

Абайлаңыз! Алаяқтар! Өзіңізді алдауға жол бермеңіз!



Өзіңіз пайдаланатын барлық аккаунтқа (интернет-банкінг, пошта, әлеуметтік желілер, мессенджерлер және т.б.) **екі факторлы аутентификация орнатыңыз.**



Интернет-банкінгті пайдаланып отырған кезіңізде **басқа интернет-сайттарда қатар жұмыс істемеңіз.** Алдымен интернет-банкінгтегі ағымдағы сессияны аяқтаңыз.



Егер сіз қоғамдық жерде отырсаңыз немесе ашық, жалпыға ортақ Wi-Fi желісін пайдалансаңыз, интернет-банкінгпен жұмыс істемеңіз. **Сондай-ақ, пошта немесе мессенджер арқылы сауда жасамаңыз немесе маңызды ақпараттар жолдамаңыз.**



Қауіпсіздік сертификаты жоқ сайттарды (http) пайдаланбаңыз. Сайттың TLS шифрлауымен қорғалғанына көз жеткізіңіз (мекенжай жолағының сол жағында жабық құлып көрініп тұруы керек).



Танымайтын адамдар пошта немесе мессенджер арқылы жіберген сілтемелерге өтпеңіз. Бейтаныс немесе күдікті e-mail адрестерден келген хаттарды немесе хабарламаларды ашпаңыз. Сізге мұра берілгені, қомақты жүлде бұйырғаны туралы хаттардағы сілтемелерге өтпеңіз.



Күмәнді сайттарға кірмеңіз. Мұндай ресурстар көбінесе вирустың көзі болып табылады.



Сілтемені баспас бұрын, сайттың атауындағы немесе мекенжайындағы әріптердің орындары ауысқан-ауыспағанын тексеріңіз. Кейде жалған сайттар нақты сайттың дизайнын толық қайталайды да, тек сілтеменің мекенжайы түпнұсқадан басқаша болады.



Егер сіз сайттардың түпнұсқа екендігіне сенімді болмасаңыз, QR кодтарын сканерлемеңіз. QR арқылы сауда жасамас бұрын, банктік қосымшаның хабарламасындағы сатушының, жасалғалы отырған сауданың және төленетін соманың түпнұсқалығын тексеріп алыңыз.



Мекенжайыңыз көрсетілген, жобалардың сипаттамасы берілген жеке және корпоративтік ақпараттарды, фотосуреттерді жарияламаңыз. Телефон нөмірін, e-mail немесе басқа жеке ақпаратты қажет ететін желілік викториналарға, ойындарға, сауалнамаларға, марафондарға қатыспаңыз. Әлеуметтік желілерде құпиялылық параметрлерін орнатыңыз. Мысалы, түсініктемелерді жабу/шектеу, фотосуреттерді қарау.



Қандай да бір стандартты емес хабарламалар пайда болса, құрылғыңыз әдеттен тыс жұмыс істесе, мысалы, парольдеріңізді, **ПИН немесе OTP-кодтар сұраған терезелер пайда болса - дереу құрылғыны өшіріп, қызмет көрсету менеджеріне хабарласыңыз.**



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