Астана қаласының полиция департаменті

Киберқылмыспен күресу

Интернеттегі алаяқтықтың негізгі түрлері

БАНКТЕР немесе мемлекеттік органдар атынан қоңырау шалу

Алаяқтар алдау мақсатында дауыстар мен беттерді бұрмалау үшін жасанды интеллектті қолдану арқылы өздерін мемлекеттік қызметкерлер немесе банк қызметкерлері ретінде таныстырып күдікті операциялар туралы ескертеді.
Құқық қорғау органдары телефон арқылы сізден ештеңе талап етпейтінін есте ұстаған жөн.

ФИШИНГ САЙТТАРЫ:

Алаяқтар сіздің деректеріңізді жинау үшін жалған сайттар жасайды, әсіресе хабарландыруларда тауар сатып алу кезінде курьерлік жеткізумен байланысты бейтаныс сілтемелерге өтпеңіз.

ИНСТАГРАМДАҒЫ САУДА АЛАЯҚТЫҚТАРЫ:

Қазіргі уақытта Instagram дүкендерінде онлайн-сатып алулар танымал бола бастады, алаяқтар жалған дүкендер құрып, алдын-ала төлемді талап етіп, жоғалып кетуде.
Сатушыларды мұқият тексеріп, тым төмен бағаларға сенбеу және ақша аударымдарын жасамағаныңыз жөн

САУДА ПЛАТФОРМАЛАРЫНДАҒЫ АЛАЯҚТЫҚ:

Алаяқтар тауар үшін алдын-ала төлем алған соң мүлтіксіз жоғалып кетеді.
Алдын ала төлем жасамас бұрын тауарды өз қолыңызбен ұстап тексеріңіз.

ИНВЕСТИЦИЯЛЫҚ СХЕМАЛАР:

Алаяқтар сізге жоғары кірісті уәде етіп, криптовалютаға немесе акцияларға инвестиция салуды ұсынуы мүмкін.
Бастапқыда олар сізге аз мөлшерде ақша қайтаруы мүмкін, бірақ содан кейін сіздің инвестицияңызды көбейтуді сұрап, ақшаңызбен жасырынып кетеді.

WHATSAPP ТІРКЕЛГІСІН БҰЗУ:

Алаяқтар сіздің жеке аккаунтыңызға рұқсатсыз кіру үшін зиянды сілтемелерді пайдаланады, содан кейін Сіздің атыңыздан қаржылай көмек сұрауларын жібереді.
Қауіпсіздікті қамтамасыз ету үшін What's App жазбаңызға кіріп "Байланыстырылған құрылғылар" тізімін тексеріп, екі факторлы аутентификацияны қосыңыз.

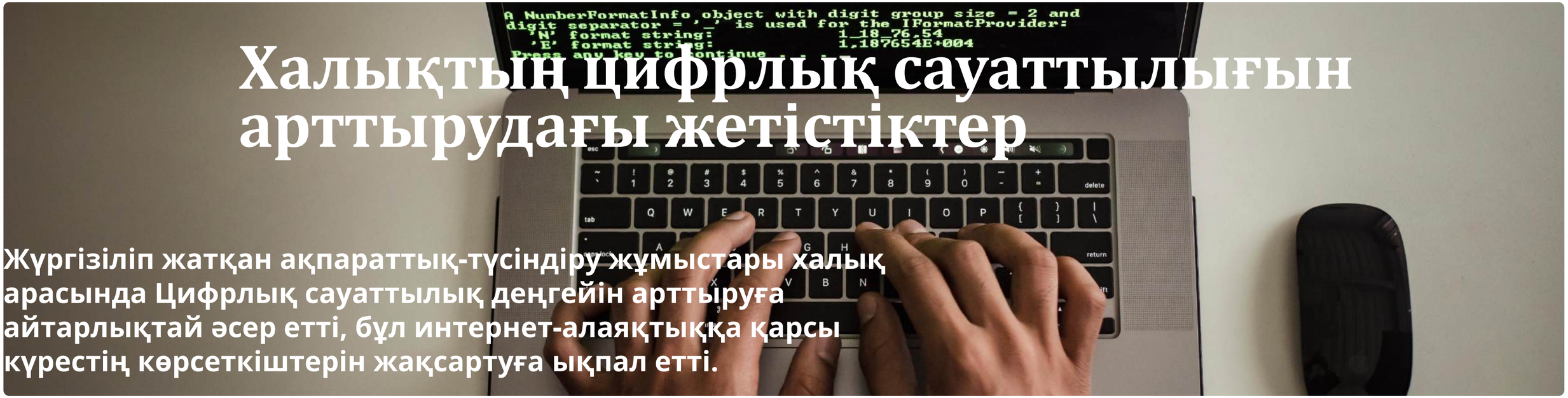
Астана қаласы полиция департаменті заңсыз әрекеттер анықталған жағдайда полицияға хабарласу керектігін еске салады !!!

10 қысқа нөмір арқылы

2

Сіздің қырағылығыңыз ақшаңызды сақтауға көмектеседі!

Халықтың цифрлық сауаттылығын арттырудағы жетістіктер



Жүргізіліп жатқан ақпараттық-түсіндіру жұмыстары халық арасында Цифрлық сауаттылық деңгейін арттыруға айтарлықтай әсер етті, бұл интернет-алаяқтыққа қарсы күрестің көрсеткіштерін жақсартуға ықпал етті.

Интернеттегі алаяқтықтың төмендеуі:
Азаматтарды белсенді ақпараттық қолдау мен оқытудың арқасында интернет-алаяқтық жағдайларының санын 2,7% - ға төмендеуге қол жеткізілді.

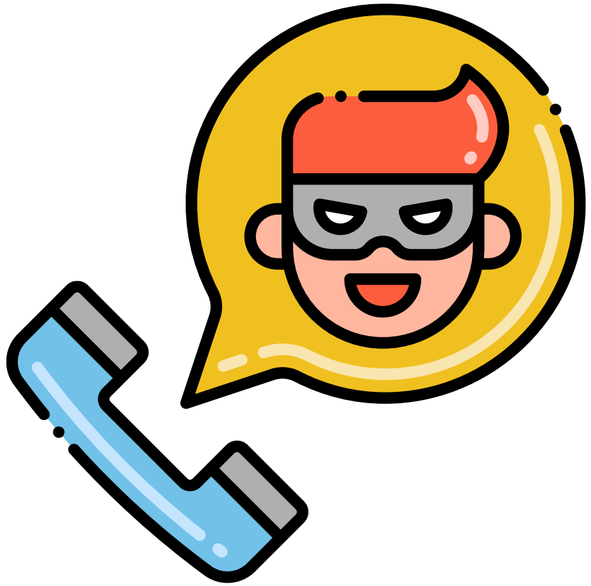
Қылмыстың ашылу деңгейі:
Азаматтардың хабардарлығы мен олардың алаяқтық схемаларды тану қабілетінің артуы құқық қорғау органдарының тиімділігінің артуына ықпал етті. Нәтижесінде интернет-алаяқтықтың ашылу деңгейі 2,8% - ға өсті.

Бұл нәтижелер халықты ағарту және цифрлық қылмыстың алдын алу бойынша ақпараттық-түсіндіру жұмыстарын жалғастырудың маңыздылығын көрсетеді.

Банктер немесе мемлекеттік органдар атынан қоңырау шалу

жасанды интелектті пайдалану арқылы банктердің қауіпсіздік қызметі немесе құқық қорғау органдарының қызметкерлерінің атынан жасалатын қоңыраулар – онда аудио немесе бейне арқылы диалог құру кезінде, олар өздерінің дауыстары мен бет-әлпеттерін ауыстырып, полиция немесе ұлттық банк қызметкері, танысы немесе туысқаны ретінде хабарласады.

Олар сіздерді күмәнді банктік операциялар немесе алаяқтарды ұстау бойынша арнайы операциялар жүргізіліп жатыр деп алдайды.



Полиция тұрғындарды құқық бұзушыларды құрықтау кезінде телефон немесе бейне байланыс арқылы тартпайды

«What’s App»messenger рұқсатсыз кіру

"What's App" мессенджеріне заңсыз қол жеткізу – алаяқтар зиянды сілтемені пайдаланып, көрсетілген сілтеме арқылы өткеннен кейін олардың "What's App" жеке жазбасына қол жеткізеді.

Осыған байланысты, біз азаматтарды, мысалға, жүлделер ұтыс ойыны, балаларға дауыс беру, кез келген тақырып бойынша сауалнама түрінде таратылатын күмәнді сілтемелер бойынша өтпеуге, сондай-ақ ешбір жағдайда өздерінің жеке деректерін енгізбеуге ескертеміз".

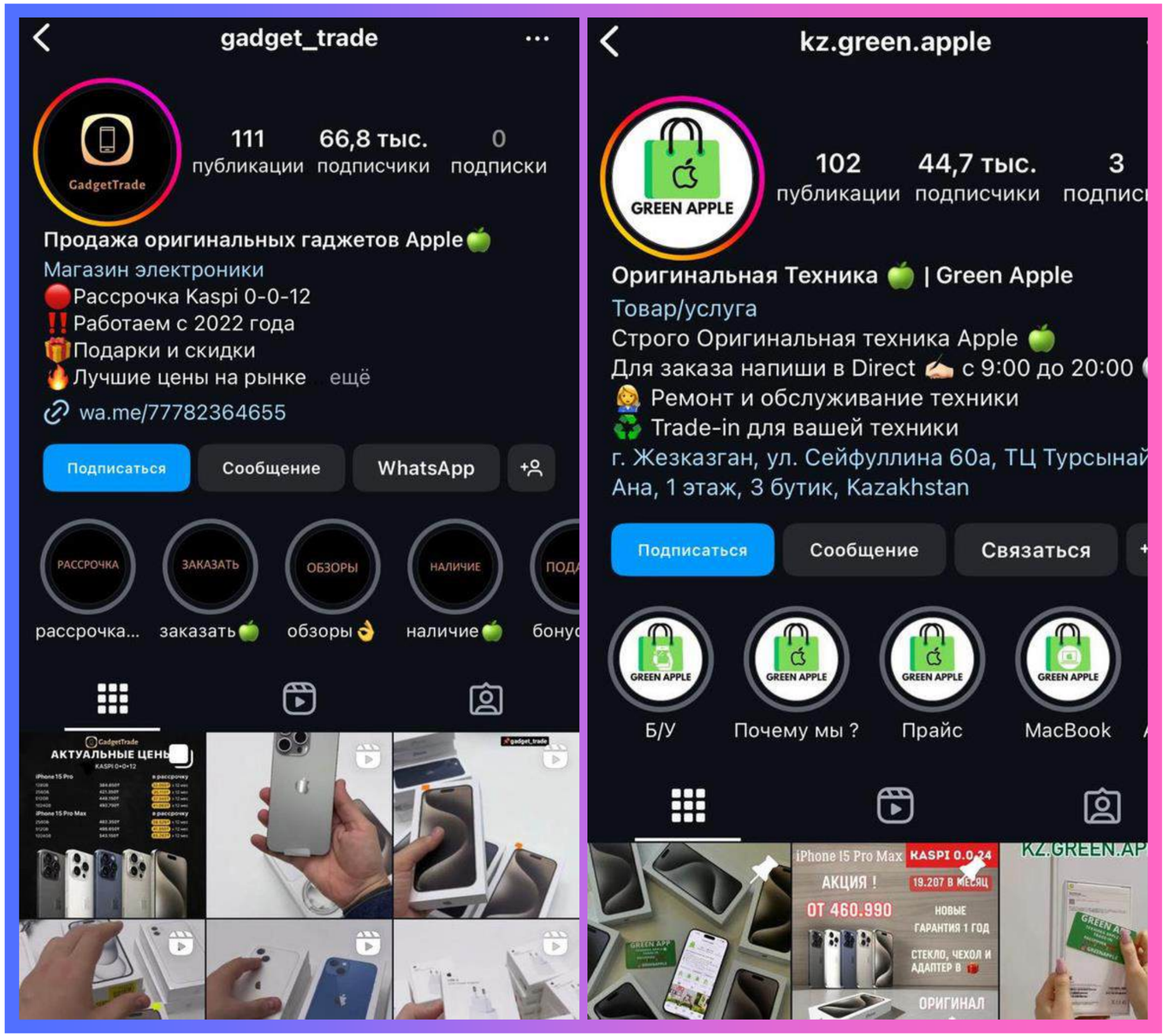
Әлеуметтік желілерде және сауда платформаларында тауарлар мен қызметтерді сату:

Әлеуметтік желілер мен интернет-платформаларда тауарлар мен қызметтерді сату – бұл түр әртүрлі тауарлар мен қызметтерді қиялмен сатуды қарастырады. Олар кез-келген жолмен ақша қаражатын алдын-ала төлем ретінде аударуды сұрайды.
Егер сіз өнімді өз көзіңізбен көрмесеңіз,
мұндай сатып алулардан бас тартқан дұрыс, әйтпесе сіз өз жинағыңызсыз қалуыңыз мүмкін;

Инстаграмдағы сауда алаяқтықтары: ұсталып қалмау үшін

Жалған Instagram акаунттарымен ұялы телефондарды сату интернеттегі алаяқтықтың кең таралған түрі болып табылады.
Зиянкестер жалған аккаунттар құрып, жаңа смартфондар үшін тым төмен бағаны көрсетіп, көбінесе сатып алушыларды алдау үшін нақты сатушыларға еліктеп, төлем үшін электронды шот жібереді.
Осыған байланысты азаматтарды барынша қырағылық танытуға және тауарды алғаннан кейін төлемді таңдауға, сондай-ақ тексерілген сауда алаңдарында телефондар сатып алуға шақырамыз.

Осы нұсқауларды орындау арқылы Instagram арқылы ұялы телефондарды сатып алу кезінде алаяқтардың құрбаны болу қаупін айтарлықтай азайтуға болады.



Фишинг сайттарын пайдалану

фишингтік сайттарды пайдалану – алаяқтықтың бұл түрі дербес деректер мен банктік мәліметтерді жинауға бағытталған. Мұндай сайттар нақты сайттардан айырмашылығы аз болады.

Мысалы, сіз сайттардың бірінде хабарландыру жарияладыңыз және сізге бұрын таныс емес адам хабарласып, жеткізу қызметін пайдалануды сұрайды. Содан кейін ол рәсімдеу үшін сілтемені жібереді. Сілтемені басу арқылы сіздің деректеріңізді, яғни аты-жөніңізді, туған жылыңызды, банк картасының нөмірін, жарамдылық мерзімін және CVV кодын енгізу сұралады. Осы деректер толтырылғаннан кейін сіздің банк картаңыздан ақша қаражатын есептен шығару басталады.

Криптовалютаға, бағалы қағаздарға және т.б. инвестициялау

Мысалы, әлеуметтік желілерде сіз акцияларды немесе криптовалюталарды сатып алу және сату арқылы ақша табу ұсынатын жарнаманы көрдіңіз және өз деректеріңізді қалдырыңыз. Сізбен, Ұлттық компанияның немесе брокерлерге қызмет көрсететін басқа ұйымның қызметкері ретінде зиянкестер хабарласады. Олар тиімді ұсыныстар туралы айтып, ақша салуға көндіреді, басында аз мөлшерде ақша салуын айтады. Бірнеше күннен кейін олар тапқан пайдасымен салынған ақшаны қайтарады. Осыдан кейін олар елеулі сомадағы ақшаны салуды сұрайды. Алаяқтардың айла-амалдарына тап болғандардың көпшілігі "зиянкестер сенімді, сенімді әрекет етеді және олардың арсеналында сіз тіркеуден өткен жақсы дамыған интернет-сайттары бар және жеке кабинетте жинақтарыңыздың өсуін бақылап отырасыз" - дейді, бірақ мұның бәрі жалған.

ДРОППЕР ЖӘНЕ ДРОПОВОД ДЕГЕНІМІЗ КІМДЕР?

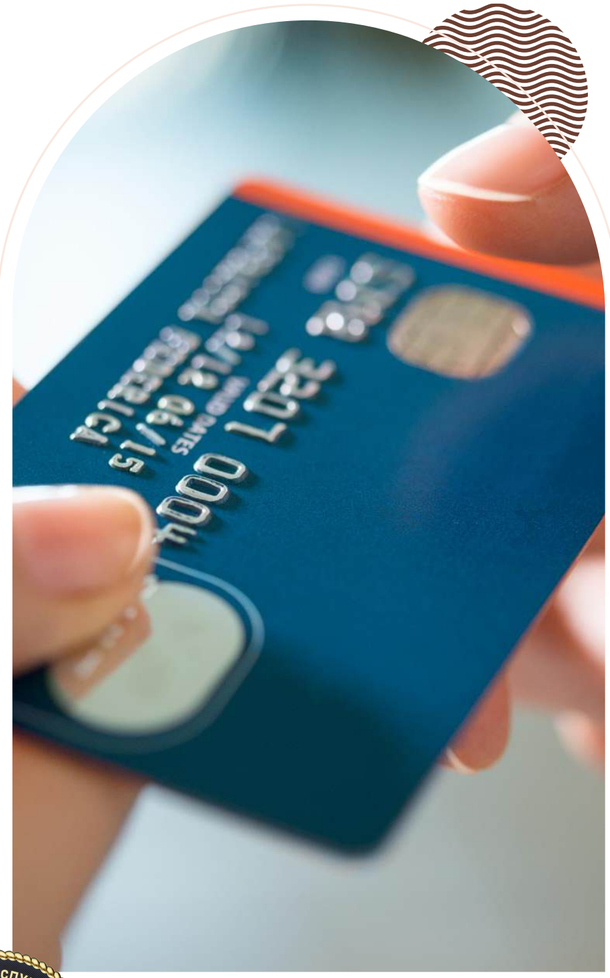
ДРОП (DROP)

Бұл белгілі бір сыйақы үшін заңсыз қаржылық операцияларды жүзеге асыру үшін өзінің жеке деректерін, банк шоттарын немесе карталарын беретін адам. Көбінесе мұндай адамдар қылмыстық схемаға қатысады деп күдіктенбейді.

ДРОПОВОД (DROP HANDLER)

Заңсыз қаржылық операцияларды жүзеге асыру үшін дропперлерді жалдайтын, бақылайтын және пайдаланатын алаяқтық схеманың ұйымдастырушысы болып табылады.

ОЛАР ҚАЛАЙ ЖҰМЫС ІСТЕЙДІ?



Дроп

- Жалған тұлғаларға тіркеу: Дропперлер банк карталары мен шоттарын өз атына тіркейді.
- Деректерді беру: содан кейін олар ұрланған қаражатты қолма-қол ақшаға айналдыру үшін алаяқтарға немесе "кураторларға" деректерді жібереді.
- Тәуекел және жауапкершілік: Дроппер шағын өтемақы алса да, ол ең үлкен тәуекелге ие, өйткені заң оны шоттың иесі деп санайды

Дропповод

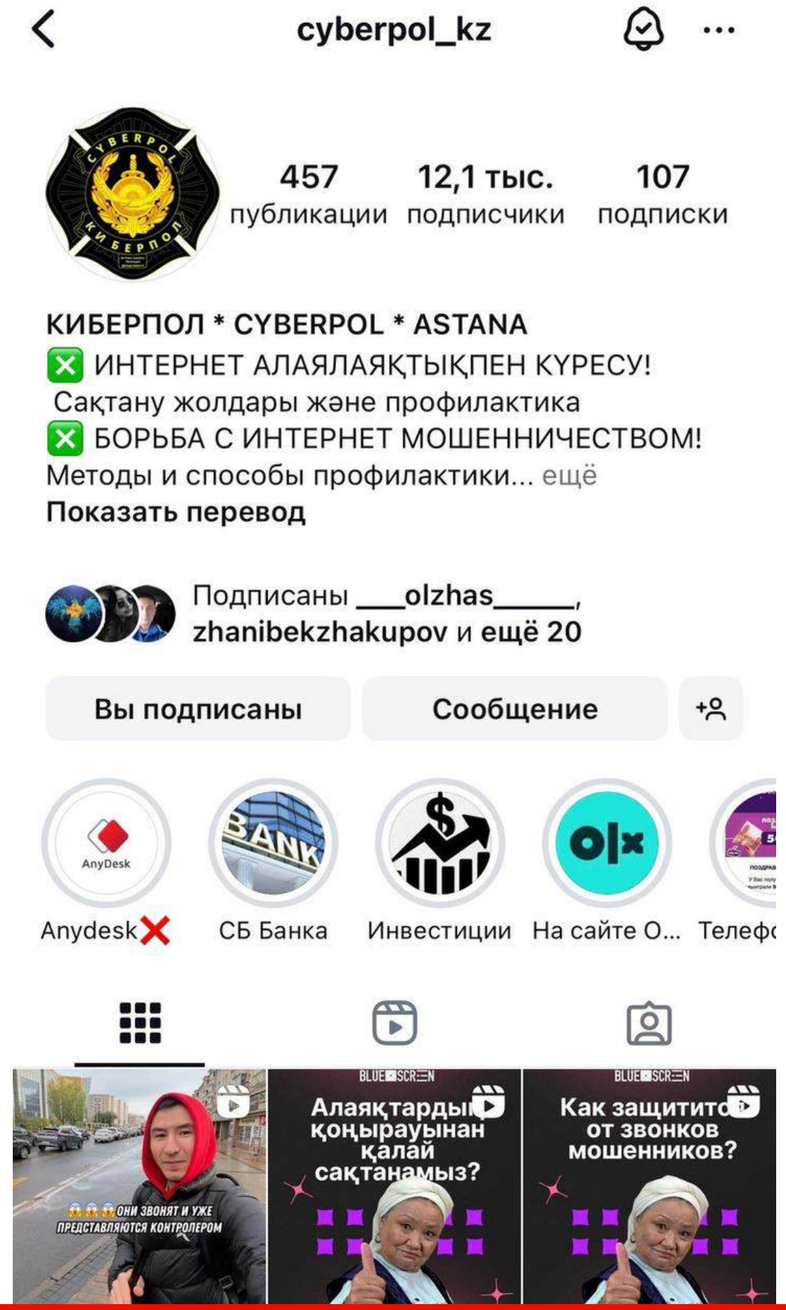
- •Жалдау: Дроповод жеңіл ақша уәде ететін жұмысты іздейтін адамдарды (дропперлерді) ж әлеуметтік желілер, хабарландырулар немесе жеке байланыстар арқылы табады.
- * Нұсқаулық: олар дропперлерге шоттарды қалай дұрыс ашу керектігін және алынған ақшамен не істеу керектігін үйретеді.
- Үйлестіру және бақылау: Дроповод бүкіл схеманы басқарады, рөлдерді тағайындайды және нұсқаулардың орындалуын қамтамасыз етеді.

Алаяқтардан бір қадам алда болыңыз: қауіпсіздік кеңестері

- **Банк қызметкерлері атынан таныстыратын алаяқтардың айла-амалдарына түспеу және сіздің атыңызға онлайн несие рәсімдемеу үшін егов сайтынын функциясын қосу керек.**
- **Сатушылар мен сайттарды тексеріңіз. Сатып алуға асықпаңыз, алдымен тауарды алу керек.**
- **Бейтаныс адамдардың күдікті сілтемелерін баспаңыз. Олар фишинг сайттары болуы мүмкін.**
- **Қиын құпия сөздерді және екі факторлы аутентификацияны пайдаланыңыз. Бұл сіздің жеке аккаунтарыңызға кіруді қауіпсіз етеді.**
- **Ешқашан банк картасының деректемелері мен құпия сөздерді бейтаныс адамдармен бөліспеңіз, олар зиянды мақсаттарда пайдаланылуы мүмкін.**
- **«Банктерден» және «құқық қорғау органдарының қызметкерлерінен» қоңыраулар мен хабарламаларды түскен кезде қырағы болыңыз. Банк қызметкерлері мен құқық қорғау органдары ешқашан сіздің жеке деректеріңізді сұрамайды**
- **Интернеттегі барлық ақпаратты екі рет тексеріңіз.**

Есіңізде болсын: сіздің Интернеттегі қауіпсіздігіңіз сіздің зейінділігіңіз бен сақтығыңызға байланысты.

Біздің Instagram каналға тіркеліңіз!



@CYBERPOL_KZ