



**ONLINEBANK**  
by Halyk

**Ақпараттық  
қауіпсіздік**



# Алаяқтардан қорғау



Алаяқтық мәселелері бойынша нақты мысалдармен қызметкерлерді жүйелі түрде оқытыңыз

## Пошта

Қызметкерлерді поштамен жұмыс істеуге және жіберушілердің мекенжайларының, сондай-ақ сенімсіз дереккөздерден алынған файлдар мен сілтемелердің шынайылығын қажетті тексеруге үйретіңіз.

## Әлеуметтік инженерия

Әлеуметтік инженерия белгілерін, мысалы, телефон арқылы манипуляция немесе жеке деректерді сұрауды тануға үйретіңіз.

## Сұхбаттасушының жеке басы

Сұхбаттасушының жеке басын, әсіресе, әдеттен тыс сұраулар жасағанда (Полиция, Ұлттық банк жәнет.с.с.) тексеріңіз және жеке деректерді хабарламаңыз.

# Киберқауіпсіздік



## Маңызды әрекеттер

- Ұйым ішіндегі ақпаратқа қолжетімділікті шектеңіз
- Onlinebank-ті пайдаланатын барлық құрылғыда тек **лицензиялық бағдарламалық жасақтаманы** және антивирус базасын пайдаланыңыз және ұдайы жаңартыңыз.  
Қауіпсіздікті жоғарылату үшін әр 10 минут сайынавтожаңартуды орнатыңыз
- Әлеуметтік желілерде өзіңіздің жеке ақпаратыңызды жарияламаңыз
- Маңызды бизнес жүйелерге кіру үшін **қосфакторлы аутентификацияны** пайдаланыңыз
- Ешкімге өзіңіздің компьютеріңізге және жұмыс кеңістігіңізге кіруге рұқсат бермеңіз, ал кетіп бара жатқанда **компьютеріңізді бұғаттаңыз**.



Компания жүйелерінде жұмыс істеген кезде жеке есептік жазбаларды және сенімді парольдерді пайдаланыңыз

# Жеке қауіпсіздік



Заңмен рұқсат етілген орындарда бейнебақылау камераларын орнатыңыз



Қолжетімділікті бақылау және басқару жүйесін (ҚБЖ) орнатыңыз



Офиске барлық келушінің жазбасын жүргізіңіз



Конфиденциалды құжаттарды бекітілетін сөреде/сейфте сақтаңыз



Басып шығарылған конфиденциалды құжаттарды қағаз ұсақтағыштан өткізіп жойыңыз



Сондай-ақ, офисіңізді қауіпсіздендіру үшін оны күзеті бар үйжайға орналастыруға болады

# Электрондық пошта хаттарындағы вирус

Ақпараттық қауіпсіздік саласындағы жағымсыз трендтер

Алаяқтар контрагенттің, банктің немесе мемлекеттік органдардың атынан компанияның қызметі немесе бұзушылықтары туралы ақпаратпен хат жіберуі мүмкін.

**Хаттың тіркемесінде ашқан кезде іске қосылатын вирус болуы мүмкін.**

Ол антивирустарға байқалмай, төлемдер, шоттардың нөмірлері, парольдер және т.б. секілді конфиденциалды ақпаратты жинап, қаскүнемдерге/ алаяқтарға беруі мүмкін.

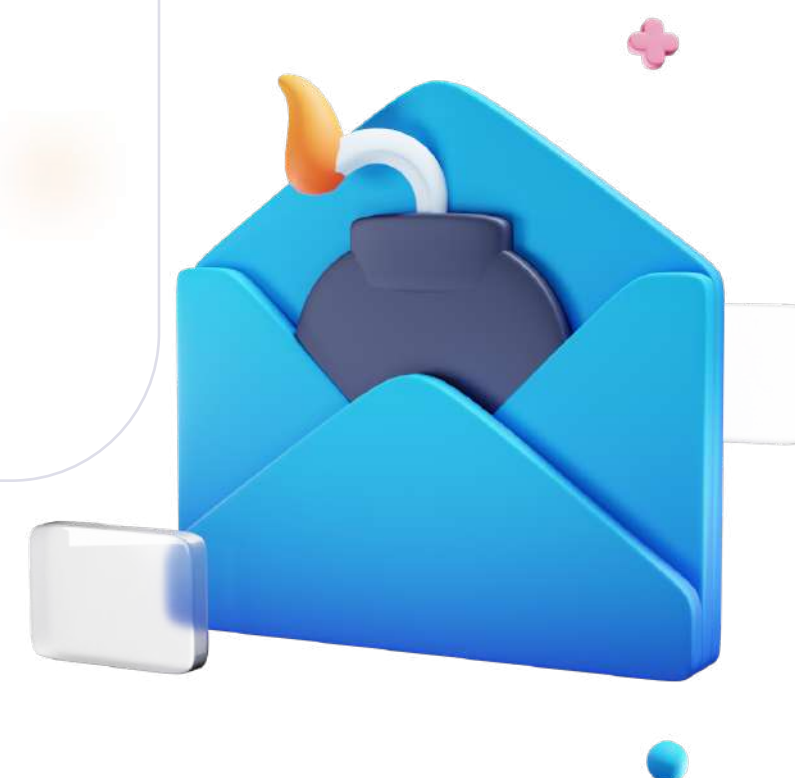
Вирус төлемдердің сомаларын және алушылардың деректемелерін өзгертуі немесе ақпаратты ұрлауы және төлемді жіберу кезінде интернет-банкінгіті басқаруы және т.б. үшін қаскүнемдерге сіздің құрылғыңызға қашықтан қолжеткізуді беруі мүмкін.



# Сенімсіз аутсорсингтік компания

Ақпараттық қауіпсіздік саласындағы жағымсыз трендтер

Сіз компьютерлер мен жүйелерді әкімшілендіру және қызмет көрсету үшін жалдаған компания сенімсіз болыпшықты. Өз міндеттерін орындау кезінде олардың өкілі вирус жұқтырған флэшканы қосып, вирус сіздің компьютеріңізге берілді.



# Үшінші тұлғалардың қол жеткізуі

Ақпараттық қауіпсіздік саласындағы жағымсыз трендтер

Сіздің компанияңыздың қызметкерлері ақпараттық қауіпсіздікке жеңіл-желпі қарайды және парольдер жазылған қағаздарды жұмыс орындарында қалдырып кетеді.

Оның үстіне, клинингтік компания сіздің офисіңізге кіре алады және олардың қызметкерлері тазалау жұмыстарын жүргізу кезінде қызметкердің есептік жазбасының паролін алуы мүмкін. Бұл деректер интернеттегі қаскүнемдерге сатылып, олар сіздің желіңізге кибершабуыл жасау үшін пайдалануы мүмкін.

Басшы қызметкеріне сеніп тапсыратын электрондық цифрлық қолтаңбаға (ЭЦҚ) қатысты немқұрайлылық, бұлоған басшының атынан құжаттарға қол қоюға мүмкіндік береді. Бұл жалған мәмілелер жасау және шоттарды басшының ЭЦҚ-мен қол қойып қолдан жасау сияқты заңсыз әрекеттерге әкелуі мүмкін.

Егер қаскүнемдер ЭЦҚ-ға қол жеткізсе, сіз компанияның шоттарындағы барлық қаражатты және компанияның өзін жоғалтуыңыз мүмкін, өйткені олар сіздің ЭЦҚ көмегімен құжаттарды қайта рәсімдеуі мүмкін.

# ONLINEBANK-пен жұмыс істеу кезіндегі қауіпсіздік

## Кіру құрылғылары

- Үшінші тұлғаларға бермеңіз
- Өзіңіз болмаған кезде компьютерге қосылулы қалдырмаңыз

## Жеке немесе жұмыс поштасы

- Жіберушінің мекенжайын тексеріңіз және шұғыл талаптардан сақ болыңыз
- Күдікті сілтемелерді баспаңыз және күмәнді файлдарды ашпаңыз

## БЖ және Антивирус

- Қашықтан басқаруға арналған бағдарламаны орнатпаңыз (TeamViewer, AmmyyAdmin, AnyDesk, RustDesk және басқалары)  [onlinebank.kz](https://onlinebank.kz)  [halyk.onlinebank.kz](https://halyk.onlinebank.kz)
- Сайттың шифрланған байланысы және түпнұсқа сертификаты бар екенін тексеріңіз.
- Onlinebank қолданатын барлық құрылғыда тек лицензиялық бағдарламалық жасақтаманы және антивирус базаларын ғана пайдаланыңыз және ұдайы жаңартып отырыңыз. Қауіпсіздікті жоғарылату үшін әр 10 минут сайына автожаңартуды орнатыңыз.
- Microsoft Edge браузерінде SmartScreen Windows Defender сүзгісін пайдаланыңыз



# ONLINEBANK –тегі қауіпсіздік бойынша ұсыныстар

## Операцияларды бақылау

- Onlinebank орнатыңыз және шот бойынша қозғалыстар туралы хабарлауды қосыңыз
- Қол қоюдың бірнеше деңгейін орнатыңыз (1-ші қол қою құқығы – Директор және 2-ші қол қою құқығы – Бас Бухгалтер)
- Қосымша пайдаланушыны Onlinebank қосымшасының «ТАҒЫ» бөлімінде қосуға болады

## Серіктестерге мұқият болыңыз

- Серіктестеріңіздің жаңа деректемелерін алған кезде олармен хабарласуды және деректемелердің өзгергенін растауды ұсынамыз



## Күдіктенесіз бе? Қоңырау шалыңыз!

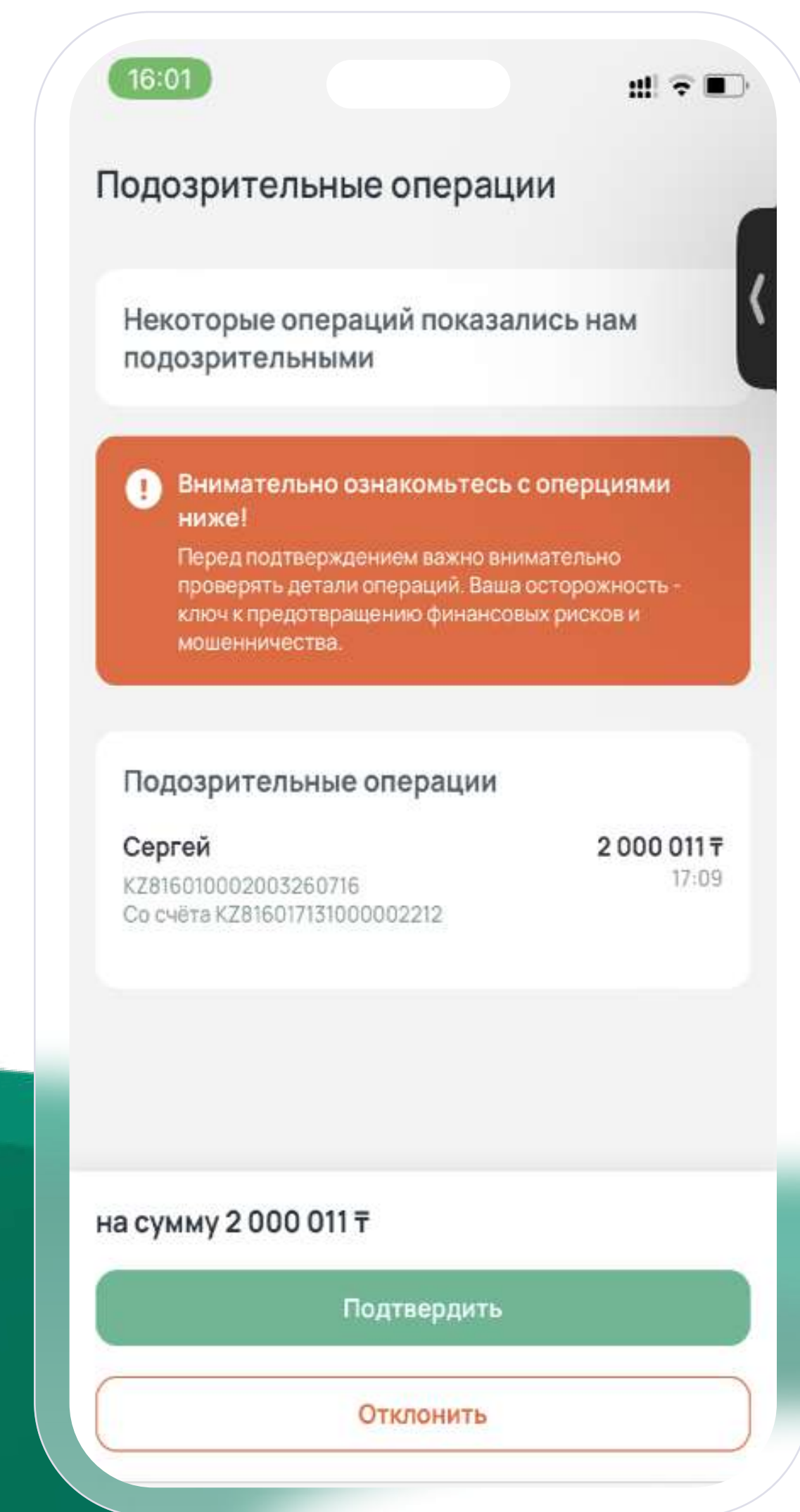
Бекітілмеген транзакциялар жүргізілген жағдайда Банктің Байланыс орталығына хабарласыңыз

### ЗТ және ЖК арналған Байланыс орталығы

- 9595 (мобильді телефоннан тегін)
- 8(727)259-07-77 (Алматы қ)
- 8 8000 8000 59 (Қазақстан бойынша тегін)

# Күмәнділікке тексеру

- **Налык фрод-талдау жүйесінің көмегімен барлық операцияны алаяқтыққа тексереді жәнеталдайды**
- Егер операциялар бойынша күдік туындаса, қосымша тексеру үшін Біз төлемдерді растау үшін SMS/Push-хабарлама жіберуіміз мүмкін немесе сізге қоңырау шалуымыз мүмкін.
- Егер Сізге SMS/Push-хабарлама келмесе, Банк бөлімшесінде сенімді нөмірді енгізіңіз
- Растауды күту уақыты – 30 минут
- Әрі қарай операцияны растау үшін Банк операторы Сізге қоңырау шалады



# AppStore және Google Play сервисіндегі фэйк қосымшалар

- Onlinebank қосымшасын жүктеген кезде оның иесі **JSC Halyk Bank** екенін тексеріңіз. Егер иесі басқа болса, бұл алдап, ақша ұрлағысы келетін алаяқтар
- SMS-пен келген немесе мессенджерлерде бейтаныс жіберушілерден келген сілтеме бойынша қосымшаны жүктемеңіз
- Қосымшаға берілген бағалар мен рейтингісіне және пікір қалдыру мүмкіндігіне қараңыз
- Заңды қосымшалар «Деректердің қауіпсіздігі» бөлімінде өз функцияларын әрдайымсипаттайды. Осы бөлімнің болуын тексеріңіз.

4:45 PM

←

Onlinebank для Бизнеса  
JSC HalykBank

4,8 ★  
5 тыс. отзывов

56 МБ

3+

Установить

ONLINEBANK by Halyk

Суперприложение для вашего бизнеса

Новый Onlinebank

Ведите бизнес в онлайн • Легко

Описание

Мобильное суперприложение для бизнеса

Финансы

Банковские услуги

Безопасность данных

Чтобы контролировать безопасность, нужно знать, как разработчики собирают ваши данные и передают их третьим лицам. Методы обеспечения безопасности и конфиденциальности могут зависеть от того, как вы используете приложение, а также от вашего региона и возраста. Информация

Бейнематериал және қосымша туралы ақпарат бар

Иесінің дұрыс атауы

Баға қою және пікір жазу рұқсат етілген

4:46 PM

←

Onlinebank для Бизнеса  
Colo Nel  
Есть реклама

11 МБ

3+

Установить

Реклама • Похожие приложения

Робот Займер Казахстан 4,4 ★

BCC Business 4,0 ★

KZ Онлайн кредит на карту

За от 5,0

Описание

Мобильное супер приложение для бизнеса

Финансы

Новый Onlinebank

Ведите бизнес в онлайн • Легко

Регистрируйте ИП  
Открывайте счета для ИП/ООО

Иесі түсініксіз

Бағалау мен пікірлер жабық

Қосымша туралы қосымша мәліметтер жоқ

Деректердің қауіпсіздігі туралы бөлім жоқ