

KIBERXAVFSIZLIK

Kuchli parol va ikki bosqichli autentifikatsiya: to‘liq qo‘llanma

Akkauntlaringizni buzib kirishdan himoyalashning eng samarali va oddiy usullari.

Muallif: **Xurshidjon Yunusov** • 22 oktabr 2026

Akkauntlarning buzilishi ko‘pincha murakkab xakerlik hujumlari tufayli emas, balki zaif yoki takroriy parollar sababli sodir bo‘ladi. Yaxshi xabar shundaki, himoya ham juda murakkab emas.

Kuchli parol nima?

AQSh standartlar instituti NIST’ning raqamli identifikatsiya bo‘yicha tavsiyalari (SP 800-63B) parolning **uzunligini** murakkabligidan muhimroq deb hisoblaydi. Shuningdek, sababsiz muntazam parol almashtirishni majburlamaslikni tavsiya qiladi.

- Kamida 12–16 belgi ishlating.
- Bir nechta tasodifiy so‘zdan iborat *parol-ibora* eslab qolishga oson va kuchli: masalan, to‘rt-besh bog‘liqsiz so‘z.
- Ism, tug‘ilgan sana, “123456” va “qwerty” kabi taxmin qilinadigan variantlardan qoching.
- Eng muhimi: **har bir sayt uchun alohida parol.**

Parol menejeri

Har bir sayt uchun noyob parolni eslab qolish imkonsiz. Shuning uchun parol menejerlari (Bitwarden, 1Password, KeePass yoki brauzerning o‘z menejeri) mavjud. Siz faqat bitta asosiy parolni eslaysiz, qolganini dastur yaratadi va saqlaydi.

Ikki bosqichli autentifikatsiya (2FA)

Hatto parolingiz o‘g‘irlansa ham, 2FA hujumchini to‘xtatadi: kirish uchun ikkinchi omil — telefon yoki qurilma — kerak bo‘ladi.

Usul	Himoya darajasi	Izoh
SMS kod	Past–o‘rta	SIM-kartani almashtirish (SIM swap) hujumiga zaif
Autentifikator ilova (TOTP)	Yuqori	Har 30 soniyada yangilanadigan kod
Apparat kalit / passkey (FIDO2)	Eng yuqori	Fishingga chidamli

Telegram uchun maslahat

Telegram’da *Sozlamalar* → *Maxfiylik va xavfsizlik* → *Ikki bosqichli tasdiqlash* bo‘limida qo‘shimcha parol o‘rnating. Shunda SMS kod qo‘lga tushsa ham akkauntingizga kirib bo‘lmaydi.

Eng yaxshi parol — siz eslamaydigan, parol menejeri eslaydigan paroldir.