Как защититься от мошенников

Общие правила безопасности:
•Проверяйте информацию только через официальные источники.
•Не торопитесь выполнять просьбы по телефону или в сети интернета.
•Используйте сложные пароли и двухфакторную аутентификацию.
•Регулярно обновляйте приложения и операционную систему на гаджетах.

Если стали жертвой мошенников:
• Немедленно обратитесь в полицию по номеру 102 либо через сайт https://qamqor.gov.kz/ - вкладка «Подать заявление в полицию».
• Заблокируйте карту через банк или банковское приложение, если были попытки списания.
• Для оказания помощи, можете обратиться на единый номер дозвона 116.

Номера телефонов банков второго уровня для блокировки карты: **Forte bank** номер 7575, **Kaspi bank** номер 9999, **Халык банк** номер 9595, **Jusan bank** номер 7711, **Bereke bank** номер 5030, **Банк ЦентрКредит** номер 505, **Home Credit Bank** номер 7979, **Алтын банк** номер +77273565777, **Евразийский банк** номера +77710007722 (Beeline), +77000007722 (Tele2/Altel), +77020007722 (Kcell/Activ), **Bank RBK** номер 7888, **Банк Фридом Финанс Казахстана** номер 595, **Банк ВТБ** номер 5050, **Нурбанк** номер 2552, номер **Заман Банк** 4077, **Исламский банк «Al Hilal»** номер +77272330000, **Шинхан Банк** номер 2468, **Банк Китая в Казахстане** номер +77272585510 вн.1140, 1153.

Важно! Вы можете заблокировать банковский счет мошенников через Антифрод-центр, сообщив информацию в банк либо обратившись в полицию.

Дополнительная информация:
В случае возникновения вопросов или необходимости консультации, можно обратиться в Контакт-центр Национального Банка Казахстана по короткому номеру 1477.

1. ***Звонок от «сотрудников и организаций»***
Мошенники подставляются работниками банка, полиции, прокуратуры, служб экономических расследований, почты, сотовых операторов, коммунальных служб и других госорганов.
Говорят о «подозрительных операциях», «взломе», необходимости обновить счетчики, продлить действие номера телефона, получении посылки
и просят сообщить код или перевести деньги.
Советы:
•Никогда не сообщайте пароли, PIN, CVV и коды из SMS.
•Кладите трубку телефона и звоните в банк сами.
•Не храните все деньги на одной банковской карте.
•Никаких «безопасных счетов» не существует.
•Не доверяйте фото, формам, логотипам и «званиям» в мессенджерах.
•Официальные органы НЕ звонят на ватсап-номера граждан и НЕ ведут следственные действия по телефону.

2. ***Звонок от «родственника» может быть обманом***
На телефон звонят мошенники и путем подделки голоса знакомого Вам человека просят «срочно» перевести деньги на лечение, штраф, «спасение».
Советы:
•Позвоните близкому человеку на его настоящий номер.
•Задайте вопрос, на который знает ответ только он.
•Предупредите пожилых родственников, именно они основные жертвы таких схем.

3. ***Фишинговые SMS и сообщения со ссылками***
Приходят поддельные сообщения, которые выглядят как официальные уведомления от банков, магазинов и других организаций («1414», «Egov», «QazPost», «E-Salyk», Нацбанк и т.д.) со ссылкой на поддельный сайт или просьбой предоставить конфиденциальную информацию граждан.
Советы:
•Не переходите по ссылкам из СМС, мессенджеров и e-mail и не отвечайте на них.
•Не вводите данные карты или личную информацию на незнакомых сайтах.
•Установите надёжный антивирус.

4. ***Вирусные программы***
Мошенники распространяют вредоносные приложения и баннеры:
они блокируют телефон или крадут ваши данные.
Советы:
•Скачивайте приложения только из официальных магазинов *(Play Market, App Store)*.
•Проверяйте отзывы и имя разработчика.
•Не заходите на подозрительные сайты и не скачивайте файлы с них.
•Не устанавливайте ничего по просьбе незнакомцев, даже если «помогают настроить телефон».

5. ***Поддельные интернет-магазины***
Злоумышленники создают фальшивые сайты, копирующие популярные магазины *(например, kaspi.kz,* Wildberries, temu и др*)*.
Советы:
• Совершайте покупки только на проверенных сайтах с хорошей репутацией.
•Проверяйте адрес сайта, подделки могут отличаться одной буквой или символом.
• Читайте отзывы и рейтинг продавца.
•Никогда не делайте предоплату на незнакомые счета или карты.

6. ***Обещания легких денег***
Мошенники, в т.ч. используя поддельные изображения известных людей, убеждают Вас инвестировать деньги под предлогом «инвестиций без риска», «вложите сейчас и получите огромную прибыль», «Это честная сделка, нужно только перевести деньги».
Советы:
•Не верьте рекламе о быстрых доходах без рисков, это уловка.
•Прекратите общение при первых подозрениях.
•Перепроверяйте информацию о компании через официальные источники и отзывы.
•Не переводите деньги «на комиссии» или «для активации».

7. ***Фальшивые благотворительные организации***
Во время бедствий, трагедий или новостей о чьей-то беде мошенники рассылают просьбы о помощи: «Пожертвуйте на лечение», «Семья осталась без дома», «Ребёнку нужна операция» и т.д.
Советы:
•Не переходите по ссылкам из СМС и мессенджеров и не переводите деньги.
•Проверяйте организацию через официальный сайт или доверенные источники.
•Делайте переводы только через известные фонды (Красный Полумесяц, «Халык» и т.д.).

8. **«Вы выиграли приз!»**
Пишут или звонят: «Вы стали победителем розыгрыша!»
Чтобы получить «приз», просят оплатить комиссию, налог или доставку.
Советы:
•Не переходите по ссылкам из таких сообщений.
•Не вводите личные данные на неизвестных сайтах.
•Не переводите деньги за участие, налог или доставку.

9. ***Трудоустройство и бизнес***
Обещают высокую зарплату, удалённую работу или выгодное партнёрство. Просят оплатить «регистрацию», «комиссию» или «обучение» и исчезают
Советы:
•Не переходите по ссылкам из спам-сообщений и сомнительных объявлений.
•Не переводите деньги за трудоустройство, доступ к базе вакансий или «вход в бизнес».
•Проверяйте работодателя и сайт компании в открытых источниках.
Куда сообщить о мошенничестве? На стартовой странице сайта https://qamqor.gov.kz/ через вкладку «Подать заявление в полицию» либо позвонить в полицию по номеру 102.
Дополнительные сведения о новых видах мошеннических схем вы можете найти на официальной странице Департамента по противодействию киберпреступности МВД в Instagram (https://www.instagram.com/cybercrime.kz/).

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:

- Дереу 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 kaspi.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/.

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи», удостоверенный посредством электронной цифровой подписи лица, имеющего полномочия на его подписание, равнозначен подписанному документу на бумажном носителе.

Согласовано
08.09.2025 16:01 Нурбаев Айдос Аскарович

08.09.2025 16:09 Мадиярова Асем Канатовна

Подписано
08.09.2025 19:29 Ашыкбеков Ерлан Таскынбекович