Санариптик коопсуздук

Электрондук почта

“Фишинг”

Ишенимдүү уюмдардын атынан жасалма билдирүүлөрдү жөнөтүү аркылуу алдоо жолу менен логиндер, сырсөздөр же банк картасынын маалыматтары сыяктуу колдонуучунун купуя маалыматын алууну көздөгөн киберчабуулдун бир түрү.

Фишинг электрондук почталарын түзүүдө шылуундар кандай ыкмаларды колдонушат

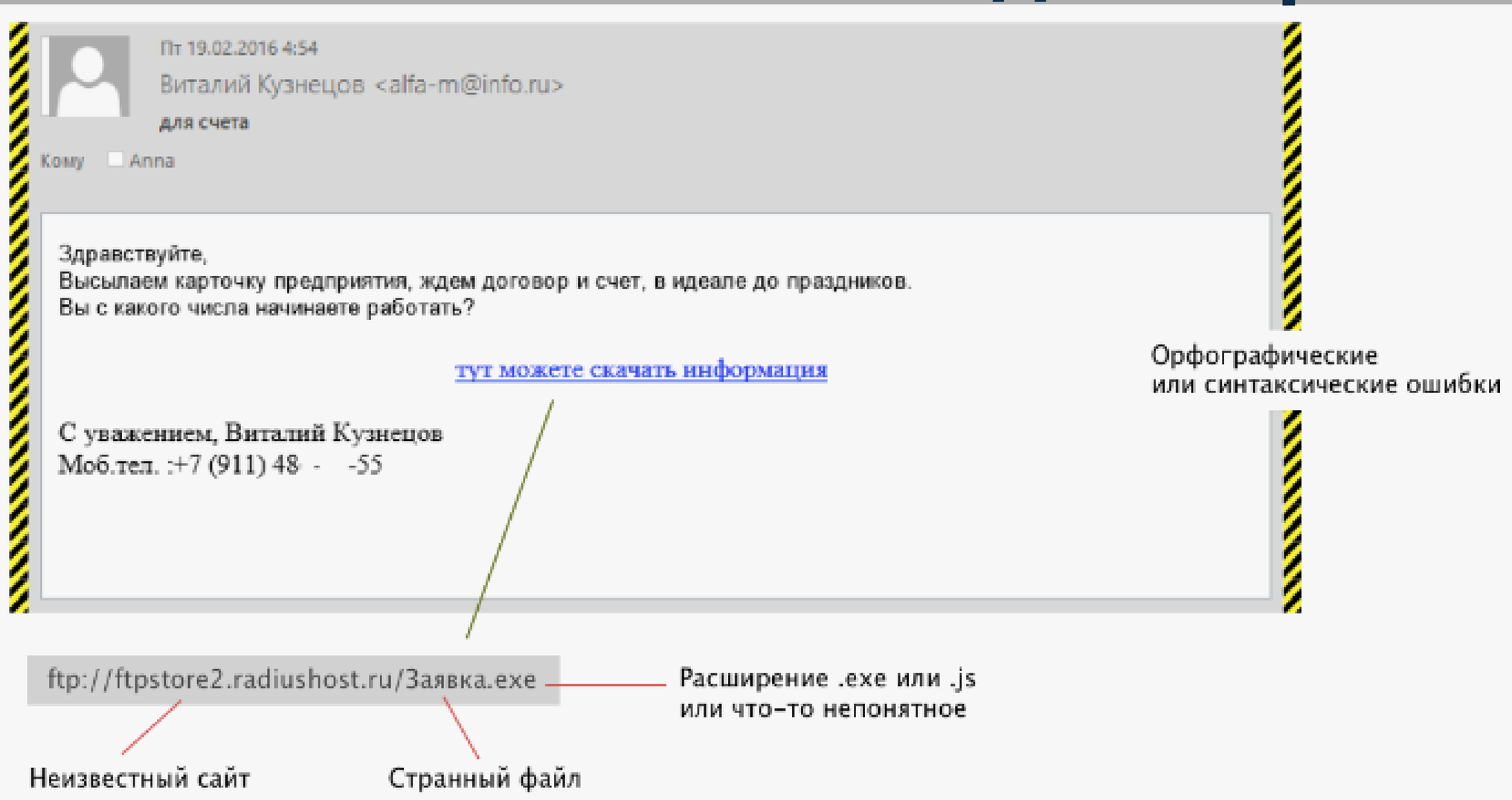
- Шилтеме боюнча өтүү

- Формага маалыматтарды киргизүү

- Тиркемелерди жүктөө

- Социалдык инженерия

Катты кантип анализдөө керек



Наведите курсор на ссылку, чтобы посмотреть куда она ведет

Электрондук почта бузулгандыгынын белгилери

- Күтүлбөгөн билдирүүлөр
- Жөнөтүлгөн билдирүүлөр
- Каттоо эсебиндеги өзгөрүүлөр
- Кирүү мүмкүн эместиги
- Электрондук почта кызматынын эскертүүлө
- Байланыш даттануулары

Хакерликтин зыянын азайтуу үчүн дароо аракет кылыңыз

- Сыр-сөздү өзгөртүү
- Коопсуздук жөндөөлөрүн текшериңиз
- Эки факторлуу аутентификацияны иштетүү
- Активдүү сессияларды текшериңиз
- Башка сайттардагы сырсөздөрдү өзгөртүңүз
- Папкаларды жана орнотууларды текшериңиз

Электрондук почта сырсөзүн киргизе албаган учурлар

Электрондук почта кызматынын расмий сайтынан, тиркемесинен же электрондук почта интерфейсинен башка каалаган сайтка почта кутусунун дарегин жана сырсөзүн киргизүүнү сунуштайт.

Бул форма бар сайтка кирүү үчүн сырсөздү киргизүү формасын же шилтемени камтыган почта кутусунан сырсөздү ырастоону сунуш кылган каттар.

Кирүү кутусунан колдонуучу атын жана паролду киргизүү формасы менен калкып чыкма же орнотулган терезелер.

Почтанын сырсөзүн качан киргизүүгө болот

Электрондук почта каттоо эсебиңизге түздөн-түз байланышкан кызматтар бар. Мисалы, почта менен байланышкан Google Play, YouTube кызматтар жана башкалар бар. Ошондой эле "Яндекс" кызматтары иштейт, мисалы "Яндекс.Диск" же "Яндекс.Маркет". Учурда кирүү ар кандай бул сервистердин системасы талап кылат бирдиктүү пароль-жылдын Сиздин аккаунта Гравив же Яндекс.

Көңүл буруңуз, система белгилүү бир каттоо эсебинен сырсөздү киргизүүнү суранат. Эгер сизден "электрондук почтаңыздын сырсөзү" деп сурашса, анда сиз жасалма баракчага киргенсиз. Шылуундар сиздин каттоо эсебиңиздин атын алдын-ала билбеши мүмкүн, андыктан сырсөзүңүздү алууга аракет кылышат.

Кандай маалыматты электрондук почта аркылуу жөнөтүүгө болбойт:

Сырсөз,
Банк картасынын маалыматтары,
Мүлк документтери,
Паспорттун көчүрмөсү ж. б.

Коопсуздук эрежелери:

Документтерди бейтааныш адамга жөнөтпөңүз;
Адресаттын аныктыгын жана суроо-талаптын туура экендигин текшериңиз;
"Жөнөтүлгөн"папкасынан каттарды жок кылыңыз

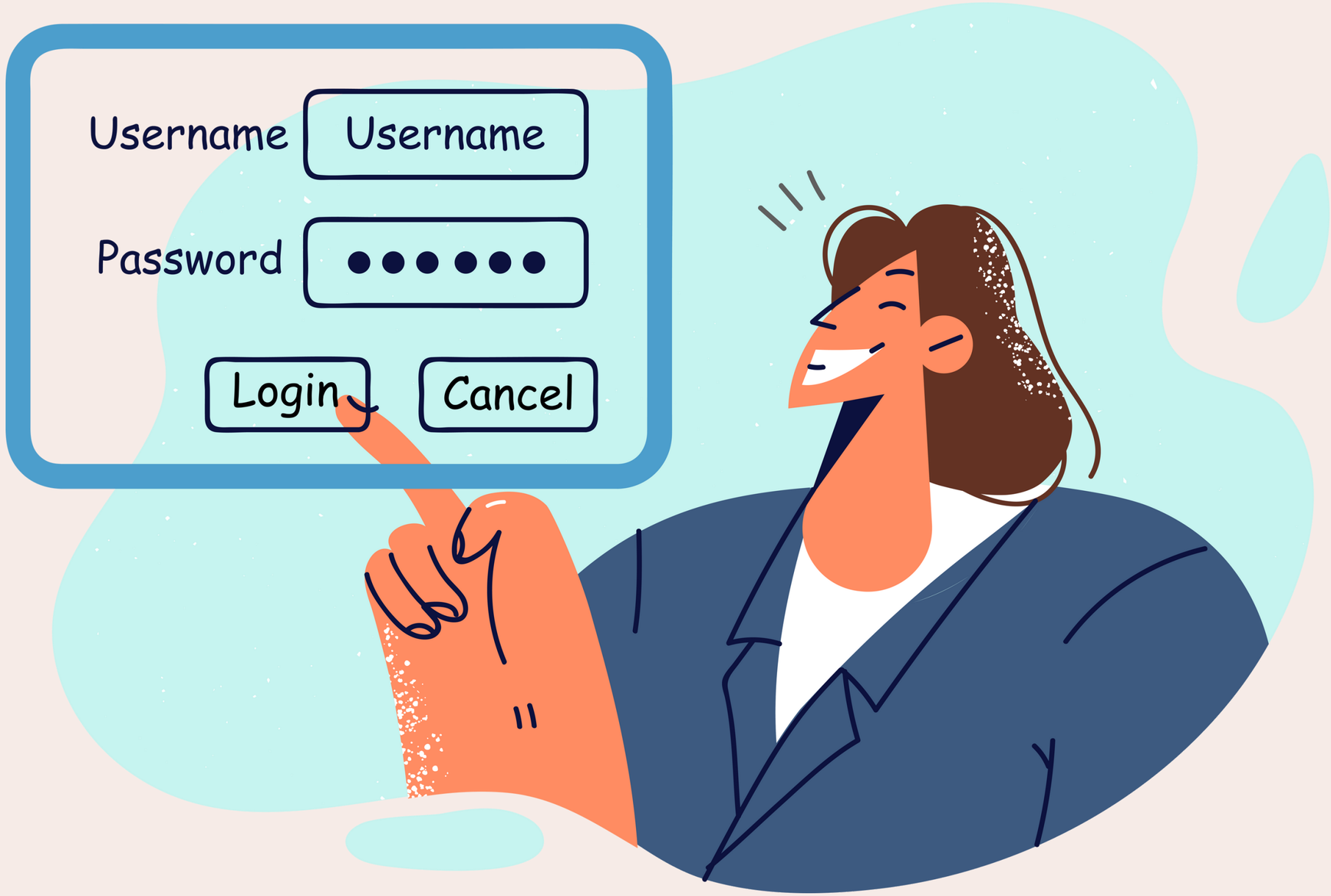
Банк картаныздын кайсы маалыматтарын жөнөтсө болот

Жөнөтүүчүгө акча которуу үчүн картанын номерин гана билүү керек. Ошондуктан, сиз аны жана тааныш адамга гана жөнөтө аласыз. Бирок ошого карабастан, номер алдамчылардын колуна түшүп калуу коркунучу бар. Картаңыздын номерин билүү менен, алар социалдык медиадан атыңызды жана фамилияңызды билип, картанын иштөө мөөнөтүн механикалык жол менен алышат. Бул маалыматтар менен, алар мониторинг коду киргизүү керек эмес, интернет-дүкөндөрдөн сатып алат. Мисалы, Ордодо.

Которууларды алуу үчүн өзүнчө нөлдүк балансы бар картаны кармаңыз жана которууну алгандан кийин, дароо негизги эсепке акча жөнөтүңүз.

Эгерде сизде банк картасынын номеринен тышкары башка которууну алуу мүмкүнчүлүгү болсо, ошону колдонунуз. Төлөмдөрдү башка идентификаторлор менен колдонуңуз: Уюлдук телефон номери, PayPal аккаунту же банк картасынын чоо-жайын колдонбогон башка төлөмдөрдү иштеп чыгуу тутуму.

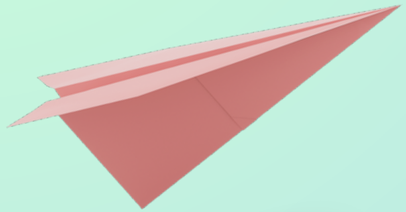
Сырсөздөр жана аккаунттар



Сырсөздөрүңүздү таанып, кибер шылуундар эмне кыла алышат

1. Сиздин почтанызга кирип жана бардык кабыл алынган жана жөнөтүлгөн каттарды окушат.
2.Каттоо эсебиңизде сакталган купуя маалыматтарды көрүшөт.
3. Жумуш дайындарыңызга кирүү, көчүрүү же биротоло жок кылуу.
4. Онлайн-банктын өздүк эсебине кирүү.

Татаал сырсөздү кантип түзүү керек



Жетиштүү узундукту колдонуңуз;
Ар кандай символдорду бириктирүү;
Ачыктан-ачык кеңештерден алыс болуңуз;
Кайталоодон алыс болуңуз;
Сырсөз фразаларын колдонуңуз;
Ырааттуулуктан жана кайталоодон алыс болуңуз;
Сырсөз генераторлорун колдонуңуз;
Сырсөздөрдү дайыма жаңыртып туруңуз.

Ушул көрсөтмөлөрдү аткаруу менен, сиз интернет эсептериңиздин коопсуздук деңгээлин кыйла жогорулатасыз.

Аккаунтуңуз бузулганын кантип түшүнсө болот

Эки мүнөздүү белги бар:

1. Сиз башкалардын активдүүлүгүнүн белгилерин байкадыңыз:
- мурда окулбаган деп белгиленген каттар күтүлбөгөн жерден окулду;
- баракчанын сүрөтү өзгөрдү;
- сиз жөнөтпөгөн билдирүүлөргө жооп алдыңыз жана башкалар.
2. Сиз жасабаган ар кандай өзгөртүү паролду шашылыш түрдө өзгөртүүгө себеп болот.

Почта кызматы сиздин каттоо эсебиңизге уруксатсыз кирүү аракети жөнүндө билдирүү жөнөтөт.

Вебсайттар жана Интернет. Жашыруун коркунуч

Зыяндуу сайттарды кантип аныктоого болот

Зыяндуу сайттар компьютериңизге жана жеке маалыматтарыңызга олуттуу зыян келтириши мүмкүн. Өзүңүздү коргоо үчүн, аларды тааный билүү маанилүү. Зыяндуу веб-сайттардын эң көп кездешкен белгилери:

Шилтемелердеги каталар, калкып чыкмалардын ашыкча саны, программалык камсыздоону жүктөп алуу сунуштары, суралбаган жаңыртуу сунуштары, жеке маалымат сурамдары, байланыш маалыматы жок, начар дизайн же грамматикалык каталар, сиздин макулдугуңуз жок башка сайттарга багыттоо, браузерге же антивируска Эскертүү

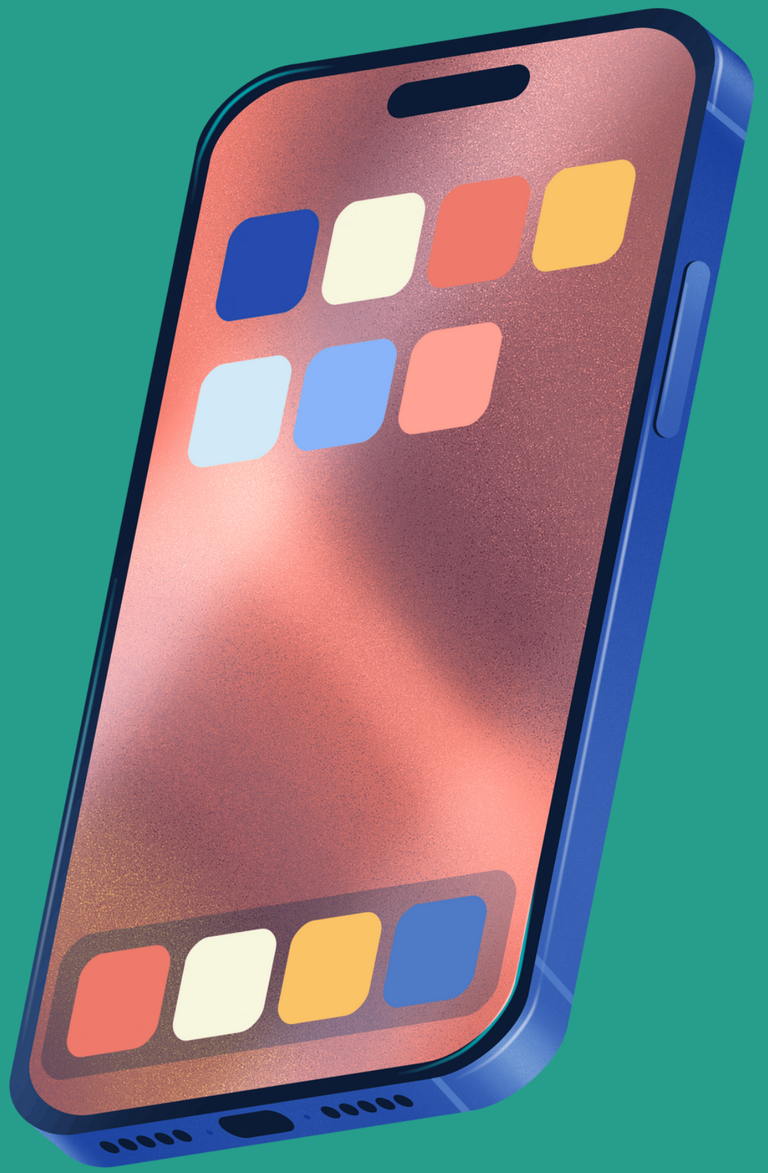
Программаны кантип коопсуз жүктөө керек

Интернеттен программалык камсыздоону (программаларды) жүктөө сиздин маалыматыңыздын жана түзмөгүңүздүн коопсуздугуна байланыштуу тобокелдиктерди алып келиши мүмкүн. Бул тобокелдиктерди азайтуу үчүн программаны түздөн-түз иштеп чыгуучулардын расмий сайттарынан же ишенимдүү платформалардан жүктөп алыңыз. Эгер компаниянын компьютерине программаларды орнотуу жөнүндө сөз болуп жатса, анда аны өзүңүз жасоого аракет кылбаңыз, тескерисинче, адистерге кайрылыңыз.

Файлдарды коопсуз жүктөө

- файлдарды расмий сайттардан же ишенимдүү платформалардан гана жүктөп алыңыз;
- файл кеңейтүүсүнө көңүл буруңуз;
- аткарылуучу файлдарды (exe, bat) текшерүүсүз иштетпеңиз.

Мобилдик түзмөктүн коопсуздугу

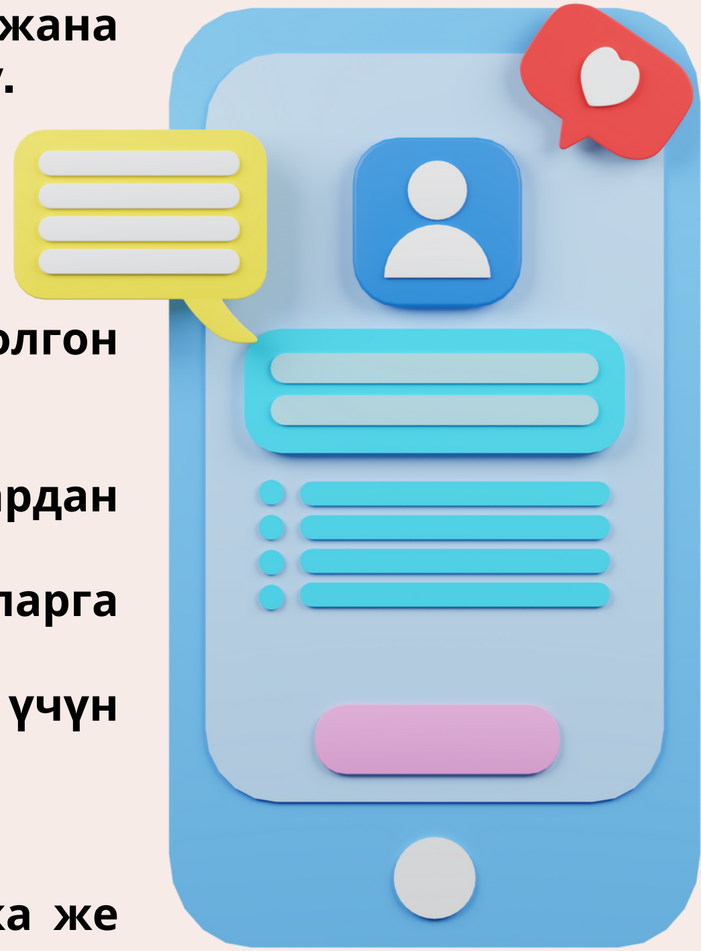


Мобилдик телефондор-бул сиздин санарип эгиздериңиз, акчаңыздын жана мааниилүү маалыматыңыздын сакчылары. Алар тийиштүү коргоого муктаж

- Эч качан смартфонуңузду кароосуз калтырбаңыз. Күчтүү сырсөздөрдү жана башка коргоо ыкмаларын колдонуңуз.
- Операциялык тутумуңуз эң ишенимдүү деп эсептесеңиз дагы, мобилдик антивирусту орнотуп, аны жаңыртып туруңуз.
- Мобилдик тиркемелерди расмий дүкөндөрдөн гана жүктөп алыңыз жана колдонмонун рейтингине, сын-пикирлердин сапатына жана канча жолу жүктөлгөнүнө көңүл буруңуз.
- Эч качан жеке маалыматтарды атабаңыз жана бейтааныш адамдардын өтүнүчү боюнча эч кандай каражат которбоңуз.

Социалдык медиа жана мессенджерлер

Социалдык тармактарда жана мессенджерлерде коопсуздугуңузду жана купуялыгыңызды камсыз кылуу үчүн бир катар чараларды көрүү маанилүү.



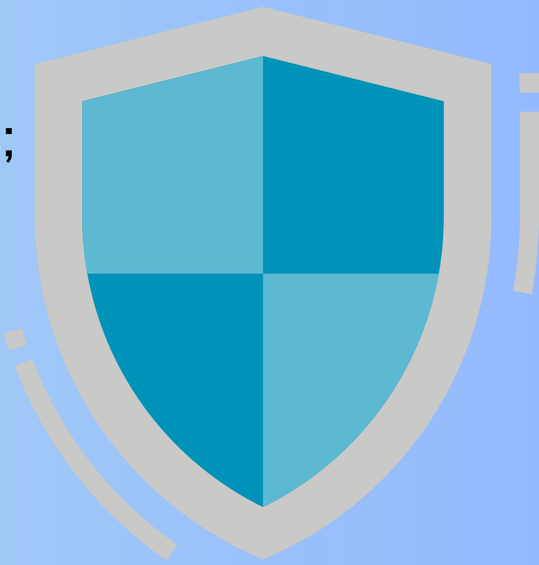
Татаал жана уникалдуу сырсөздөр.
Эки факторлуу аутентификация.
Шектүү шилтемелерди чыкылдатпаңыз.
Каттоо эсептериңизди аныктоо же бузуу үчүн колдонулушу мүмкүн болгон жеке маалыматтарды жарыялоодон алыс болуңуз.
Купуялык жөндөөлөрүңүздү дайыма текшерип, жаңыртып туруңуз.
Досторуңуздун же жолдоочуларыңыздын өтүнүчтөрүн сиз билген адамдардан гана кабыл алыңыз.
Социалдык медиа колдонмолору жана иштөө тутумдары акыркы нускаларга жаңыртылгандыгын текшериңиз.
Зыяндуу программалардан жана шпион программаларынан коргоо үчүн ишенимдүү антивирустук программаны колдонуңуз.
Каттоо эсебиңиздеги адаттан тыш аракеттерге сергек болуңуз.
Маанилүү маалыматтын камдык көчүрмөсүн дайыма сактаңыз.
Эгер Сиз шектүү иш-аракеттерге туш болсоңуз, анда социалдык тармакка же мессенжердин администрациясына кабарлаңыз.

Интернет коопсуздугу колдонуучунун туруктуу көңүлүн жана жигердүү аракетин талап кылат. Убакыттын өтүшү менен коргоо ыкмалары өнүгүп, киберкоопсуздуктун акыркы тенденцияларынан кабардар болуу маанилүү.

Компьютердин коопсуздугу

Компьютердин коопсуздугун камсыз кылуу үчүн негизги эрежелерди сактаңыз:

- Ар бир колдонуучу үчүн өзүнчө каттоо эсептерин жана аларга жеке татаал сырсөздөрдү түзүңүз;
- WI-FI ачык тармагына туташканда, VPN байланышты колдонуңуз жана https протокол боюнча иштеген сайттарга гана кириңиз.
- Антивирус дайыма күйүп турганын, анын базалары жаңыртылганын жана лицензиясы жарактуу экенин текшериңиз;
- Иштөө тутумуңузду жана браузериңизди жаңыртып, дайындарыңыздын камдык көчүрмөсүн дайыма сактап туруңуз;
- Лицензияланган программаны гана орнотуңуз.
- Интернет аркылуу компьютериңизге уруксатсыз кирүүдөн сактоого жардам берген брандмауэрди күйгүзүңүз.
-

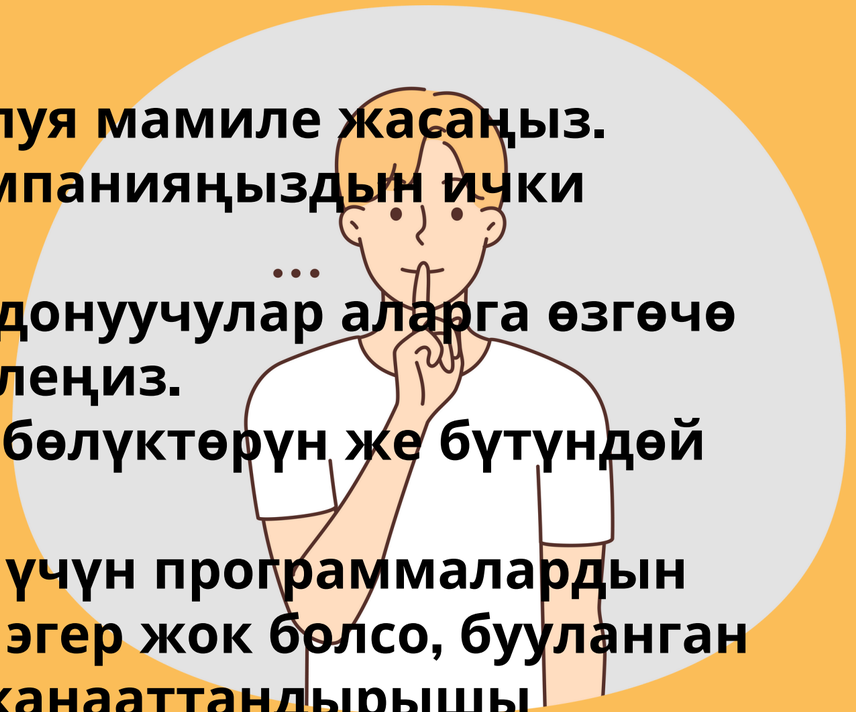


Компьютериңиз ар дайым ишенимдүү корголгон бойдон калсын!

Купуя маалыматты коргоо

Купуя маалымат-*бул жалпыга жеткиликтүү болбогон улам коргоону талап кылган маалыматтар. Ал жеке, корпоративдик, мамлекеттик же башка маалыматты каттышы мүмкүн, ал уруксатсыз адамдарга ачыкка чыкканда, каржылык, репутациялык, юридикалык же жеке болобу, зыян алып келиши мүмкүн.*

- Демейки боюнча, ар кандай жумуш маалыматына купуя мамиле жасаңыз.
- Купуя маалымат менен иштөөдө биринчи кезекте компанияңыздын ички эрежелерин жетекчиликке алыңыз.
- Сиз түзгөн купуя документтерди ар дайым башка колдонуучулар аларга өзгөчө мамиле жасоо керектигин түшүнгөндөй кылып белгилеңиз.
- Купуя маалыматты сактоо үчүн катуу дисктин айрым бөлүктөрүн же бүтүндөй дискти шифрлөөнү колдонуңуз.
- Сакталган файлдарды сырсөз менен коргоңуз. Коргоо үчүн программалардын же кызматтардын функцияларын колдонсоңуз болот, эгер жок болсо, бууланган архив. Сырсөз күчтүү сырсөздөрдү түзүү эрежелерин канааттандырышы керектигин унутпаңыз.
- Компанияңыздын коопсуздугу үчүн жооптуу адамдар бекиткен булут сактоочу жайларды гана колдонуңуз.
- Булут сактоочу документтерге түз шилтемелерди эмес, жеке чакырууларды колдонуу менен өтүңүз.
- Купуя документтерди жөнөтүүдө даректердин кирүү деңгээлин текшериңиз.



- Эч качан купуя документтерди шаблон катары колдонбоңуз. Калыпты нөлдөн баштап жасап, андан кийин жаңы документ түзүп жатканда, аны керектүү маалыматтарды толтуруу үчүн негиз катары колдонуңуз.
- Зарыл болбосо, купуя документтердин көчүрмөсүн түзбөңүз. Эсиңизде болсун: нускалар канчалык көп болсо, агып кетүү коркунучу ошончолук жогору болот.
- Купуя документтерди коопсуз жолдор менен гана өткөрүп бериңиз жана ошол маалыматтар менен таанышууга укугу бар адамдар гана.
- Шифрленген файлды жана ага сырсөздү багыттоонун ар кандай каналдарын колдонуңуз. Мисалы, эгер сиз шифрленген документти коопсуз корпоративдик почта аркылуу жөнөтүп жатсаңыз, сырсөз ага жөнөтүлөт ХОО же мессенджер аркылуу.
- Эгер купуя маалыматты камтыган документ сизге эч качан керек болбосо, аны жок кылыңыз. Муну жасоодо купуя материалдарды алып салуу үчүн атайын утилиталарды колдонуңуз.
- Чоочун адамдар менен иштөөдө жана коомдук жайларда иштөөдө маалыматтык коопсуздук эрежелерин сактоону унутпаңыз. Иш-аракеттериңизге жана сөздөрүңүзгө этият болуңуз.
- Жашыруун маалыматтын чыгып кетүү мүмкүнчүлүгүнө анча-мынча шек санаганда, компанияңыздын коопсуздук боюнча жооптуу кызматкерине кайрылыңыз.

Доксинг: коркунучтар жана алдын алуу чаралары

Доксинг-*бул жеке адам же уюм жөнүндө купуя маалыматты Интернетте атайылап издөө жана жайылтуу. Мындай маалыматка төмөнкүлөр кирет: сакталуучу жайга кирүү мүмкүндүгү бузулгандан кийин алынган жеке фото жана видеолор, социалдык тармактардагы билдирүүлөр, байланыш маалыматтары, жеке мүнөздөгү маалыматтар, медициналык жана финансылык маалыматтар ж.б.*

Доксердин бутасы аны жактырбоо же кандайдыр бир пайда табууну каалаган адам болушу мүмкүн.

Бирок, доксерлердин куугунтуктоосунан, алар керектүү маалыматты издөөдө колдонгон ыкмаларын билип, өзүн коргой алса болот.

Караңгы желедеги дайындарыңыз канча турат

Паспортту сканы:$6-15
Айдоочулук күбөлүктү сканы:$5-25
Документтер менен Селфи:$40-60
Электрондук ден соолук жазуусу: $ 1-30
Банк картасынын маалыматтары:$6-20
Интернет-банкка кирүү маалыматы: 50-500$
Электрондук почта жана социалдык медиа логиндери жана сырсөздөрү:$400-800

Доксерлерден кантип коргоносуз?

- Жеке маалыматтарды — чыныгы аты-жөнүн, дарегин, иштеген жерин жана башкаларды Интернеттен алыс кармаңыз.
- Соцтармактардагы аккаунттарды бөтөн адамдардан жабыңыз, аларды күчтүү жана уникалдуу сырсөздөр, ошондой эле эки факторлуу аутентификация менен коргоңуз.
- Сиздин чыныгы маалыматтар көрсөтүлгөн эсептер менен үчүнчү жактын кызматтарына кирүү эмес, - Ошентип, Сиз жеке маалымат үчүн боксчу жолду коюп жатышат.
- Активдүү иш-аракет: досьени чогултуп, көп нерсени билген кызматтарга маалыматтарды жок кылуу өтүнүчүн жөнөтүңүз.
- Доксерлер менен күрөшүүнүн радикалдуу, бирок жеңилген ыкмасы — эсептериңизди таптакыр жок кылуу. Муну кантип туура жасоо жана маанилүү маалыматтарды сактоо жөнүндө бир катар посттордо талкууладык.

Криптовалютала рдын коопсуздугу

Криптовалюта-бул санариптик же виртуалдык формадагы валютанын ар кандай түрү; крипто валютасындагы транзакцияларды коргоо үчүн шифрлөө (криптография) колдонулат. Криптовалюталарды чыгаруу же жөнгө салуу боюнча борбордук орган жок.

- Крипто үнөмдөөлөрүңүздү ар кандай сактоочу жайларга жайыңыз, жакшысы суук; аларды коргоонун бардык жолдорун колдонуңуз.
- Эч кимге, эч кандай шартта, сырттан келгендер Сиздин каражатыңызга кире турган жеке маалыматты бөлүшпөңүз.
- Сиз колдонгон крипто биржаларынын жана крипто капчыктарынын даректерин кылдат текшериңиз жана эч качан электрондук почталардан же тармактык жарнамалардан шилтемелерди чыкылдатпаңыз.
- Байлыгыңызды тез жана арзан баада көбөйтүүнү убада кылган фонддорго же белектерге ишенбеңиз.
- Гана ишенимдүү жана колдонуучулар тарабынан тастыкталган сайттарды тандоо. Жок дегенде жарымы ийгиликтүү болгон көптөгөн келишимдери бар сатуучуларга артыкчылык бериңиз.

Укканыңыз үчүн рахмат!