АҚТӨБЕ ОБЛЫСЫНЫҢ
ПРОКУРАТУРАСЫ

АҚТӨБЕ ҚАЛАСЫНЫҢ
ПРОКУРАТУРАСЫ

ПРОКУРАТУРА
АКТЮБИНСКОЙ ОБЛАСТИ

ПРОКУРАТУРА
ГОРОДА АКТОБЕ

030006, Ақтөбе облысы,
Ақтөбе қаласы, Ы.Алтынсарин көшесі, №34 үй
тел.: 8 (7132) 21-12-19, кеңсе: 8 (7132) 22-14-46
www.akt.prokuror.kz

030006, Актюбинская область,
город Актобе, улица И. Алтынсарина, дом №34
тел.: 8 (7132) 21-12-19, канц.: 8 (7132) 22-14-46
www.akt.prokuror.kz

25.01.2024 № 2-03-24-00525

Ақтөбе облысының
Білім басқармасының басшысы
Ж.И. Сұлтанға

алаяқтықпен байланысты қылмыстарды
алдын алу бойынша

Ақтөбе қаласы бойынша қабылданып жатқан шараларға қарамастан алаяқтықпен байланысты қылмыстардың саны өсуде *(а.ж. өткен кезеңінде 23,3%-ға немесе 121-ден 148-ге дейін, соның ішінде интернет-алаяқтықтар 60-тан 76-ға дейін артқан).*

Алаяқтықтардың басым бөлігі онлайн-несие рәсімдеу, «Olx.kz», «Krisha.kz» сайттары мен онлайн-дүкендері арқылы сатып алу жасау, инвестиция салу, оқуға түсіріп беру немесе біліктілік туралы сертификат алып беру және т.б. тәсілдер арқылы жасалады *(Instagram, telegram, whatsapp және т.б. желілері арқылы).*

Мысалы, белгісіз тұлға инстаграм парақшасы арқылы мемлекеттік грант алу үшін бизнес-жоспар жасап беремін деп алдап, адамның жеке мәліметтерін алғаннан кейін 200 мың теңгеге несие рәсімдеген; «Almaz Credit» атаулы телеграмм арнасынан белгісіз біреу несие алып беремін деп алдап, жәбірленушіге тиесілі 163 теңге қаражатын иемденген; өзін Ұлттық банк қызметкері деп таныстырып, жәбірленушінің атынан жалпы сомасы 1,6 млн. теңге несие рәсімдеген; «WhatsApp» арқылы белгісіз тұлға өзін туысы ретінде деп хабарласып, баласы ауырып жатқанын жалған айтып, «Kaspi» қосымшасы арқылы 30 мың теңге аудартқан.

Бұндай фактілер біршама.

Осыған орай, Ақтөбе қаласы прокуратурасы жасақтаған алаяқтықпен алдын алу бойынша 2024 жылға арналған ведомствоаралық өзара іс-қимыл жоспарына сәйкес, Білім басқармасына бағынысты барлық білім беру ұйымдарының *(мемлекеттік, жеке)* қызметкерлері мен білім алушылар арасында алаяқтық қылмыстарынан қорғану, оның алдын алу мақсатында кешенді түсіндіру жұмыстарын жүргізу қажет *(қызметкерлер, білім алушылар қатысуымен жиналыстар).*

Жүргізілген жұмыстар туралы ақпаратты *(жиналыстар хаттамасымен қоса, фотокестелер)* қала прокуратурасына **20.02.2024 ж.** жолдау сұралады.

Қосымша: буклет 10 парақта.

Ақтөбе
қаласының прокуроры **Б. Қыдырәлі**

Алаяқтармен күрес бойынша өткізілген іс-шаралар туралы есеп

№	Білім бөлімінің,білім беру ұйымының атауы	Қатысқан адам саны (педагогтар)	формат	сілтеме
1	«TUMAR»МДҰ	10	жиналыс	https://tumarbalabaksha.kz/

«TUMAR»МДҰ меңгерушісі: Прмаханова А.Ж.

«Сақтансан сақ боларсың !»

(алаяқтыққа қарсы жиналыс)

Хаттамасы

Барлығы:13

Қатысқан: 10

Қатыспаған: 3

Мақсаты: Алаяқтыққа қарсы түсіндірме жұмыстарын жүргізу,Білім басқармасына бағыныcты қызметкерлер арасында алаяқтық қылмыстарынан қорғану,оның алдын алу,интернет желісінде алданып қалмау.

Күн тәртібінде

1. Интернет алаяқтық: ауыздықтау мен алдың алудың қиындықтары-Жауапты:меңгеруші Прмаханова А.Ж.
2. Интернет алаяқтарынан қалай қорғануға болады?
3. Бір бірлерімен пікір алмасу,өз ойларын айту.

Бірінші мәселе бойынша балабақша меңгерушісі Прмаханова А.Ж.: «Мемлекет басшысы өткен жылғы Жолдауында алаяқтыққа, соның ішінде қаржы пирамидалары мен интернет алаяқтығына қатысты құқық қорғау органдарына кешенді әрі нақты шараларды әзірлеуді тапсырған. Өйткені Қазақстанда қазір интернет алаяқтығына тыйым болмай тұр. Технологияның тілін мықты меңгерген әккілердің құрығы ұзарып, алдап-арбау әдіс-тәсілдері күн санап мың құбылуда. Рас, интернет пен цифрлы технологиялардың кеңінен таралуы жаһандану құрылымын ғана емес, қылмыс әлемінің сипатын, соның ішінде қылмыс түрін түбегейлі өзгертті. Қазір бәріміздің өмірімізде цифрлы технологиялар маңызды рөл атқарады. Олардың көмегімен виртуалды қызметтер мен өнімдерге қол жеткіземіз, белгілі бір тауарларға сұраныс та артты. Бүгінде әлеуметтік желілер мен түрлі интернет платформалар тек ақпарат алмасудың емес, сауда-саттықтың негізгі алаңына айналды. Ал компьютерлендірудің салдары соңғы 10 жылдың ішінде қылмыстық құқық бұзушылық түрінде де айқын көріне бастады.Полиция мен банк қызметкері, қаржыгерлердің сан рет айтқан ескертулеріне қарамастан аңқау халық адал ақшасынан күн сайын айырылып қалып жүр.Өткен жылы елімізде интернет алаяқтыққа қатысты 21 мыңнан астам дерек тіркелген екен. Ал бұл сан 2020 жылы 14 мыңның айналасында болған. ІІМ мәліметтеріне сенсек, 1200-ден астам деректе жәбірленушілер «фишингтік» интернет-ресурстарға жеке деректерін ерікті түрде өздері енгізген. Ал 2 мыңға жуық алаяқтық түрлі жоба,

онлайн ойындар, инвестициялар мен бәс саудаларда «үлкен ұтысқа ие боласыз» деген желеумен жасалған.Жыл басталғалы екі айдың ішінде елімізде интернет алаяқтықтың 2900 дерегі тіркелген. Қарапайым халықтың ақшасын алаяқтық жолмен алдап алу қазіргі таңда ең көп тіркелетін қылмыс түріне айналғанын жеткізді. Оның айтуынша, статистикаға сәйкес еліміздегі барлық қылмыстың оннан бір бөлігі алаяқтыққа қатысты екен. «Соның ішінде, интернет алаяқтыққа құрық салу күннен-күнге қиындап барады. Уақыт талабына сай технологияның дамуымен қатар алаяқтықтың әдістері мен саны да өсіп келеді. Мұндай қылмыстарға жол бермеу, алдын алу еліміздің ғана емес, қазіргі таңда бүкіл әлем елдерінің өзекті мәселелерінің біріне айналып отыр», дейді ол.
Екінші мәселе бойынша меңгеруші Прмаханова А.Ж.: «Соңғы уақытта өзге адамның әлеуметтік желідегі аккаунтын пайдаланып, қаржылай көмек сұрайтын алаяқтардың әрекеті күшейіп кетті. Мұндай алаяқтықтың құрбандары көбейген. Бұған дейін танымал тұлғалардың, әлеуметтік желі белсенділерінің жалған аккаунттарын жасау арқылы азаматтардан ақша сұрау жиі кездесетін болса, енді алаяқтар қарапайым азаматтарға да көшкен.

Алаяқтық схемасы қарапайым: кез келген адаманың әлеуметтік желідегі жалған аккаунты жасалады. Сол арқылы оның жақын туыстарына, достарына не өзге таныстарына хат жазу арқылы белгілі бір банк картасына ақша аудару сұралады. Мұндай деректер әсіресе Telegram мессенджерін пайдаланушылар арасында жиілеген.
KZ-CERT компьютерлік инциденттерге әрекет ету қызметінің мамандары шабуылға ұшырағандардың әлеуметтік желілерде байланыс деректерінің дербестігін сақтамағанын, сондай-ақ, байланыс деректерінің еркін таралып кеткенін айтып отыр.
Осы орайда интернет алаяқтарынан сақтану үшін KZ-CERT қызметі келесі кеңестерді ұсынады:
Интернет жүйесі арқылы келген сілтеме бойынша өткен кезде мекенжай жолына, яғни, доменнің дұрыстығына, акция жүргізетін ұйымның не компанияның ресми атауындағы артық символдарға назар аудару керек.
Әлеуметтік желілердегі өз профиліңіздің дербестігін баптауларда байланыс деректерін (қызметтік және жеке телефон нөмірі) көпшілікке қолжетімді етпеген дұрыс. Мобильдік нөмірді (бизнес-аккаунт) көрсету қажет болған жағдайда, жеке және жұмыс нөмірлерін бөлу қажет, яғни, жеке нөмірді туыстармен және жақындармен байланысу үшін ғана пайдаланған дұрыс.

Есептік деректеріңізді үнемі тексеріп, көп факторлы аутентификация пайдаланылатын сенімді парольдерді қолданыңыз.
Браузерде, операциялық жүйеде және мобильдік құрылғыларда пайда болатын түрлі терезелер мен хабарламаларға қатысты абай болыңыздар.
Банк картаңыздың деректерін сақтап, картаның сыртқы жағындағы 3 санды CVV/CVC-кодын ешкімге айтпаңыз. Сондай-ақ, банктен келіп түсетін SMS-кодты ешбір жағдайда бейтаныс жандарға хабарламаңыз.
Интернетке қол жеткізудің ашық қоғамдық Wi-Fi-нүктелеріне сенбеңіз, сонымен қатар өз аутентификациялық деректеріңізді қорғалмаған сымсыз желілер арқылы енгізбеуге тырысыңыз.
Бопсалаушылардың телефон бойынша талаптарын орындамаңыз, ал егер Сіз интернет-алаяқтардың құрбаны болсаңыз ең жақын полиция бөліміне немесе 102 телефоны арқылы дереу жүгініңіз.
Жеке деректерді, жеке куәлік деректерін, банк карталарының деректерін және тағы басқа мәліметтерді қамтитын құжаттарыңыздың көшірмелері бен банк картасының суретін ешкімге жібермеңіз.
Күдікті интернет-ресурстар немесе ақшалай пайдаға үміттендіретін сілтемелер айқындалған жағдайда KZ-CERT қызметіне (1400 (тәулік бойы) нөмірі, қызмет сайты, Telegram мессенджеріндегі "ҚР ақпараттық қауіпсіздігі" тобына не жеке хабарлама жіберу арқылы) хабарлаңыз.

Сақтық шаралары және қорғаныс

- Жеке ақпаратты бергенде абай болыңыз. Құпия сөздер, банк ақпараты немесе несие картасының нөмірлері сияқты жеке ақпаратты ешқашан электрондық пошта арқылы немесе сенімсіз веб-сайттарда бермеңіз. Веб-сайт мекенжайларын тексеріңіз және олардың HTTPS арқылы қорғалғанына көз жеткізіңіз.

- Электрондық хаттар мен сілтемелерді ашқанда сақ болыңы

- Белгісіз жіберушілердің электрондық пошталарын ашпаңыз немесе күдікті сілтемелерді баспаңыз. Әсіресе электрондық пошта немесе сілтеме жеке ақпаратты немесе қаржылық транзакцияларды сұраса, сақ болыңыз.

- Сенімді антивирустық бағдарламалық құралды пайдаланыңыз. Құрылғыларыңызға сенімді антивирустық бағдарламалық құралды орнатыңыз және оны жүйелі түрде жаңартыңыз. Бұл сізді зиянды

бағдарламалардан қорғауға және күдікті веб-сайттарға кіруге тыйым салуға көмектеседі.

- Қаржылық операциялар мен есептерді қадағалаңыз. Қаржылық транзакцияларыңыз бен есептерді жүйелі түрде қарап шығыңыз. Күдікті әрекетті немесе рұқсат етілмеген транзакцияларды байқасаңыз, дереу банкке немесе қаржы мекемесіне хабарласыңыз.

- Білім және хабардарлық. Интернеттегі алаяқтықтың әртүрлі түрлерін және өзіңізді қалай қорғау керектігін жақсы біліңіз. Интернеттегі алаяқтықтың алдын алу бойынша ұсыныстар мен кеңес беретін ресми ақпарат көздеріне немесе мамандандырылған ұйымдарға жүгініңіз.

Қорыта айтқанда, интернеттегі алаяқтық Қазақстанда үлкен қауіп болып табылады, бірақ дұрыс сақтық шаралары мен ақпараттандыру шаралары арқылы сіз өзіңізді және қаржылық мүдделеріңізді қорғай аласыз. Жеке ақпаратты беру кезінде сақтық, сенімді антивирустық бағдарламалық құралды пайдалану желідегі алаяқтықты болдырмаудың негізгі факторлары болып табылады. Бұл мәселемен күресуде білім мен хабардарлық та маңызды рөл атқарады.

Сол сияқты, Ұлттық Банктің kazcoins.nationalbank.kz интернет-дүкенінің сатып алушыларына сатып алынатын коллекциялық монеталар санына қойылған шектеулерді айналып өту үшін арнайы бағдарламалық қамтамасыз етуді сатып алуды ұсынатын алаяқтардың белсендірілгені туралы ескертеді. Осылайша, мессенджерлерде және әлеуметтік желілерде Қазақстан нумизматтарының тақырыптық топтарындағы алаяқтар Ұлттық банк интернет-дүкенінің қоржынына коллекциялық монеталарды автоматты түрде қосатын «ассистенттік бағдарламаға» бір реттік кіруді ақылы түрде (кез келген мөлшерде) ұсынады.

Интернет-алаяқтық көптеген елдерде, соның ішінде Қазақстанда да кездесетін күрделі мәселе. Интернеттегі алаяқтық түрлеріне фишинг, картамен алаяқтық, кибер бопсалау және т.б. жатады. Алаяқтар жалған электрондық пошталарды, веб-сайттарды және әлеуметтік желілерді қолданатын сенімді ұйымдар мен жеке тұлғалар ретінде көрінеді. Қазақстанда қаржылық алаяқтық пен киберқылмыспен байланысты мыңдаған интернет-алаяқтық фактілері тіркеліп жатыр. Дегенмен, көптеген алаяқтық

жағдайлары тиісті орындарға хабарланбайды, сондықтан нақты сандар одан да көп болуы мүмкін. Өзіңізді онлайн алаяқтықтан қорғау үшін жеке ақпаратты беру кезінде абай болу, күдікті электрондық пошталар мен сілтемелерді ашпау, сенімді антивирустық бағдарламалық құралды пайдалану және қаржылық транзакцияларыңызды жүйелі түрде тексеру маңызды. Білім және алаяқтық туралы хабардар болу да онлайн алаяқтардан қорғауда маңызды рөл атқарады.

Шешімі:

1. Ешқандай жеке деректерді ешкімге жібермеу керек.
2. Банк картасының нөмерлерін,смс хабарламаларын ешкімге жібермеу.
3. Алаяқтыққа қарсы жұмыстар жүргізілсін.

Төрайымы: Прмаханова А.Ж.

Хатшысы: Берманова Ж.С.