i dyshuari” në forume ose mesazhe që s’ke dërguar.

Çfarë të bësh nëse dyshon se je viktimë

1. **Ndrysho fjalëkalimet** menjëherë (email, banka, rrjete sociale).
2. **Njofto bankën** dhe ndal ose blloko kartat e dyshimta.
3. **Ruaj provat** (mesazhe, email-e, screenshot) dhe bëj screenshot të çdo gjëje të dyshimtë.
4. **Raporto** te policia lokale dhe platforma ku u krye mashtrimi (Facebook, Instagram, banka).
5. **Bëj verifikim të llogarive** — kërko nga banka të verifikojë aktivitetin dhe të marrë masa.
6. Nëse je i/e ri/ e — **trego një të rritur** (prind, mësues) menjëherë
-

Fakte dhe këshilla për sigurinë e vajzave e grave online

1. **Vajzat janë më shpesh target i ngacmimeve online.**
   – Sipas studimeve të OKB-së, **1 në 3 vajza** ka përjetuar forma ngacmimi, përfshirë **mesazhe ofenduese, shpërndarje fotosh pa leje** apo **komente negative në rrjete sociale**.
   – Këshillë: Mos u ndje kurrë në faj për sjelljen e tjetrit. Ruaj provat dhe njofto një të rritur ose autoritetet.

2. **Fotot personale janë të tua – jo të internetit.**
   – Shpërndarja e një fotoje private, edhe në mënyrë "të fshehtë", mund të dalë jashtë kontrollit shumë shpejt.
   – Këshillë: para se të postosh diçka, pyet veten:
   "A do të doja që kjo foto të mbetej online përgjithmonë?"

3. **Mos prano kërkesa nga persona që nuk i njeh.**
   – Shumë vajza mendojnë se "nuk do të ndodhë me mua", por mashtruesit online shpesh përdorin **profil të rremë** dhe **komplimente për të fituar besim.**
   – Këshillë: nëse dikush kërkon informacione personale ose foto, **blloko dhe raporto.**

Si të mbrohemi nga bullizmi online?

Mos reagoni menjëherë

- Merrni një moment për të qetësuar emocionet para se të përgjigjeni.

Ruani provat

- Bëni screenshot ose ruani mesazhet që tregojnë bullizmin.

Bllokoni dhe raportoni

- Përdorni opsionet e platformës për të bllokuar personin dhe për të raportuar sjelljen abuzuese.

Flisni me dikë të besuar

- Njoftoni një prind, mësues ose mik që mund t'ju mbështesë.

Vendosni kufij për privatësinë

- Kontrolloni cilësimet e profilit dhe kufizoni se kush mund t'ju kontaktojë.

Kërkoni ndihmë profesionale

- Kontaktoni organizata dhe linja të specializuara për mbështetje.

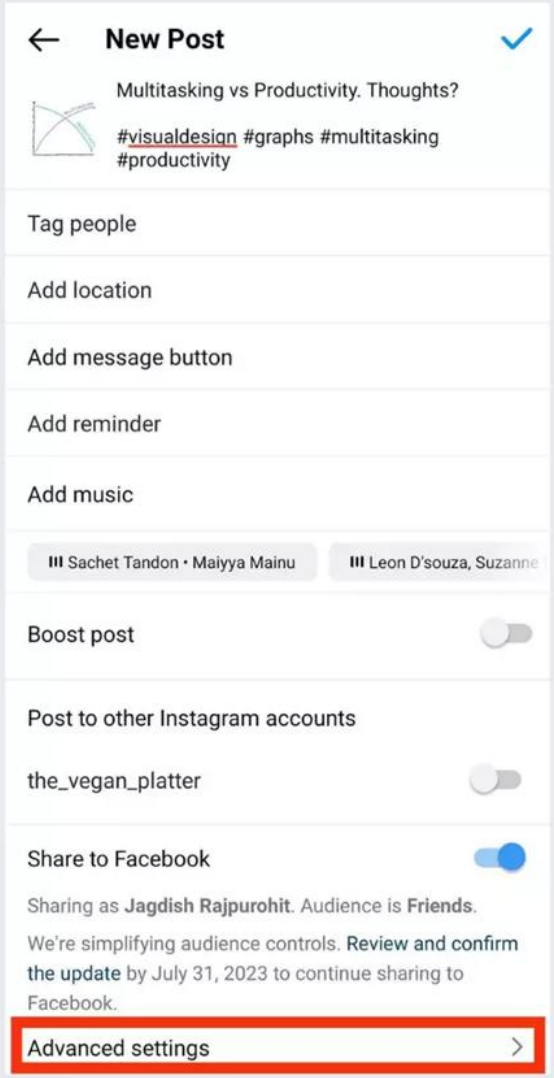
📞 **Kontakte të dobishme në Shqipëri:**

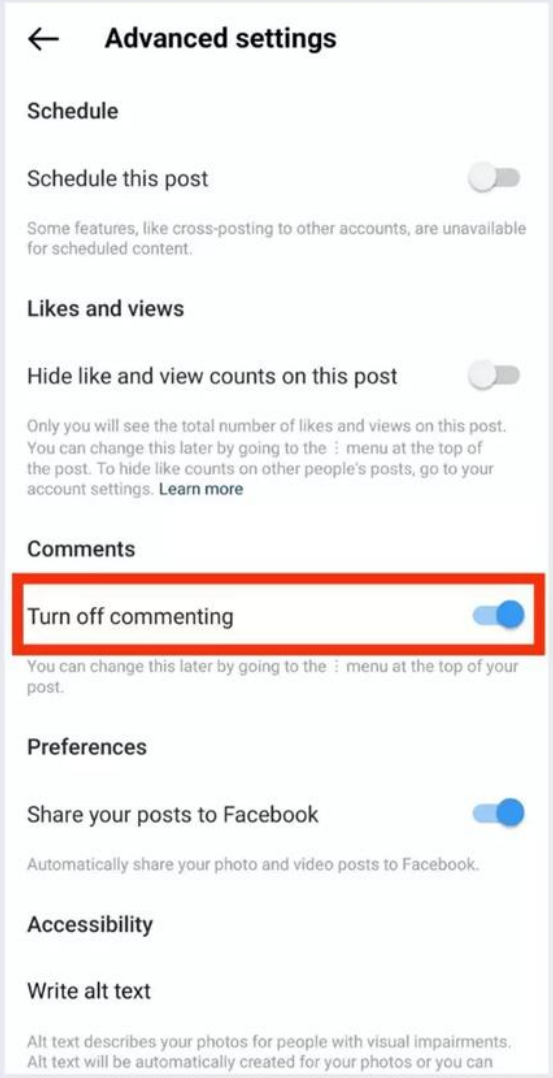
- **116-111** – Linja Kombëtare për Fëmijët dhe të Rinjët (falas, 24/7)

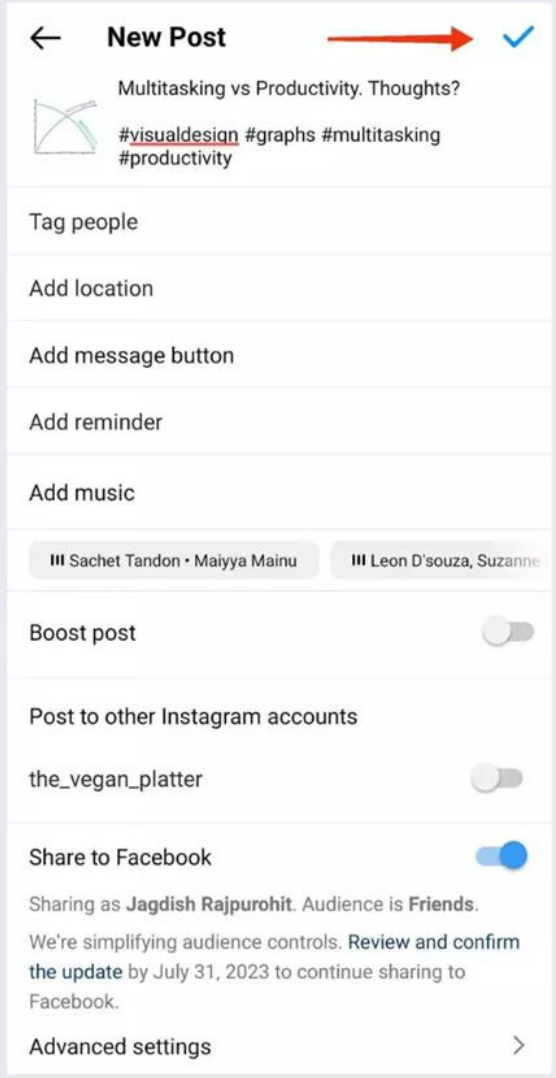
Mënyrat për comment restriction / kontroll komentesh:

1. Filtër fjalësh kyçe (Keyword filter)
2. Aprovimi manual i komenteve (Comment moderation)
3. Kufizimi për përdorues të panjohur (Restrict unknown users)
4. Kufizimi i shprehjeve të ofenduese (Profanity filter)
5. Limiti i frekuencës së komenteve (Comment rate limit)
6. Përdor opsionin “Restrict / Shadowban”
7. Raportimi dhe bllokimi i automatikshëm

How To Turn Off Comments On Instagram Before Posting?







STATUSREW

Fakte interesante për Shqipërinë dhe internetin

Shqipëria ka mbi **80% përdorues të internetit**, por shumë fshatra të vogla ende kanë **akses të kufizuar** ose të ngadaltë.

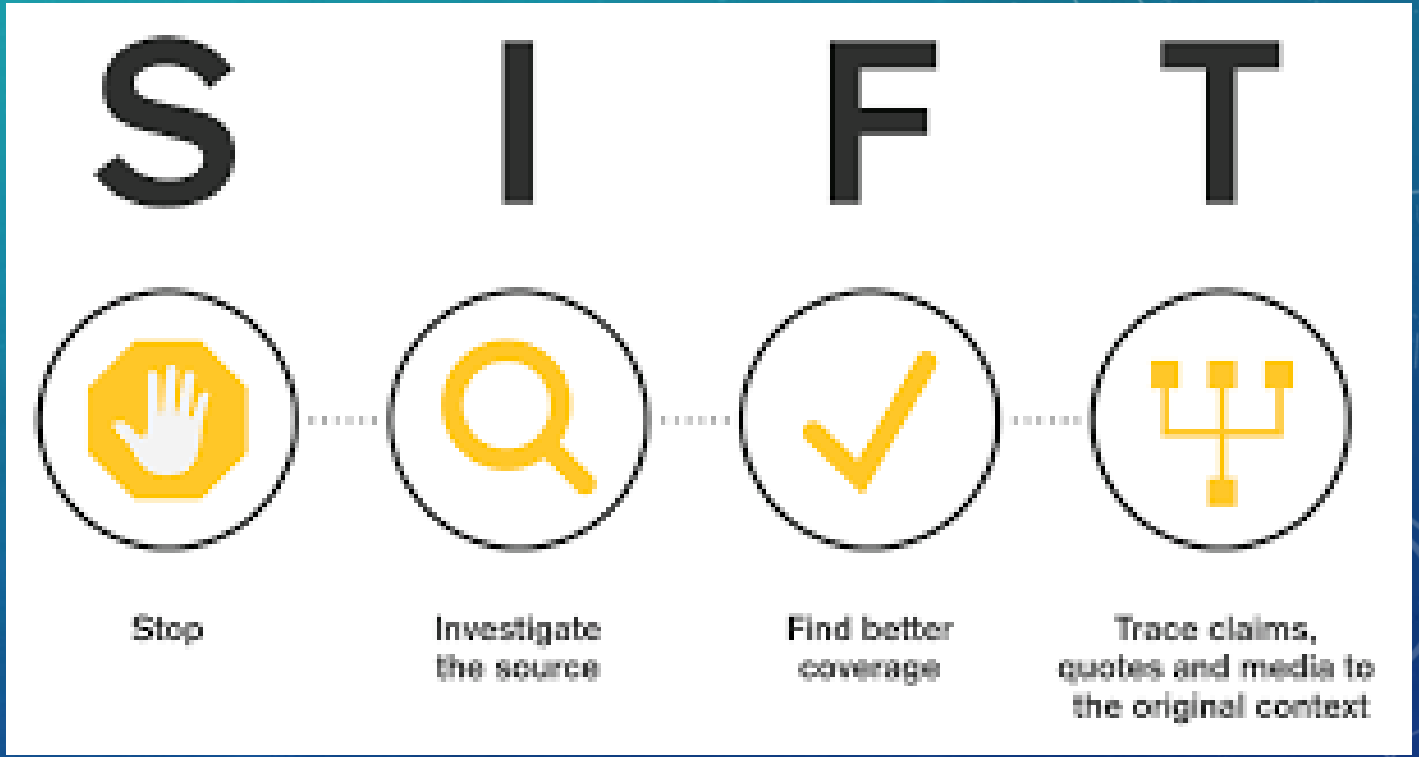
Shqipëria është një nga vendet e Ballkanit ku **përhapja e lajmeve të rreme** është shumë e shpejtë, sidomos në **Facebook** dhe **TikTok**.
Fakt interesant: sipas studimeve, **1 në 3 të rinj shqiptarë** kanë ndarë pa dashje një lajm të rremë në rrjete sociale.
Fjalëkalimet e lehta janë shumë të zakonshme!
Një nga fjalëkalimet më të përdorura në Shqipëri është… **"123456"**
(dhe kjo e bën shumë të lehtë që dikush të hyjë në llogarinë tënde!)

Fëmijët shqiptarë janë shumë aktivë online!

Mbi **90% e nxënësve nga 9 deri në 16 vjeç** përdorin internetin çdo ditë, por vetëm gjysma **kanë biseduar me prindërit** për rreziqet që sjell ai.

Si të dallojmë lajmet e pavërteta?

1. Kontrollo burimin
2. Lexo përtej titullit
3. Verifiko autorin
4. Kontrollo datën
5. Verifiko faktet
6. Shiko fotot dhe videot
7. Analizo qëllimin emocional
8. Mos beso çdo gjë që shpërndahet shumë
9. Shiko domenin dhe URL-në
10. Mendo para se ta shpërndash



Disa fakte për botën online

🌍 Çdo ditë krijohen mbi **300 miliardë email-e** në botë — por rreth **70% janë spam**!

🔐 Fjalëkalimi më i përdorur në botë është ende **“123456”** — dhe mund të çahet për më pak se **1 sekondë**.

👀 Çdo foto që poston online mund të qëndrojë në internet **përgjithmonë**, edhe nëse e fshin më vonë.

📱 Fëmijët nga 8 deri në 12 vjeç kalojnë mesatarisht **4 orë në ditë online**, sipas një studimi të UNICEF-it.

🕵️‍♀️ Hakerët mund të krijojnë faqe që duken **identike me ato zyrtare**, vetëm duke ndryshuar një shkronjë në adresë (p.sh. “instaqram” në vend të “instagram”).

👦 1 në 3 përdorues të internetit në botë janë **fëmijë ose të rinj nën 18 vjeç.**

🚫 Në shumë vende, shkollat po krijojnë “**dita pa internet**” për t’u mësuar fëmijëve rëndësinë e pushimeve dixhitale.

SI MUND TË NDIHMOJNË SHKOLLAT DHE UNIVERSITETET?

- Futja e mësimeve mbi privatësinë digjitale si pjesë e kurrikulës.
- Organizimi i trajnimeve mbi sigurinë kibernetike dhe mënyrat e mbrojtjes së të dhënave.
- Krijimi i moduleve edukative për përdorimin e sigurt të internetit dhe rrjeteve sociale.
- Përdorimi i simulimeve dhe skenarëve praktikë për të rritur ndërgjegjësimin mbi rreziqet dhe mbrojtjen e informacionit.
- Angazhimi i profesorëve për të edukuar studentët mbi rëndësinë e privatësisë online.