

# Meelespea KOV 2025 valimiste kandidaadile

KÜBERKINDLUS • POLIITREKLAAM

## Hea kandidaat!

Soovime sulle edu valimisteks valmistumisel ja kandideerimisel! Selleks oleme koostanud meelespea, kus käime üle olulised punktid, et kohalike omavalitsuste valimised mööduksid sujuvalt. Eesti on demokraatlik riik, mille avalike teenuste digitaliseeritus on maailmas üks suurimaid. See toob endaga kaasa vajaduse pöörata suuremat rõhku küberturvalisusele ja igapäevasele küberhügieenile. KOV valimiste kandidaadina oled avaliku elu tegelane, mis tõstab huvi ka sinu tegevuse vastu internetis või võtavad hoopiski küberkurjategijad sind sihikule. Anname nippe ja näpunäiteid, kuidas käituda küberturvalisemalt ning mida kampaaniat tehes silmas pidada.

## Valimiskampaania küberkindlus

### 1. Tea küberohtusid – ennetamine on odavam kui intsidendi lahendamine

Kui küberkuritegevus oleks riik, oleks selle majandus maailmas suuruselt kolmas, seega kurjategijaid kasutavad osavalt ära inimeste hooletut käitumist. Võta alati hetk ja mõtle, enne kui kuhugi vajutad: kui tajud ajasurvet, hirmutamist või on pakkumine lihtsalt liiga hea, siis tõenäoliselt on tegu pettusega. Kontrolli alati saatja e-posti või veebilehe aadressi, et see oleks korrektne. Võimalusel väldi lühilinkidel (tiny-URL) klikkimist ja QR-koodide skaneerimist. Kurjategijaid võivad üritada nende kaudu võtta üle su sotsiaalmeediat, varastada tundlikke andmeid ning proovida saada ligipääsu sinu seadmele. Loe lähemalt [pettuste](#) ja [pahavara](#) kohta.

### 2. Kaitse oma kontosid

Kasuta igal kontol unikaalset ja tugevat parooli ning lülita sisse kaheastmeline autentimine. Märkimisväärne osa valimistega seotud suhtlusest toimub meilitsi ja sotsiaalmeedias ning seetõttu on oma kampaania kaitsmiseks oluline kaitsta oma kontosid, kasutades unikaalseid ja tugevaid paroole ja kaheastmelist autentimist. Kasutades ühte ja sama nõrka parooli näiteks e-postil, sotsiaalmeedias ja veebipoes, pääseb ründaja lekkinud parooli kaudu ligi kõikidele sinu kontodele. Kaheastmeline autentimine on turvameede, mis lisab sinu kontole täiendava kaitsekihi, nõudes kasutajalt enda tuvastamist kahel sõltumatul viisil (näiteks mobiil-ID või parool ja telefonile tulev kinnituscode). Kui kahtlustad, et su parool on saanud teatavaks kõrvalisele inimesele, olgu või heale tuttavale, vaheta see kohe. Lisainfot tugeva parooli kasutamise ja kaheastmelise autentimise seadistamise kohta loe [siit](#).

### 3. Logi oma kontodele sisse ainult turvalistest seadmetest

Turvaline seade on oluline, et vältida parooli või andmete lekkimist. Väldi avalike arvutite kasutamist (näiteks raamatukogus või koolis). Kui siiski pead seda tegema, kasuta incognito profiili, kustuta alati oma sirvimisjalugu, ära salvesta paroole veebilehitsejasse ning võimalusel vaheta järgmine kord turvalist seadet kasutades oma paroolid. Oma andmete ja kasutajakontode kaitsmiseks ära anna oma seadmeid teistele inimestele kasutamiseks, ka mitte lastele mängimiseks.

### 4. Pööra tähelepanu turvalisele kaugtööle

Paljud meist töötavad kodukontoris, kohvikus või rongis. Arvesta, et sinu ekraan ja mis sinna kirjutad võivad olla nähtavad teistele inimestele või kaameratele. Ära jäta oma seadet avalikus ruumis mitte kunagi järelevalveta, hoia ekraan lukustatuna ning võta arvutist välja ID-kaart. Loe ka [soovitusi turvaliseks kaugtööks](#).

### 5. Juhi oma kampaaniameeskonda küberturvaliselt

Tehes kampaaniat meeskonnaga, loo igale meeskonnaliikmele personaalsed kasutajakontod ja anna sotsiaalmeedia lehe õigused personaalselt vaid neile, kellel seda on vaja. Väldi jagatud kontode kasutamist ja kontrolli regulaarselt jagatud õigusi. Koolita oma kampaaniameeskonda küberturvaliselt käituma kasutades seda juhendit ja [IT-vaatliku portaali](#).

## 6. Väldi liigse info jagamist internetis

Internetis on meie kohta väga palju infot, suure osas sellest teeme ise avalikuks. See teeb küberkurjategijate või oponentide elu lihtsamaks. Tee enda kohta ise internetis (kasutades otsingumootoreid, sotsiaalmeediat) taustauuring ja kustuta või piira ligipääs andmetele, mis ei peaks olema avalikud. Mõtle alati enne postitamist, kas postitus on vajalik ja sisaldab tõest informatsiooni. Loe lisaks oma [digitaalse elu turvalisuse](#) kohta.

## 7. Väldi avalikke wifi-võrke

Võimalusel väldi avalikke ja tundmatuid wifi-võrke, sest need ei pruugi olla turvalised. Kasuta isiklikku wifit või mobiilset andmesidet, jagades seda vajadusel arvutisse (*hotspot*).

Lisainfot nutiseadmete turvalisuse kohta leiad [siit](#).

## 8. Tee andmetest koopiaid

Tee oma seadmes olevatest andmetest regulaarselt varukoopiaid või seadista automaatne varukoopiategemine, et seadme kadumise, katki minemise või viirusega nakatumise korral ei läheks kaduma tähtsad failid, pildid või videod.

Loe lähemalt [varukoopia tegemise](#) kohta.

## 9. Uuenda regulaarselt oma seadmete tarkvara

Uuenda regulaarselt oma telefoni ja arvuti tarkvara, nii kaitsesid enda andmeid tarkvara turvanõrkuste ära kasutamisest tulevate ohtude eest. Lisaks arvutitele ja telefonidele on internetti ühendatud väga palju muid seadmeid: tolmuimejad, muruniidukid, printerid, telekad jne. Kõigi nende tarkvarades leitakse ja parandatakse pidevalt turvanõrkusi, mistõttu on vajalik regulaarselt paigaldada turvauuendusi. Kui seadmete tarkvara on uuendamata või kasutusel on nõrk tehaseparool, võib kurjategija saada nende kaudu ligipääsu ka teistele võrgus olevate seadmetele.

Kuidas seadistada turvaliselt oma kodust võrku ja seadmeid, loe [siit](#).

## 10. "Appi, mu konto on häkitud!"

Kui oled kaotanud ligipääsu oma tähtsale kontole või avastad oma sotsiaalmeedias kahtlaseid tegevusi, võib sinu konto olla häkitud. Sellisel juhul tuleb reageerida kohe, et päästa oma kampaania sotsiaalmeedias. Nõu saamiseks võid pöörduda [cert@cert.ee](mailto:cert@cert.ee) või lugeda lisa siit.

Lisainfo: [www.ria.ee](http://www.ria.ee), [www.itvaatlik.ee](http://www.itvaatlik.ee)

## 11. Digiteenuste määrus: kandidaatide roll sisu turvalisuse tagamisel valimiste ajal

Digiteenuste määrusest tulenevalt on väga suurtel digiplatvormidel suurenenud kohustused riskihalduse ja sisu monitoorimisega, et tagada valimisprotsessi plaanipärane kulgemine. Kuid oma osa digiplatvormidel nähtava sisu turvalisusele saavad anda ka kandidaadid ise. Selle jaoks on TTJA [juhendis](#) välja toonud vajalikud juurdepääsulingid teatavaks platvormidele nii ebaseaduslikust sisust kui ka platvormi enda kasutajatingimustega vastuolus olevast sisust. Soovitame juhendiga aegsasti tutvuda. Erakorraliste ja kiireloomuliste sotsiaalmeediaga seonduvate küsimuste puhul saab valimisnädalal pöörduda aadressile [valimised@ttja.ee](mailto:valimised@ttja.ee).

## Poliitreklaami uued nõuded ja hea tava

10. oktoobrist hakkab kehtima Euroopa Parlamendi ja nõukogu poliitreklaami läbipaistvuse määrus, mille kohaselt peab iga poliitreklaamiga tegema avalikkusele kättesaadavaks järgmise info:

- teate, et tegemist on poliitreklaamiga;
- poliitreklaami tellija või tellija üle lõplikku kontrolli omava üksuse nime
- märke valimiste, rahvahääletuse, seadusandliku või regulatiivse protsessi kohta, millega poliitreklaam on seotud
- teate selle kohta, et poliitreklaami puhul on kasutatud suunamis- või reklaamiedastusmeetodeid
- läbipaistvusteate või selge viite selle kohta, kust seda on võimalik lihtsalt ja otse leida.

Täpsema info leiab justiits- ja digiministeeriumi [veebilehelt](#).

## Ligipääsetavus

Kampaaniamaterjalide koostamisel tasub jälgida, et neid oleks lihtne mõista ja kasutada kõigil. Eesti Puuetega Inimeste Koja juhised ligipääsetavusele leiab [siit](#).

## Isikuandmete töötlemine valimiskampanias

- Igal andmetöötlaste toimingul peab olema õiguslik alus. Valimiskampania korraldamiseks ei tohi kasutada tööalast juurdepääsu andmekogule.
  - Valimisreklaami igakordne saatmine, sh e-postile või SMS-ina, toimub vaid reklaami saaja selge ja vabatahtliku nõusoleku alusel.
  - Kampaniamängude kaudu isikuandmete kogumise ankeedil ei tohi kasutada „eeltäidetud linnukesi“ nõusoleku saamiseks. Inimene peab üheselt aru saama, millisel eesmärgil ja kus tema isikuandmeid kasutatakse.
- Täpsemad juhised leiab andmekaitse inspeksiooni [veebilehelt](#).

## Valimised ja kool

Haridus- ja teadusministeerium ja Eesti noorteühenduste liit on koostanud hea valimistava noortega töötavatele inimestele.

### Mida võib teha?

- Selgitada, kuidas valimiste protsess toimub
- Arutada, kuidas demokraatia toimib ning milline on institutsioonide roll
- Tutvustada võrdset kõiki maailmavaateid ja kandidaate.
- Korraldada neutraalseid ja tasakaalustatud arutelusid, kus on võimalik osaleda kõikide maailmavaadete esindajatel.
- Kaasata noored ürituste planeerimisse ja modereerimisse.
- Kutsuda esinema poliitikuid, kui sisu toetab õpitulemuste saavutamist ja tagatud on tasakaal.

### Mida ei tohi teha?

- Jagada noortele kampaaniamaterjale (nt pastakad, flaierid).
- Reklaamida ainult konkreetset erakonda, kandidaati või maailmavaadet.
- Lubada levitada valimisreklaami noortele suunatud keskkonna sotsiaalmeedias või ametlikes kanalites.
- Lubada noortel või noortega töötavatel inimestel kampaania tegemiseks oma ametipositsiooni kasutada.
- Värvata noori erakondadesse noortele suunatud keskkondades.

Hea tava on leitav haridus- ja teadusministeeriumi [veebilehelt](#).

## Valimisreklaami paigaldamine

Valimisreklaami tohib paigaldada vastavalt kehtestatud reeglitele. Igas kohalikus omavalitsuses kehtivad oma nõuded reklaamile ja selle paigaldamisele. Reklaami paigaldamiseks peab olema maaomaniku nõusolek.

Kui reklaam paigutatakse riigitee kaitsevööndisse, siis liiklusseaduse järgi võib valimisreklaami paigaldada ainult Transpordiameti loal. Enne reklaami paigaldamist riigitee äärde, tuleb esitada taotlus [Transpordiametile](#).

Taotlusele lisada ka asukohajoonis ja reklaami eskiisjoonis. Paigaldada võib ainult sellist valimisreklaami, mis ei eksita liiklejat ega varja tema eest liikluskorraldusvahendit, ei raskenda liikluskorraldusvahendi eristamist, ei ohusta liiklust liikleja pimestamisega ega tähelepanu hajutamisega ning ei piira nähtavust ristmikul. Täpsemalt saab lugeda [siit](#).

## Valimiskampania aruande esitamine

Valimistel osalevatel erakondadel, valimisliitudel ja üksikkandidaatidel tuleb ühe kuu jooksul arvates valimispäevast esitada Erakondade Rahastamise Järelevalve Komisjonile valimiskampania aruanne. Aruandekohuslase meespea leiab ERJK [veebilehelt](#).

