

**Алаяқтар су тасқыны жағдайын азаматтарды алдау үшін пайдалануда**

*«Жеке сәйкестендіру нөміріңізді төлемдердің бар-жоғына тексеріңіз»,   
«Сілтемеге басып, 3 млн теңгеге дейін өтемақы алыңыз,», «Мемлекеттен тезірек жәрдемақы алыңыз» - әлеуметтік желілерде қаскүнемдер осындай сынды жалған ақпараттар орналастырып, Қазақстандықтардың дербес деректерін қолға түсіруге тырысып бағуда.*

*Алаяқтықтың бұл түрі жаңа емес, алайда соған қарамастан кейбір азаматтар алаяқтардың айла-шарғыларының құрбаны болып жатады. Fingramota.kz негізгі қауіпсіздік шараларын еске салады.*



**Су тасқынынан зардап шеккендерге өтемақы төленіп жатыр ма?**

Мемлекет басшысының тапсырмасы бойынша су тасқынынан зардап шеккендер жергілікті атқарушы органдардан, яғни әкімдіктерден біржолғы төлем алатын болады. Төлемдер мөлшері әр өңірде келтірілген материалдық залалды есептеу үшін құрылған арнайы комиссиялардың шешімі бойынша жеке белгіленетін болады. Ол үшін су тасқыны салдарынан айырылған мүліктің тізімдерін, залалды растайтын фото -, бейнематериалдарды, жылжымайтын мүлік объектісін идентификаттау құжаттарын және басқа да құжаттарды қоса бере отырып, әкімдіктерге өтінішпен жүгіну қажет. Өтемақы төлеу рәсімі жөнінде неғұрлым толық ақпаратты тек жергілікті атқарушы органдардан алуға болады.

**Қазақстанның барлық азаматтарына банктерден және Еңбек министрлігінен «өтемақы» төленеді**

Жалған хабарландыруларды барынша шынайы етіп көрсету үшін қылмыскерлер қазақстандық банктер мен мемлекеттік органдардың атауларын пайдаланады. Мысалы, соңғы аптада Facebook, Instagram, Telegram әлеуметтік желілерінде ҚР Еңбек және әлеуметтік қорғау министрлігінің Халық банкпен бірлесіп өтемақы төлейтіні, сондай-ақ Қаржы министрлігінің жаңа қаулысы шыққаны жөнінде хабарламалар жариялануда. Вижуалда ұйымдардың логотиптері мен брендбук элементтері, сондай-ақ Қазақстан Республикасының елтаңбасы пайдаланылады.



Алаяқтар адамдарды жаңылыстыру үшін әр жарнама постының астында «Жедел төлем үшін рақмет», «Сома сол күні түседі», «Өтінімдерді шұғыл беріңіз» деген мәтінімен боттар түсіндермелерін орналастырады.

Алаяқтардың басты мақсаты – азаматтардың «Толық» немесе «Өз өтемақымды тексеру» дегенді басып, фишингтік сілтемелерге өтуін мәжбүрлеу. Одан кейін пайдаланушы алаяқтық сайтқа тап болады, ол сайтта ақша алу үшін тіркеу ұсынылады. Ал бұл үшін ЖСН, банктік карталардың деректемелері, SMS-хабарлама сияқты дербес деректер енгізу қажет болады.

Азамат бұл талапты қалай орындайды, солай олардың деректері автоматты түрде алаяқтардың қолына түседі. Қаскүнемдер өз құрбандарының шоттарындағы бүкіл ақша қаражатын алуы мүмкін немесе «бөгдеге» кредит ресімдеуі мүмкін. Сондай-ақ күмәнді сайттарға өткеннен кейін хакерлік шабуылға тап болу тәуекелі бар, ол пайдаланушының құрылғысына шпиондық бағдарламалар орнатуға негізделеді. Алаяқтар осы қосымша арқылы онлайн-банкингке және басқа да құпия ақпаратқа қол жеткізе алады.

Рас-өтірігін атынан жалған ақпарат таратқан ұйымға жүгіне отырып білуге болады. Мысалы еңбек және халықты әлеуметтік қорғау министрлігі фейкке хабарламада көрсетілген сілмете қаскүнемдердің пайдаланушының жеке деректерін алу тәсілі болып табылады деп хабарлап жедел ден қойды. «Мемлекеттік қолдаудың тиесілі шаралары туралы ресми ақпарат 1414 нөмірінен SMS-хабарламалар арқылы ғана таратылады. Азаматтарды ресми дерекөздеріне ғана сенуге шақырамыз», - деп атап өтті ведомство өкілдері ресми релизде.

Алаяқтар кез-келген нөмірлерді, оның ішінде төрт таңбалы нөмірлерді қолдан жасай алатындығын есте ұстаған жөн, сондықтан ұйымдардың жедел желілерінің нөмірін терген кезде ешқандай жағдайда SMS-хабарлама арқылы жіберілетін нөмір бойынша қайта қоңырау шалуға немесе сілтемелерге өтуге болмайды.

**Тағы қандай қауіпсіздік ережелерін білу керек?**

* Әрқашан банктің, мемлекеттік органдардың ресми сайттарынан төлемдер туралы ақпаратты тексеріп жүріңіз.
* Өзіңіздің жеке және банктік деректеріңізді, әсіресе картаның арғы бетіндегі үш санды және оның жарамдылық мерзімін жарияламаңыз.
* Ақша туралы сөз қозғайтын бейтаныс адамдардың қоңыраулары мен хабарламаларына сенбеңіз.
* Картаңыздың 3D-Secure функциясын өшірмеңіз.
* Барлық транзакцияларды көріп отыру үшін мобильді қосымшадағы SMS- және push-хабарламаларды қосып қойыңыз.
* Электрондық поштаға және мессенджерлерге жіберілген қоса берілген белгісіз файлдарды ашпаңыз.
* Алаяқтардың сайттарына өтуге мүмкіндік бермейтін вирусқа қарсы сенімді бағдарламаны орнату қажет.
* Ақшалай қаражат тоналған жағдайда, құқық қорғау органдарына өтінішпен жүгініңіз.

***Өзіңізге, жақындарыңызға қамқорлық жасаңыз және қаржылық сауаттылығыңызды***[***Fingramota.kz***](http://fingramota.kz/)***-пен  бірге арттырыңыз!***