

Абайлаңыз! Алаяқтар! Құрылғыңызды қорғаңыз

Стационарлық компьютер немесе ноутбук

- Құрылғыдағы **операциялық жүйені және қосымшаларды** үнемі жаңартып отырыңыз.
- Зиянды бағдарламалардан қорғану үшін жаңартылған лицензиялық **антивирус бағдарламасын ғана пайдаланыңыз!** Антивирустың күнделікті автоматты түрде жаңартылып отыратынына көз жеткізіңіз. Құрылғыда зиянды бағдарламалардың бар-жоғын үнемі тексеріп отырыңыз.
- **Құрылғыңыздағы есептік жазбаны күрделі, бірегей құпия сөзбен қорғаңыз.** Өртүрлі бағдарламаға кіру рұқсаты үшін бірдей құпия сөзді пайдаланбаңыз. Құпия сөздерді оқтын-оқтын жаңартып отырыңыз. Құпия сөздерді браузерде сақтамаңыз («Сақтау» белгісін алып тастаңыз). Логиндерді, парольдерді немесе пин-кодтарды стикерге немесе қағазға жазып, ашық жерде қалдырмаңыз. Оларды ешкімге, оның ішінде қызметтестеріңізге, жүйе әкімшісіне, техникалық қолдау маманына немесе өзін Fortebank қызметкері немесе барлау қызметкері деп таныстыруы мүмкін кез-келген басқа адамдарға бермеңіз.
- Өзіңіз қолданатын барлық маңызды жүйеге **екі факторлы аутентификацияны** орнатыңыз.
- Құрылғыңызда қашықтан қол жеткізу бағдарламасын (**AnyDesk, TeamViewer және т.б.**) пайдаланбаңыз.
- Интернет-банкингті жеке, арнайы құрылғыда ғана қолдануға тырысыңыз және ол **құрылғыны үшінші тараптардың қолына ұстатпаңыз.**
- Жұмыс орныңыздан **аз уақытқа тұрсаңыз да, құрылғының экранын құлыптап кетіңіз.**
- **Интернеттен сенімсіз файлдарды жүктеуден аулақ болыңыз.** Құрылғыға бұзылған немесе лицензиясы жоқ бағдарламалық жасақтаманы орнатпаңыз.
- Қол жеткізу құқығын шектейтін функцияны, стандартты құқықтары бар есептік жазбаны пайдаланыңыз. **Күнделікті жұмыста әкімшілік артықшылығы бар есептік жазбаны пайдаланудан аулақ болыңыз.** Бұл құрылғыдағы қажетсіз өзгерістердің алдын алуға көмектеседі.
- Портативті медианы (флэш-дискіні) қолданар алдында, оны әрқашан антивирустық бағдарламамен тексеріңіз. **Интернеттен жүктелген файлдарды да ашпас бұрын, антивируспен тексеріңіз.**
- **Құрылғыңызда кірістірілген желіаралық экранды (брандмауэр) қосыңыз.** Бұл шара құрылғыңызға желі арқылы рұқсатсыз кірудің алдын алуға көмектеседі.
- Вирустық шабуыл жасалған немесе құралыңыз істен шыққан жағдайда, деректерді қалпына келтіру үшін **міндетті түрде маңызды ақпараттардың сақтық көшірмесін** жасап отырыңыз.
- Егер қауіпсіздік жаңартулары жоқ болса, **ескірген операциялық жүйені пайдаланбаңыз.**

Мобильді смартфон немесе планшет

- 01 Құрылғыдағы операциялық жүйені және қосымшаларды үнемі жаңартып отырыңыз.
- 02 Лицензиялық антивирус бағдарламасын орнатыңыз және автоматты түрде жаңарту сигнатурасын қойыңыз.
- 03 Құрылғыға кіру үшін биометриялық деректерді немесе күрделі құпия сөзді/графикалық кілтті пайдаланыңыз. Смартфонға құпия сөзді (немесе графикалық кілтті) терген кезде, сырттан ешкімнің бақылап тұрмағанына көз жеткізіңіз.
- 04 Құрылғыны үшінші тұлғаларға бермеңіз.
- 05 Поштаға, мессенджерлерге, интернет-банкингтерге және басқа да маңызды қосымшаларға екі факторлы аутентификацияны орнатыңыз.
- 06 Смартфондағы қосымшаларда құпия сөздерді сақтап қоймаңыз («Құпия сөзі сақтау» белгісін алып тастаңыз);
- 07 Мессенджер арқылы күдікті қоңырауларды қабылдамаңыз, олар алаяқтар болуы мүмкін. Күдікті немесе шетелдік нөмірлерден келген хабарламаларды оқымастан, жойып тастаңыз.
- 08 Барлық орнатылған қосымшалардың рұқсаттарын тексеріңіз. Қолданбалар тізімін үнемі тексеріп отырыңыз. Пайдаланылмағандарды алып тастаңыз.
- 09 Мобильді қосымшаларды тек ресми дүкендерден (Play Market, App Store) жүктеңіз, бұл оларды үнемі жаңартып отыру процедурасын жеңілдетеді.
- 10 Ресми дүкеннен қосымшаны жүктеп алар кезде өндірушіні, қосымшаның рейтингін және санын тексеріңіз. Қолданбаны бұрын орнатқан пайдаланушылардың пікірлеріне назар аударыңыз.
- 11 ДК, смартфон немесе планшетті (корпоративті немесе жеке) сатпас бұрын, жадыдағы файлдарды мүлдем жою немесе бастапқы жүйелік күйге оралу арқылы оларды тазарту қажет.



Толығырақ ақпаратпен **forte.kz** сайтында танысуыңызға болады, сондай-ақ сайтқа өту үшін **QR сканерлеуіңізге** болады