



Udhëzues i Detajuar për Sigurinë Kibernetike

STAR Sh.p.k. - Mbrojtja e të dhënave tuaja në internet

STAR Sh.p.k. – Operator i Shërbimeve të Komunikimeve Elektronike

Gusht 2026 | Versioni 3.0

© 2026 STAR Sh.p.k. – Të gjitha të drejtat e rezervuara

 www.starcom.al |  support@starcom.al |  +355 69 2023 337

1 Kërcënimet Kibernetike: Si t'i njohim?

Ky udhëzues është hartuar për të ndihmuar abonentët tanë të mbrojnë aktivitetin e tyre në internet përmes hapave konkretë dhe edukimit mbi kërcënimet bashkëkohore.



Phishing (Peshkimi)

Hakerët dërgojnë email-e, SMS ose WhatsApp që imitojnë banka ose shërbime të njohura.

- ⚠️ Adresa e dërguesit e dyshimtë
- ⚠️ Gjuhë urgjente dhe kërcënuese
- ⚠️ Linke me shkurtues (bit.ly)
- ✅ Kontrolloni adresën e dërguesit
- ✅ Asnjë institucion serioz nuk kërkon fjalëkalimin përmes email-it



Ransomware (Kërkesa për haraç)

Program keqdashës që enkripton fotot dhe dokumentet tuaja, duke kërkuar pagesë për zhbllokim.

- ⚠️ Email-e me bashkëngjitje të infektuara
- ⚠️ Faqe interneti të komprometuar
- ✅ **Mos paguani!** Nuk ka garanci
- ✅ Shkëputeni menjëherë nga interneti
- ✅ Bëni backup të rregullt të skedarëve



Social Engineering

Manipulimi psikologjik për të marrë informacione konfidenciale.

- ⚠️ Thirrje nga "punonjës të bankës"
- ⚠️ Mesazhe nga "miq" në rrjete sociale
- ✅ **Kurrë** mos jepni fjalëkalime përmes telefonit
- ✅ Verifikoni identitetin e personit që ju kontakton

2 Mbrojtja e Pajisjeve

Kompiuter, Smartphone, Tablet - të gjitha këto pajisje kërkojnë masa mbrojtëse për të garantuar sigurinë tuaj.



Përditësimet (Patching)

Sistemet operative lëshojnë përditësime për të mbyllur "vrimat" e sigurisë. **Rreth 60% e sulmeve ndodhin për shkak të mungesës së përditësimeve.**

- ✓ Aktivizoni "Automatic Updates"
- ✓ Përditësoni aplikacionet dhe shfletuesit
- ✓ Përditësoni firmware-in e router-it



Antivirus dhe Firewall

Antivirus-i zbulon dhe eliminon malware-in, ndërsa firewall-i kontrollon trafikun e rrjetit.

- ✓ Përdorni Windows Defender ose një antivirus të licensuar
- ✓ **Mos mbani dy antiviruse** njëkohësisht
- ✓ Sigurohuni që firewall-i është aktiv



Backup (Rezervimi i të Dhënave)

Rregulli "**3-2-1**" për backup: 3 kopje, 2 media të ndryshme, 1 kopje jashtë vendit.

- ✓ Bëni backup të paktën një herë në javë
- ✓ Përdorni Cloud (Google Drive, OneDrive)
- ✓ Mbani një disk të jashtëm të enkriptuar

3

Siguria e Rrjetit Wi-Fi në Shtëpi

Router-i juaj është porta e hyrjes për hakerët nëse nuk është konfiguruar saktë.



Fjalëkalimi i Router-it

Ndryshoni fjalëkalimin "default" (admin/admin) të hyrjes në panelin e router-it.

- ✓ Përdorni të paktën 12 karaktere
- ✓ Kombinoni shkronja, numra dhe simbole
- ✓ Mos përdorni informacione personale



Kriptimi i Rrjetit

Sigurohuni që Wi-Fi juaj të jetë i konfiguruar me standardin më të sigurt.

- ✓ **WPA3** – Më i sigurti
- ✓ **WPA2-AES** – I sigurt
- ✗ **WEP** – Nuk duhet përdorur



Guest Network

Aktivizoni një rrjet "Guest" për vizitorët, që të mos kenë akses në pajisjet tuaja kryesore.

- ✓ Izoloni pajisjet në Guest Network
- ✓ Vendosni një fjalëkalim të ndryshëm
- ✓ Ndryshoni fjalëkalimin periodikisht

4

Menaxhimi i Llogarive dhe Fjalëkalimeve



Fjalëkalime Unike

Rregulli i "**Një fjalëkalim për llogari**" – nëse përdorni të njëjtin fjalëkalim kudo, një shkelje në një faqe rrezikon të gjitha llogaritë.



Përdorni një fjalëkalim të fortë:
\$t@rC0m#2026_S3cUr3!



Password Managers

Mjete që ruajnë fjalëkalimet në mënyrë të enkriptuar. Ju duhet të mbani mend vetëm **një** fjalëkalim kryesor.

- ✓ **Bitwarden** – Falas, Open Source
- ✓ **KeePass** – Lokal, Falas
- ✓ **1Password** – Me pagesë



Autentikimi me Dy Faktorë (2FA/ MFA)

Hapi më i rëndësishëm! Shton një shtresë shtesë sigurie përveç fjalëkalimit.

- ✓ **SMS** – Mesatar
- ✓ **Authenticator App** – Google, Microsoft
- ✓ **Hardware Key** – YubiKey, më e sigurta



Aktivizoni 2FA në Email, Bankë, Rrjete Sociale dhe Cloud!

5

Çfarë të bëni nëse bini viktimë?

Nëse keni dyshime se jeni hakuar, ndiqni këto hapa menjëherë:

1

Shkëputeni nga interneti

Fikni Wi-Fi dhe të dhënat celulare për të ndaluar përhapjen e malware-it.

2

Ndryshoni fjalëkalimet

Nga një pajisje tjetër e sigurt, ndryshoni të gjitha fjalëkalimet.

3

Kontaktoni bankën

Nëse keni futur të dhëna karte, njoftoni menjëherë bankën tuaj.

4

Njoftoni STAR Sh.p.k.

Na kontaktoni për të kontrolluar trafikun e pazakontë nga pajisja juaj.

5

Ruani provat

Mos fshini email-et ose mesazhet – ato mund të jenë prova të rëndësishme.

6

Raportoni te AKEP

Nëse është një sulm i rëndësishëm, raportoni te AKEP (www.akep.al).

6

Përmbledhje e Rekomandimeve Kryesore

NR.	REKOMANDIMI	PRIORITETI
1	Aktivizoni 2FA/MFA në të gjitha llogaritë	KRITIK
2	Përdorni fjalëkalime unike për çdo llogari	KRITIK
3	Përdorni një Password Manager	KRITIK
4	Aktivizoni përditësimet automatike	KRITIK
5	Përdorni WPA2/WPA3 për Wi-Fi	I LARTË
6	Bëni backup të rregullt të të dhënave	I LARTË
7	Përdorni antivirus dhe firewall	I LARTË
8	Shmangni rrjetet publike Wi-Fi pa VPN	I MESËM
9	Ndryshoni fjalëkalimin e router-it	I MESËM
10	Aktivizoni Guest Network për vizitorët	I ULËT



Kontakte për Mbështetje



OPERATORI
STAR Sh.p.k.



ADRESA
Lagja Apollonia, Rruga Jakov
Xoxa Nr. 17, Fier



WEB
www.starcom.al



EMAIL
support@starcom.al



TELEFON
+355 69 2023 337

Publikuar nga: STAR Sh.p.k.

Data: Gusht 2026

Versioni: 3.0 (I Detajuar)

© 2026 STAR Sh.p.k. – Të gjitha të drejtat e rezervuara