



**FREEDOM  
BROKER**

**АЛАЯҚТАРДЫҢ АЙЛАЛАРЫНА  
ҚАЛАЙ ТҮСІП ҚАЛМАУҒА БОЛАДЫ**

### Қоңырау шалып отырған адамның алаяқ екенін қалай түсінуге болады

#### Құпия ақпаратты сұрайды.

Банк картасының деректері, қаржы операциялары туралы ақпарат, жеке деректер, парольдер, логиндер және т.б.

**Асықтырып, үрей туғызады.** Дереву әрекет ету керек, әйтпесе



"Смс-тегі үш таңбалы кодты хабарлаңыз..."



AAAAaaaa

#### Жасанды қауіп төндіреді.

Талаптарды орындамаған жағдайда ақшаны жоғалтумен, заңды, қаржылық және кредиттік салдармен қорқытады.

«ҚК 125 бабына сәйкес...».

**Күрделі терминологияны пайдаланады.** Шатастыру үшін жоқ заңдар мен банктік рәсімдерге сілтеме жасайды.

### Алаяқтар нені пайдалана алады



#### Сенімсіздік.

Егер сіз банк істерін нашар білетін болсаңыз немесе сервистер қалай жұмыс істеуі керектігіне сенімсіз болсаңыз, алаяқтар оны пайдалана алады.

#### Жылдам және

оңай ақша табу ниеті Егер сізге жеңіл ақша, мысалы, үлкен ұтыс немесе күтпеген бонус уәде етілсе, бұл тұзақ болуы мүмкін.

#### Жаңғалақтық.

Егер қолыңыз бос болмаса немесе асығыс болсаңыз, алаяқтар сізді шатастыруға немесе ойланбаған іс жасауға мәжбүрлеуге тырысуы мүмкін.

#### Ақшадан айырылу қорқынышы.

Егер сізге жинақ ақшаңызға қауіп төніп тұрғанын және тез арада бірдеңе істеу керектігін айтса, бұл сізді ойланбастан әрекет етуге мәжбүрледің жолы болуы мүмкін.

### Телефон алаяқтарынан қалай қорғануға болады



1.

**Кез келген ақпаратты тексеріңіз.** Егер сізге банк немесе басқа ұйым атынан қоңырау шалынса, талаптарын орындауға асықпаңыз. Ақпаратты растау үшін компанияның ресми нөміріне қоңырау шалыңыз.



2.

#### Бас тартудан қорықпаңыз.

Егер күмән туса, кез келген ұсыныстардан немесе талаптардан сенімді түрде бас тартыңыз.



3.

#### Қысыммен әрекет етпеңіз.

Қысым немесе үрей сезінетін болсаңыз, ешқандай әрекет жасамаңыз және жеке мәліметтерді ұсынбаңыз.

5.

#### Құпия ақпаратты ұсынбаңыз.

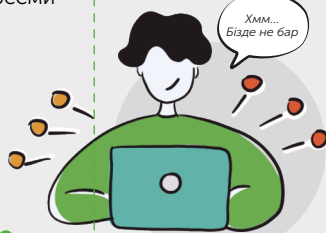
Мысалы, парольдер немесе ПИН-кодтар. Адал ниетті компаниялар мен сервистер мұндай ақпаратты ешқашан сұрамайды, өйткені бұл цифрлық қауіпсіздік талаптарына қайшы



4.

#### Алаяқтардың әдістерін зерттеңіз.

Алаяқтықтың негізгі схемаларын білу үшін алаяқтардың қалай әрекет ететіні туралы оқыңыз.



6.

**Біреудің сұрауы бойынша бағдарламалық қамтамасыз етуді немесе бағдарламаларды орнатпаңыз.** Әсіресе, белгісіз нөмірден қоңырау шалынса.



# ФИШИНГТІК ХАТТАРДЫ ҚАЛАЙ ТАНУҒА БОЛАДЫ және интернетте алаяқтардан қорғану амалдары қандай

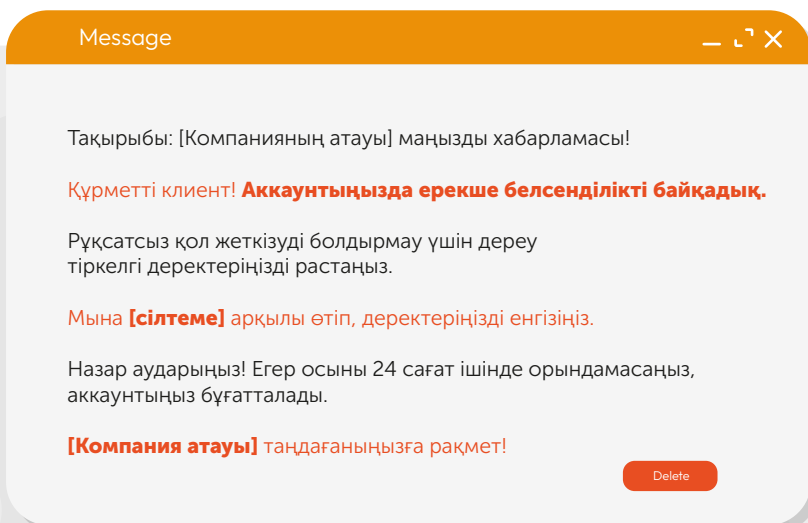
## Фишингтік хаттар дегеніміз не



Бұл қаржы ұйымдарының, сервистердің немесе тіпті достарыңыздың ресми хаттары сияқты көрінетін жалған хабарламалар. **Мұндай хаттардың мақсаты - сіздің жеке ақпаратыңызды ұрлау** (мысалы, құпия сөздер және банк карталарының нөмірлері).

## Фишингтік хаттар қалай көрінеді

- 1 Әдетте олар бірденені тез арада растауды, құпия сөзді өзгертуді немесе есеп туралы ақпаратты жаңартуды сұрайды.
- 2 Хаттарда жалған сайттарға сілтемелер болуы мүмкін, онда сізден жеке деректеріңізді енгізу сұралады.
- 3 Кейде мұндай хаттарда грамматикалық қателер болуы мүмкін (спам-сүзгілерді айналып өту үшін).



## Алаяқтықтың кең таралған схемалары



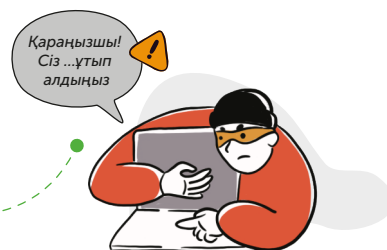
### Шотты бұғаттау туралы жалған хабарламалар.

Алаяқтар шотыңыздың бұғатталғанын және оны қалпына келтіру үшін жеке деректерді енгізуді сұрайды.



### Көмек туралы өтініштер.

Алаяқтар сіздің таныстарыңыздай болып, жедел көмек көрсету үшін ақша аударуды сұрауы мүмкін.



### Ұтыс немесе мұрагерлік туралы ұсыныстар.

Олар күтпеген ұтыс немесе мұра туралы жазуы мүмкін, бірақ алу үшін ақша төлеуге немесе жеке деректерді ұсынуға тура келеді.

## Қорғану амалы

**Күдікті сілтемелер арқылы өтпеңіз.** Егер сізге қызық хат келсе, оның ішіндегі сілтемелерді баспаған дұрыс.

yes

**Жіберушінің мекенжайын тексеріңіз.** Егер электрондық пошта мекенжайы ерекше болса, ол фишингтік хат болуы мүмкін.

yes

**Екі факторлы аутентификацияны пайдаланыңыз.** Бұл аккаунттарыңыз үшін қосымша қорғау деңгейі.

yes

**Жеке ақпаратыңызды бөліспеңіз.** Дереккөздің сенімділігіне сенімсіз болсаңыз, құпия сөздеріңізді, карта деректерін және басқа маңызды құпия сөздерді ешқашан және еш жерде енгізбеңіз.

yes

**Антивирусты пайдаланыңыз.** Компьютерде вирусқа қарсы бағдарламалық жасақтаманы үнемі жаңартып тұрыңыз.

yes

**Мұқият болыңыз.** Егер хат күдікті болып көрінсе, қаржы ұйымына тікелей қоңырау шалып, ақпаратты қайта тексерген жөн.

yes



**Есіңізде болсын:** Алаяқтық зардаптарына тап болудан гөрі, алдын ала сақтанып, ақпаратты тексерген дұрыс. Интернетте сөйлескенде сақ болыңыз.

### Фишингтік сайттар дегеніміз не

Бұл жеке деректерді (логиндерді, құпия сөздерді, банк карталарының нөмірлерін және басқа да құпия ақпаратты) ұрлау үшін жасалған қолдан жасалған веб-парақшалар. Мұндай сайттар пайдаланушыларды алдау және оларды жеке деректерді енгізуге мәжбүрлеу үшін танымал беттер мен сервистердің кейпінде болуы мүмкін.

Интернет-банкинг

Әлеуметтік желілер

Электрондық поштаға кіру парақшалары

Онлайн-дүкендер

Сауда платформалары

Корпоративтік сайттар

Жеке кабинеттер

### Алаяқтар фишингтік сайттарда пайдаланатын әдістер



#### Жалған кіру пішіндері.

Фишингтік сайттар көбінесе логин мен құпия сөзді енгізуге арналған пішіндерді қамтиды, олар шынайы болып көрінгенмен, бірақ шын мәнінде енгізілген деректерді алаяқтарға жібереді.

#### Ресми дизайнды имитациялау.

Сайттар белгілі брендтердің, қаржы ұйымдарының немесе сервистердің шынайы сайттарының дизайнын дәл көшіре алады.

#### URL мекенжайларын манипуляциялау.

Алаяқтар шын мәніне өте ұқсас URL-ді пайдалана алады. Бұл үшін олар тек бірнеше әріпті өзгерте алады (*ffln.kz орнына ffin.kz*) немесе жоғарғы деңгейдегі басқа домендік атауды (*мысалы, .net орнына .com*) пайдалана алады.

#### Жалған ұсыныстар мен акциялар.

Жеке қаражатты дереу енгізуді талап ететін сенгісіз тиімді ұсыныстар, жоғары кірістілік немесе мерзімді акциялар

#### Зиянды БҚ.

Кейбір фишингтік сайттар сіздің құрылғыңызға пайдалы бағдарламалар ретінде зиянды бағдарламалық қамтамасыз етуді орнатуға тырысуы мүмкін.

#### Жасырын қайта бағыттаулар.

Мұндай сайтқа кіру сізді басқа фишингтік немесе зиянды сайттарға жіберуі мүмкін.

### Фишингтік сайттарды қалай тануға болады



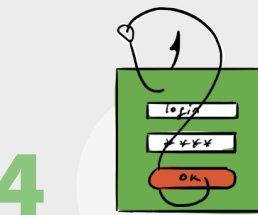
**1 URL мекенжайын тексеріңіз.** Жалған сайттар көбінесе шынайы сайттарға ұқсас, бірақ аздаған айырмашылықтары немесе қателіктері бар мекенжайларды пайдаланады.



**2 HTTPS болуы.** Қауіпсіз сайттар жіберілетін деректерді қорғауды қамтамасыз ететін HTTPS хаттамасын пайдаланады. HTTPS болмауы фишингтің белгісі болуы мүмкін.



**3 Дизайн және орфография.** Сайттағы сапасыз дизайн, грамматикалық және пунктуациялық қателер фишингті көрсетуі мүмкін.



**4 Жеке ақпаратты сұрату.** Егер сайт бірден құпия деректерді енгізуді сұраса, сақ болыңыз.

### Қалай қорғануға болады

#### Жеке деректерді енгізбеңіз

Адал ниетті компаниялардың ресми сайттары ешқашан банк карталарының барлық деректерін, басқа сервистердің логиндері мен парольдерін және басқа да жеке деректерді сұрамайды

yes

#### Фишингтен қорғау функциясы бартаңтивирустарды пайдаланыңыз.

Олар күдікті сайттарда кіргеніңізді ескерте алады.

yes

#### Екі факторлы аутентификация.

Оны мүмкіндігінше қосыңыз. Осылайша аккаунттарыңызды қосымша қорғай аласыз.

yes



**Интернетке жеке деректерді енгізгенде әрқашан мұқият және сақ болыңыз.** Егер сайттың шынайылығына қатысты күмәніңіз болса, алдын ала сақтанып, деректерді енгізбеген дұрыс.

#### Құпия сөздерді браузерде сақтамаңыз.

Сенімді құпия сөздер менеджерін пайдаланыңыз.

yes

#### Бағдарламалық жасақтаманы жүйелі түрде жаңартып тұрыңыз.

Браузеріңіз бен операциялық жүйеңіздің соңғы нұсқаларға дейін жаңартылғанына көз жеткізіңіз.

yes