

Өзіңізді алаяқтардан қалай қорғауға болады

Жалпы қауіпсіздік ережелері:

- Ақпаратты тек ресми дереккөздерден тексеріңіз.
- Телефон арқылы немесе интернетте айтылған өтініштерді орындауға асықпаңыз.
- Күрделі құпиясөздер мен екі факторлы аутентификация қолданыңыз.
- Қолданбаларды және операциялық жүйені тұрақты түрде жаңартып отырыңыз.

Егер алаяқтардың құрбаны болсаңыз:

- Дереву полицияға **102** нөмірі арқылы немесе <https://qamqor.gov.kz/> сайтында «Полицияға өтініш беру» бөлімі арқылы хабарласыңыз.
- Ақша шешу әрекеті байқалса, картаңызды банк арқылы немесе мобильді қосымша арқылы бұғаттаңыз.
- Көмек алу үшін бірыңғай **116** нөміріне хабарласыңыз.

Банктердің картаны бұғаттау нөмірлері:

- **ForteBank** – 7575
- **Kaspi Bank** – 9999
- **Halyk Bank** – 9595
- **Jusan Bank** – 7711
- **Bereke Bank** – 5030
- **Банк ЦентрКредит** – 505
- **Home Credit Bank** – 7979
- **Altyn Bank** – +7 (727) 356-57-77
- **Еуразиялық банк** – +7 771 000 7722 (Beeline), +7 700 000 7722 (Tele2/Altel), +7 702 000 7722 (Kcell/Activ)
- **Bank RBK** – 7888
- **Freedom Finance Bank Kazakhstan** – 595
- **VTB Bank** – 5050
- **Nurbank** – 2552
- **Zaman Bank** – 4077
- **Al Hilal Ислам Банкі** – +7 (727) 233-00-00
- **Shinhan Bank** – 2468
- **Bank of China Қазақстан** – +7 (727) 258-55-10 ішкі 1140, 1153

Маңызды! Сіз алаяқтардың шотын **Антифрод-орталық** арқылы бұғаттай аласыз: банкке хабарлап немесе полицияға өтініш беріп.

Қосымша ақпарат:

Сұрақтар туындаған жағдайда немесе кеңес қажет болса, Қазақстан Ұлттық Банкінің Байланыс орталығына **1477** қысқа нөмірі арқылы хабарласуға болады.

1. «Қызметкермін» деген қоңыраулар

Алаяқтар банк, полиция, прокуратура, экономикалық тергеу, пошта, ұялы байланыс операторлары, коммуналдық қызмет және басқа органдардың қызметкерлері болып танысады. Олар «күдікті операциялар», «бұзу», «есептегіштерді жаңарту», «нөмірді ұзарту», «сәлемдеме алу» туралы айтып, кодты айтуыңызды немесе ақша аударуыңызды сұрайды.

Кеңестер:

- Құпиясөздерді, PIN, CVV және SMS-кодтарды ешқашан айтпаңыз.
- Телефонды қоя салыңыз да, банкке өзіңіз қайта қоңырау шалыңыз.
- Барлық ақшаңызды бір картада сақтамаңыз.
- «Қауіпсіз шоттар» болмайды.
- Мессенджерлердегі суреттерге, формаларға, логотиптерге сенбеңіз.
- Ресми органдар азаматтарға WhatsApp арқылы қоңырау шалмайды және тергеу жүргізбейді.

2. «Туысыңыз қоңырау шалды» деген алдау

Алаяқтар таныс адамның даусын қолдан жасап, «жедел» ақша аударуды сұрайды: емге, айыппұлға, «құтқару» үшін.

Кеңестер:

- Таныс адамның нақты нөміріне өзіңіз хабарласыңыз.
- Тек ол білетін сұрақ қойыңыз.
- Егде жастағы туыстарыңызды ескертіңіз — олар басты нысана.

3. Фишингтік SMS және сілтемелер

Алаяқтар «1414», «Egov», «QazPost», «E-Salyk», Ұлттық Банк атынан жалған хабарламалар жібереді. Онда жалған сайтқа сілтеме немесе жеке деректерді енгізу өтініші болады.

Кеңестер:

- SMS, мессенджер, e-mail арқылы келген сілтемелерге өтпеңіз.
- Жеке мәліметтер мен карта деректерін бейтаныс сайттарға енгізбеңіз.
- Сенімді антивирус қолданыңыз.

4. Вирустық бағдарламалар

Алаяқтар зиянды қосымшалар мен баннерлер таратады: олар телефоныңызды бұғаттап немесе деректеріңізді ұрлайды.

Кеңестер:

- Қосымшаларды тек ресми дүкендерден жүктеңіз (Play Market, App Store).
- Пікірлерді және әзірлеушінің атын тексеріңіз.
- Күдікті сайттарға кірмеңіз, файл жүктемеңіз.
- Бейтаныстардың өтініші бойынша ештеңе орнатпаңыз.

5. Жалған интернет-дүкендер

Алаяқтар kaski.kz, Wildberries, temu сияқты танымал дүкендерді көшіріп, жалған сайттар жасайды.

Кеңестер:

- Тек тексерілген сайттардан сауда жасаңыз.
- Сайттың мекенжайын мұқият тексеріңіз (бір әріп, таңба айырмашылығы болуы мүмкін).
- Сатушы туралы пікірлерді оқыңыз.
- Бейтаныс шоттарға алдын ала төлем жасамаңыз.

6. Жеңіл табыс уәделері

Алаяқтар жалған суреттер мен танымал тұлғалардың атын пайдаланып, «тәуекелсіз инвестиция», «қазір салыңыз, көп пайда табасыз» деп сендіреді.

Кеңестер:

- Тәуекелсіз тез пайдаға сенбеңіз.
- Күмән туса, сөйлесуді тоқтатыңыз.
- Компания туралы ресми дереккөздерден тексеріңіз.
- «Комиссияға», «активацияға» ақша жібермеңіз.

7. Жалған қайырымдылық ұйымдары

Төтенше жағдайлар кезінде «емге көмектесіңіз», «үйсіз қалды», «баланың операциясы қажет» деген жалған хабарламалар таратады.

Кеңестер:

- Бейтаныс сілтемелер арқылы ақша аудармаңыз.
- Ұйымды ресми сайтынан тексеріңіз.
- Тек белгілі қорлар арқылы көмек көрсетіңіз («Красный полумесяц», «Халық» қоры және т.б.).

8. «Сіз ұттыңыз!»

«Сіз ұтыстың жеңімпазысыз!» деп хабарласып, «сыйлық алу үшін» комиссия, салық немесе жеткізу ақысын төлеуді сұрайды.

Кеңестер:

- Мұндай хабарламалардағы сілтемелерге өтпеңіз.
- Жеке деректеріңізді бейтаныс сайттарға енгізбеңіз.
- Сыйлық үшін ешқашан ақша төлемеңіз.

9. Жалған жұмыс пен бизнес ұсыныстары

Алаяқтар «жоғары жалақы», «қашықтан жұмыс» немесе «пайдалы серіктестік» ұсынып, «тіркелу ақысын», «оқу ақысын» сұрап, жоғалып кетеді.

Кеңестер:

- Спам-хабарламалардағы сілтемелерге өтпеңіз.
- Жұмысқа тұру немесе «бизнеске кіру» үшін ақша төлемеңіз.
- Жұмыс берушіні ресми көздерден тексеріңіз.

Алаяқтық туралы хабарлау үшін:

<https://qamqor.gov.kz/> сайтындағы «Полицияға өтініш беру» бөлімі арқылы немесе 102 нөміріне қоңырау шалыңыз.

Қосымша ақпаратты ІІМ Киберқылмысқа қарсы күрес департаментінің Instagram парақшасынан табуға болады: <https://www.instagram.com/cybercrime.kz/>.