



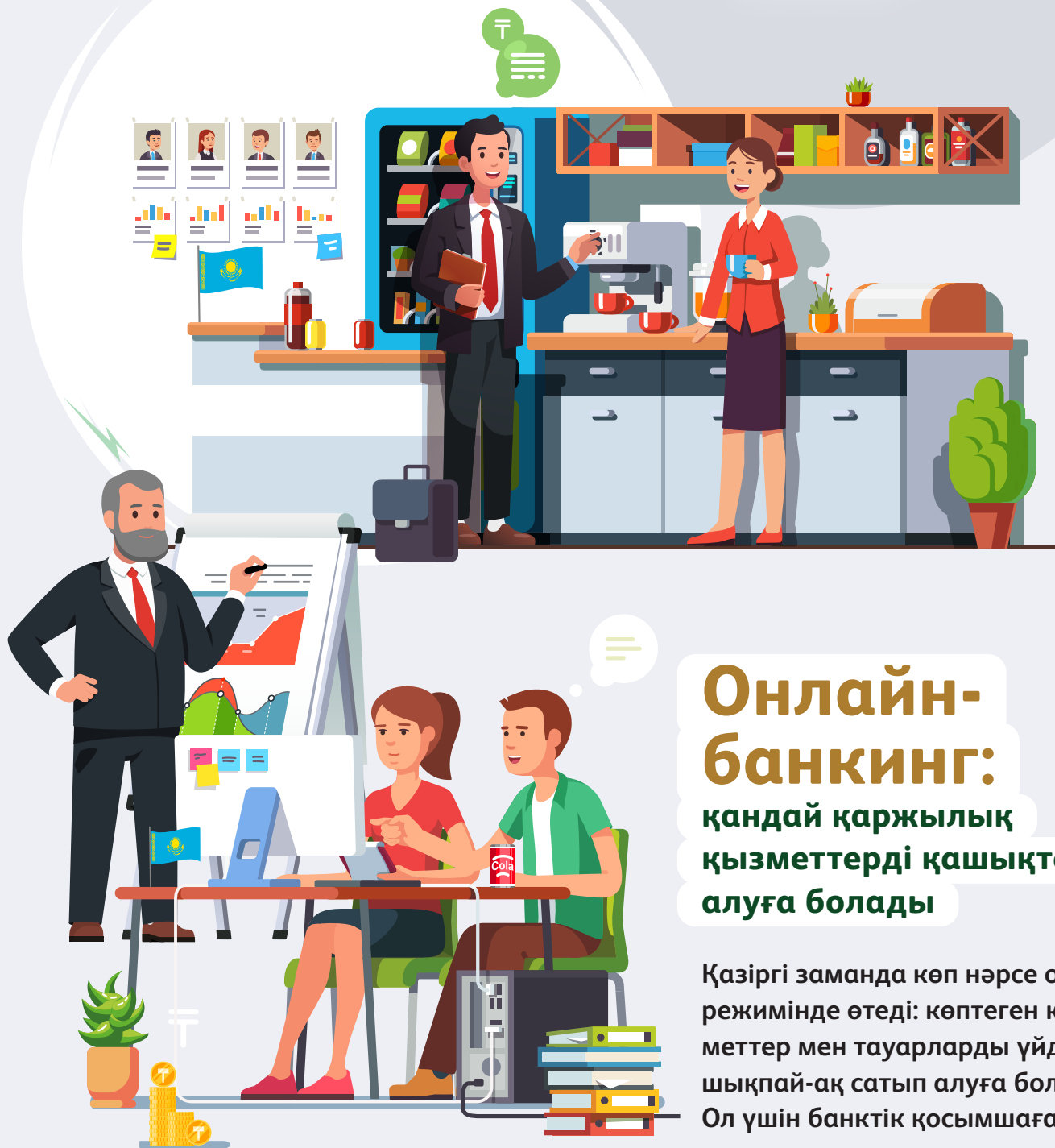
ЭКОНОМИКА



FinGramota

Халықтың қаржылық сауаттылығын арттыру

Fingramota.kz — Қазақстан Республикасы
Қаржы нарығын реттеу және дамыту Агенттігінің
халықтың қаржылық сауаттылығын арттыруға
бағытталған жобасы



**Онлайн-
банкинг:**
қандай қаржылық
қызметтерді қашықтан
алуға болады

Қазіргі заманда көп нәрсе онлайн режимінде өтеді: көптеген қызметтер мен тауарларды үйден шықпай-ақ сатып алуға болады. Ол үшін банктік қосымшаға кіру және интернетке шығу мүмкіндігі бар гаджет қажет.

ОНЛАЙН-БАНКИНГ ДЕГЕН НЕ?

ОНЛАЙН-БАНКИНГ — бұл шотыңыздағы ақшаны банк қосымшасы арқылы қашықтан басқару тәсілі. Оны **мобильді банкинг** деп те атайды.

Өткен шығарылымда біз балалар банк картасын қалай ашуға және оны қалай пайдалануға болатынын айттық. Егер сіз өз «пластигінің» иесі болсаңыз, онда сізге қызмет көрсететін банктің мобильді қосымшасын жүктей аласыз. Осы қосымшаны пайдалануды бастау үшін тіркеуден өту: өз деректеріңізді (тегі, аты, бар болса әкесінің аты, ЖСН, телефон нөмірі, электрондық пошта) толтыру және картаның деректемелерін көрсету керек. Банк кеңсесіндегі менеджер де бұны сіз үшін жасай алады, онда сіз ата-анаңызбен бірге келуіңіз керек.

Онлайн-банкингті қосу өте қарапайым,

қашықтан қызмет көрсету үшін сізге тек интернет және дұрыс жұмыс істейтін телефон, компьютер немесе планшет қажет.

Авторизациядан өткеннен кейін онлайн-банкингті пайдалана бастауға болады. Балалардың банктік қосымшасы функционалының ересек адамның банктік қосымшасының функционалы сияқты ауқымды емес екенін есте сақтаңыз. Сонымен қатар, банктер ата-аналық бақылау функциясын ұсынады, бұл ретте әкесі немесе ананы сіздің шотыңызда қанша қаражат бар екенін көріп, ол туралы үзінді көшірмемен таныса алады. Яғни, ата-аналар сіз қайда және қанша ақша жұмсағаныңызды, сондай-ақ онлайн-банкинг арқылы ақшаны кім сізге немесе сіз кімге аударғаныңызды біледі.

ОНЛАЙН-БАНКИНГТІҢ КӨМЕГІМЕН НЕ ІСТЕУГЕ БОЛАДЫ?

Онлайн-банкингтің көмегімен қандай қызмет түрлерін алуға болатынын талдап көрейік.



1 Тіркеуден өткеннен кейін, сіздің жеке кабинетіңіз пайда болады. Ол арқылы сіз шотыңызда қанша ақша қалғанын, қанша ақша түскенін, қызметтердің, тауарлардың немесе аударымдардың төлеміне қанша кеткенін көре аласыз.

2 Онлайн-банкингтен барлық онлайн-операцияларды, сондай-ақ шот бойынша (балалардың шоты ата-анасының шотына бекітілген) барлық жазбаларды көре аласыз: яғни, қайда, кімге және қашан, не үшін ақша аудардыңыз, сонымен қатар қашан және қай уақытта сізге ақшалай қаражат келіп түсті?

3 Өз шотыңыздағы ақшаны осы банк ішіндегі өзге шотқа аударып, дүкендегі сатушыға төлем жасап, таксидің құнын төлеп, туысқаныңыздың немесе досыңыздың картасына ақша аударып аласыз. Қазіргі таңда банктердің көбі қызметтер мен тауарлардың құнын телефондағы банк қосымшасы арқылы QR-кодпен төлеуге мүмкіндік береді.

Ересектер, өз кезегінде, мобильдік банк қосымшасы арқылы тағы басқа қызметтерді, мысалы қашықтан сақтандыруды, кредитті ресімдеуді немесе депозит ашуды жүзеге асырады. Ата-аналар интернет-банкингтің көмегімен еш қиындықсыз коммуналдық шотты төлеп, әуе және темір жол билеттерін сатып алып, бөліп төлеуді ресімдейді. Ересектер онлайн-банкинг арқылы айыппұлдар мен салық бойынша өз қарыздарын көріп, оларды төлеп, сондай-ақ жеке кәсіпкер ретінде тіркеліп, осылайша өз бизнесін ашуға алғашқы қадам жасай алады. Сонымен қатар түрлі мемлекеттік қызметтерді де алуға болады: мысалы, кей банктердің тұтынушыларына ХҚКО мен Азаматтарға арналған электронды үкіметтің (*egov.kz*) жекелеме қызметтері ұсынылған. Дегенмен, мұндай қызметтер тек кәмелет жасқа толғандар үшін қолжетімді.





Оқушылар үшін онлайн-банкінг керексіз шығындарды бақылап отыру үшін пайдалы, осылайша өз бюджетіңізді жоспарлауды шындап қолға алып, қаржылық мақсаттар құрып, кез келген затқа, мысалы велосипедке, скутерге, жаңа киімге, жақындарыңа сыйлыққа және т.б. ақша жинауға болады. Ең дұрысы — ата-анаңыздан олардың мобильді қосымшалары арқылы депозит ашып беруді сұраңыздар, оған ақшаны күнделікті жұмсауға берілген ақшадан жинақтап, онлайн-банкінг арқылы өз шотыңыздағы ақшаны ата-анаңыздың шотына аударып, әрі банктің салым бойынша қанша сыйақы бергенін тексере аласыздар. Сөмә барған сайын өсе береді, сіздің ақша жинасам деген ынтаңыз да артады.

Естеріңізде болсын, банктер өз қызметтері үшін, мысалы, өзге банктердің картасына ақша аударғанда, шот ашқанда және т.б. түрлі комиссиялар орнатады. Сондықтан, мұндай бағаларды алдын ала зерттеп алыңыздар, сонда банк комиссия ұстап қалғандықтан, керекті сөмәге толмай қалу секілді қолайсыз жағдайлар туындамайды.

Сонымен қатар банктер клиенттерін өз онлайн-банкінгтерінің қызметтерін пайдалануға ынталандырып, осы үшін балл немесе ақша түріндегі арнайы бонус — кешбэк береді. Әр операция мен саудадан кейін олар жинала береді, соңында онымен дүкенде төлем жасап, не телефонның бірлігін толтыруға болады.

Жоғарыда көрсетілген мүмкіндіктер тұтынушылардың барлығына бірдей қолжетімді емес, түрлі банктердің онлайн-банкінгтегі қызметтері де әртүрлі, әсіресе банк картасы ашылған балалар үшін.

ИНТЕРНЕТ-КЕҢІСТІКТЕГІ ҚАРЖЫЛЫҚ АЛАЯҚТАР

Кез келген дүниенің екі жағы бар екенін ұмытпаған боларсыздар? Онлайн-банкінгте бұл — деректеріңіздің дербес қорғанысы.

Шотыңыздағы қаражатыңыздың амандығы қаржылық онлайн-операцияларды қаншалықты сақтықпен орындайтыныңызға байланысты.

Қашықтық банкінгі дамыған сайын қаржылық алаяқтар да өз жұмыстарына белсенді кірісіп, олардың ақшаларына онлайн қол сұғу мақсатында адамдарды алдаудың алуан түрлі жолдарын ойлап тауып, енгізіп жатыр. Осындай қылмыскерлердің әрекетінен банк клиенті белгісіз сілтеме арқылы өтіп, мобильді қосымшаға сенімсіз пароль қойып және тағы басқа жағдайларда шотындағы барлық ақшасы жойылып, қаншама зардап шегіп жатады.

Әрине, банктер өз тараптарынан жүйелерін киберқылмыскерлердің бұзып кіруінен қорғау үшін, клиенттердің деректерінің қауіпсіздігін сақтау үшін қолдан келгеннің бәрін жасайды. Әйтсе де, көбінесе онлайн-режимдегі қауіпсіздік банкінгі пайдаланушылардың өздеріне байланысты: олар төлем картасының деректемелері, оның ішінде келесі бетіндегі код, SMS-код, пин-код секілді дербес мәліметтерін өздері жариялап, көпшілікке таратып жатады.

АЛАЯҚТАР ӘДЕТТЕ ҚАНДАЙ ТӘСІЛДІ ПАЙДАЛАНАДЫ?

Қастандық ойлаушылар интернеттегі түрлі сайттар арқылы арзан бағаға өз қызметтерін немесе тауарларын ұсынып, жылдам арада жеткізіп беретіндерін айтады. Клиент «тұзаққа түсіп қалады», одан төлемнің жартысын немесе толық соманы көбінесе үшінші біреудің атына ресімделетін шотқа аударуды сұрайды. Бірақ алдын ала төлем жасалғаннан кейін тапсырыс жеткізілмейді. Мұндай қылмыскерлерді табу өте қиын, себебі, сатып алушы нақты кіммен хабарласқанын, және деректерін білмейді.

Көп жағдайда алаяқтар түрлі банк клиенттеріне хабарласып, өздерін қауіпсіздік қызметінің қызметкерлері ретінде таныстырады. Олар клиенттің картасында күмәнді қаржылық операциялар жүріп жатқанын хабарлап, оны бұғаттау үшін төлем картасының келесі бетіндегі үш таңбалы нөмір керек екенін жеткізеді. Осы цифрларды алғаннан кейін қылмыскерлер интернет-банкінгке қосылып, бірнеше минут ішінде клиенттің онлайн-шотындағы бар ақшаны жымқырады. Клиенттің картасын өз мақсатына пайдалану үшін алаяққа оның нөмірі, иесінің есімі, жарамдылық мерзімі, CVC немесе CVV нөмірі (бұл кез келген төлем картасының келесі бетіндегі сол баяғы үш сан — ол карта иесінің қолы қойылған жолда немесе оның қасында орналасқан) керек.

Қаржылық алаяқтар сізге қоңырау шалып немесе SMS жолдап: абонент нөміріңіздің компания байқауында жеңімпаз атанғанын хабарлауы мүмкін. Сыйлықты басқа қаладан алуды немесе банк картаңызға ақшалай аударым түрінде алуды ұсынады. Алаяқтар адамның жеке деректерін сұрастырып, құрылғыны өз интернет-банкінгтеріне қосуға мүмкіндік беретін түрлі қосымшаларды жүктеп алуды өтініп, ондағы ақшаны иемденеді.



Қазіргі таңда кеңінен тараған келесі бір тәсіл

— қылмыскерлер өздерін сатып алушымыз деп таныстырады. Олар сатушының телефонына түрлі фишинг сайттарына сілтеме жіберіп, онда тауарға төлем жасауға керекті деректерін енгізуді сұрайды.

Сол кезде, оның ақшасы төлем картасы иесінің келісімінсіз-ақ автоматты түрде жоғалады, себебі оның гаджетіне зиянкес БҚ (бағдарламалық қамтамасыз ету), яғни вирус енді.

Мұндай алаяқтар үшін балалар — оңай олжа. Қастандық ойлаушылар түрлі психологиялық амалдарды пайдаланып балалардан ата-аналарының: ЖСН, аты-жөні, карта деректері секілді тағы басқа ақпараттарды біліп алады және ересектердің атына онлайн-кредит рәсімдейді.





ӨЗІМІЗДІ ҚОРҒАП, АЛАЯҚТЫҢ ТҰЗАҒЫНА ТҮСПЕУ ҮШІН НЕ ІСТЕЙМІЗ?

Бірінші кезекте, қандай жағдай болмасын, өзіңіздің және ата-анаңыздың дербес деректерін, оның ішінде пластик карталардың деректемелерін ешкімге жарияламаңыздар, ақша аударымдары туралы квитанцияларды ешкімге бермеңіздер және кодтар мен құпия сөздерді айтпаңыздар.

Тексерілмеген және күмәнді ақпарат көздеріне, мысалға, танымайтын адамдарға әсіресе интернеттегі дереккөздерге сенім артуға болмайды. Алаяқтар сіздің сеніміңізге кіру үшін өзін сіздің құрдас ретінде таныстыруы мүмкін. Мәселе ақшаға қатысты болғанда кез келген ақпаратты тексеріңіз, ересектермен, ата-анаңызбен және жақындарыңызбен кеңесіңіз.

Тексеріп алмай тұрып тауардың құнын

төлеуге болмайды, төлемді затты алғаннан кейін жасаймын деп келісіңіз.

Егер сатып алушының немесе сатушының сөзіне күмәнмен қарасаңыз, егер ол Сізді алдап тұрған секілді болып көрінсе, келісімді тоқтатыңыз, тауар немесе қызмет үшін дереу төлеуге асықпаңыз. Кез келген уақытта күте тұруға болады. Ақша Сіздің қолыңызда болғанда жағдайды Сіз басқарасыз, яғни қандай да бір тауар не қызметті сатып алу керек пе әлде жоқ па — оны өзіңіз шешесіз.



Ешқашан күмәнді сілтемелер арқылы өтпеңіздер. Тағы да қайталаймыз: алаяқтар ақшаны шотыңыздан автоматты түрде шешіп ала алады. Белгісіз нөмірлерге қайта қоңырау шалмаңыз. Өзіңізге белгісіз сайттардың бәрін интернет арқылы қарап, пікірлерді оқып, ақпаратты талдаңыз.



Егер сіздерге жеңімпаз атанғаныңызды немесе картаңыздан банк кездейсоқ ақша шешіп алғанын хабарлап, операцияны тоқтату үшін өз деректеріңізді айту керектігін сұраса, сөйлесуді бірден тоқтатып, картаңыздың келесі бетінде көрсетілген телефон нөмірі арқылы банкке қоңырау шалыңыз. Немесе ересектерден солай істеуін сұраңыз.



Өз онлайн-банкінг қызметіңізге кіру паролін жиі ауыстырыңыз, ата-анаңыздан гаджетіңізге антивирус орнатып беруін сұраңыз.



Шотыңыздағы ақша айналымын қашан және қанша ақша түскенін және жұмсалғанын тұрақты түрде тексеріп отырыңыз.



Егер интернет арқылы бірдеңе сатып алсаңыз, операцияны растау үшін құпия кодты ешкімге айтпаңыз. Әдетте ол SMS арқылы келеді.

Егер сізге банктен шотыңызға ақша аударылғаны туралы SMS келсе, артынша белгісіз біреу хабарласып, шотыңызға қателесіп ақша жіберілгенін, оны қайтару керектігін айтса, бұлай жасауға асықпаңыз. Оның алаяқ болуы әбден мүмкін. Негізі, Сізге ешқандай ақша түскен жоқ, ал SMS — жалған. Бірден барлық шоттарыңызды тексеріп, онлайн-банкингтегі үзінді көшірмелерді қараңыз, болмаса ата-анаңыз өз онлайн-банкингі арқылы тексеріп көрсін.

Егер телефоныңызға «Сатып алғаныңызды растаңыз» деген хабарлама мен код келсе, артынша дәл жоғарыдағыдай беймәлім біреу қоңырау шалып, қателесіп Сіздің телефон нөміріңізді беріп жібергенін айтып, кодты беруіңізді өтінсе, ешқашан олай жасамаңыз.

Қылмыскерлерге Сіздің кодыңыз шотыңыздан ақша шешіп алу үшін немесе Сізді керексіз ақылы сервиске жазып қою үшін керек.

Әдетте балалар картасы бекітілген банк қосымшаларында бала онлайн-сатылымға жұмсай алатын және біреуге аудар

алатын соманың шегі көрсетіледі. Мысалы, айына 30 мың теңгеден артық емес. Бұл сіздердің ақшаларыңызды сақтау үшін қауіпсіздік мақсатында жасалған.

Егер алаяқтар жеке пароліңізді бұзуға қадам жасаса, жеке деректеріңізді пайдаланса немесе төлем картаңызды жоғалтып алсаңыз, жылдам арада бұл туралы ата-анаңызға хабарлап, банкке барыңыз. Банктен картаны уақытша бұғаттай тұруды өтінуге болады, мұндайда оны қайта шығаруға тура келеді. 🕒



ЖЕЛІДЕГІ АККАУНТТАРЫҢЫЗҒА ҚАЛАЙ СЕНІМДІ ПАРОЛЬДЕР ЖАСАУҒА БОЛАДЫ?

Сенімді пароль жеке деректеріңізді қорғауға, жазбаларыңыздың, файлдарыңыз бен өзге де материалдарыңыздың құпиялылығын сақтауға және аккаунттыңызды бұзғысы келетін алаяқтардың қадамынан қорғауға көмектеседі.

1 Пароль кем дегенде 12 белгіден тұруы қажет. Бұл сүйікті әріптердің, сандардың және басқа да белгілердің жиынтығы болуы мүмкін. Пароль неғұрлым ұзын болған сайын, соғұрлым сенімді.

Ол: өлеңнің немесе әннің бір жолы; фильмнен алынған цитата не танымал адамның сөзін; кітаптан алынған цитата; сіз үшін маңызды сөйлем; аббревиатура (мысалы — сөйлемдегі сөздердің бірінші әріптері) болуы мүмкін.

2 Тез тауып алуға болатын парольді қолданбаңыздар. Егер адам сізді жақсы білсе, пароліңізді оңай тауып алады. Мысалы, әлеуметтік желідегі деректеріңізге қарап табады.

3 *Danik123* деген секілді тым жеңіл пароль көрсетпеңіздер, онда туған күн, ай, жылдарыңыз болмасын. Жеке деректеріңіз бен жалпыға ортақ сөздерді қолданудан аулақ болыңыздар. Дұрысы, өзіңіз тез есте сақтап қалатын, алайда басқалар таба алмай қиналатын комбинацияны орнатыңыздар. Парольді жиі ауыстырыңыздар.

4 Сенімді пароль жасағаннан кейін оның қауіпсіздігін қамтамасыз етіңіз. Жазылған құпиясөздерді сенімді жерде сақтаңыздар. Егер ұмытып қалмау үшін құпиясөзді жазып алған болсаңыз, оны үстел үсті, компьютер монитормы, телефондағы ескертпелер секілді айқын көзге түсетін орындарға қалдырмаңыз.

Қандай да бір операцияны онлайн жүзеге асырғанда сақ болыңыз. Желіде сауда жасағанда мұқияттылық керек. Әрдайым сіздерге тек жақсылық тілейтін ата-аналарыңызды тыңдаңыз.

Қаржылық сауатыңызды балалық шақтан бастап жетілдіріңіз!

