ЭКОНОМИКА

FinGramota
Повышение финансовой грамотности населения

Fingramota.kz — проект Агентства Республики Казахстан по регулированию и развитию финансового рынка, направленный на повышение финансовой грамотности населения

Онлайн-банкинг:

какие финансовые услуги можно получить удалённо

В современном мире многое переходит в онлайн: большинство услуг и товаров вы можете приобрести, не выходя из дома. Для этого всего-то нужны доступ к банковскому приложению и гаджет с выходом в интернет.

Что такое онлайн-банкинг?

ОНЛАЙН-БАНКИНГ — это способ удалённого управления деньгами на своём счёте через банковское приложение. Его ещё называют **мобильным банкингом**.

В прошлом выпуске мы рассказали, как открыть детскую банковскую карту и как ею пользоваться. Если вы стали обладателем собственного «пластика», то можете скачать мобильное приложение банка, в котором обслуживаетесь. Следует пройти регистрацию, чтобы начать пользоваться этим приложением: заполнить свои данные (фамилию, имя, отчество — при наличии, ИИН, номер телефона, электронную почту) и указать реквизиты карты. То же самое может сделать за вас и менеджер в офисе банка, куда вам нужно прийти вместе с родителями.

Онлайн-банкинг подключается очень просто. Для дистанционного обслуживания вам нужны только интернет и исправно работающий телефон, компьютер или планшет.

Как только вы пройдёте авторизацию, то можете начать пользоваться онлайн-банкингом. Имейте в виду, что функционал детского банковского приложения не такой широкий, как у взрослого. К тому же банками предусмотрена функция родительского контроля: ваши папа или мама могут посмотреть, сколько средств находится у вас на счёте, и ознакомиться с выпиской по нему. То есть родители будут знать, куда и сколько денег вы потратили, а также кто вам или кому вы посредством онлайн-банкинга перевели деньги.

Что можно делать с помощью онлайн-банкинга?

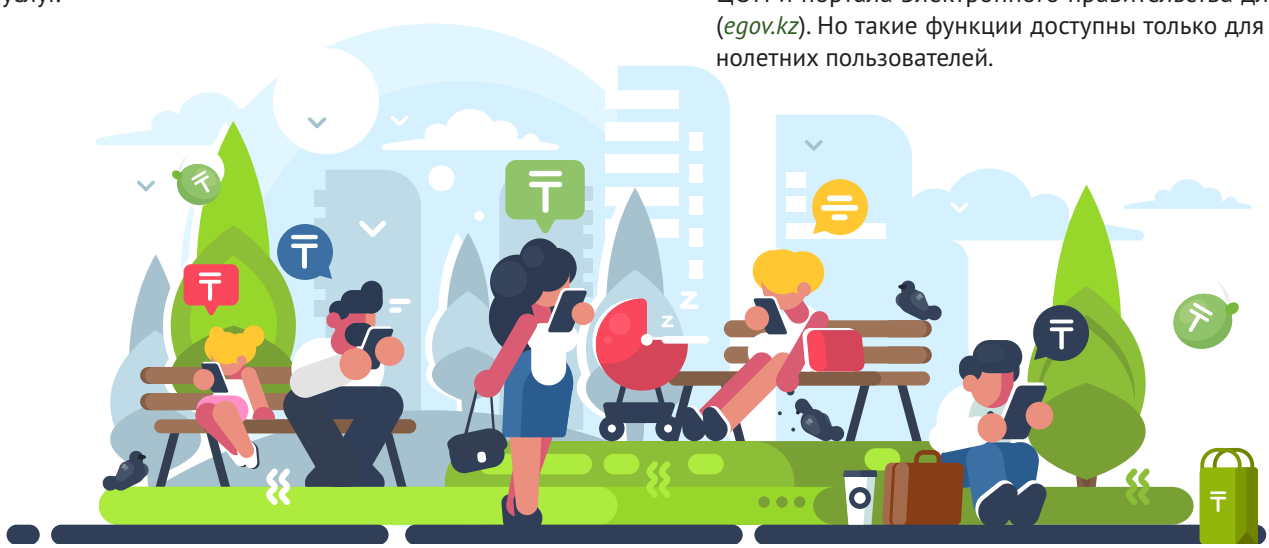
С помощью онлайн-банкинга вы можете получить множество услуг.

1. После регистрации у вас появляется свой личный кабинет. В нём вы можете видеть, сколько денег у вас сейчас на счёте, сколько поступило, а сколько ушло на оплату услуг, товаров или на переводы.

2. В онлайн-банкинге можно просмотреть всю историю ваших онлайн-операций, а также все выписки по вашему счёту (детский счёт привязан к родительскому): то есть куда, кому, за что и когда вы что-то отправляли, а также сколько и в какое время вам поступало денежных средств.

3. Вы можете переводить деньги со счёта на счёт внутри вашего банка, можете заплатить продавцу в магазине, расплатиться с таксистом, перевести деньги на карту родственникам или одноклассникам. Многие банки сегодня предоставляют возможность оплачивать услуги и товары посредством банковского приложения на телефоне через *QR*-код.

Взрослые, в свою очередь, в мобильном банковском приложении могут подать онлайн-заявку на получение дополнительных услуг — к примеру, оформить дистанционно страховку, кредит или открыть депозит. Родители легко оплачивают коммунальные счета с помощью интернет-банкинга, покупают авиа- и железнодорожные билеты, оформляют рассрочки. Через онлайн-банкинг взрослые могут увидеть и оплатить свои задолженности по штрафам и налогам, а также зарегистрироваться как индивидуальный предприниматель, тем самым сделав первый шаг к открытию своего бизнеса. Можно ещё получить различные государственные услуги: к примеру, для пользователей некоторых банков доступны отдельные услуги ЦОН и портала Электронного правительства для граждан (*egov.kz*). Но такие функции доступны только для совершеннолетних пользователей.



Школьникам же с помощью онлайн-банкинга удобно отслеживать свои ненужные траты: можно всерьёз заняться планированием своего бюджета, ставить финансовые цели и копить деньги на что угодно — на велосипед, скутер, новую одежду, подарок близким и т. д. А ещё лучше — попросите родителей открыть новый депозит в их мобильном банковском приложении. Вы сможете откладывать на него деньги из своих карманных расходов, переводить деньги со своего счёта на счёт родителей через онлайн-банкинг, а заодно проверять, сколько вознаграждения по вкладу начислил банк. Сумма будет увеличиваться, вместе с ней будет расти и ваш стимул копить деньги дальше.

Следует отметить, что банки устанавливают различные комиссии за свои услуги, к примеру, за переводы на карты других банков, открытие счёта и так далее. Поэтому изучите эти расценки заранее, чтобы не оказалось так, что вам не хватает нужной суммы, потому что её «съела» банковская комиссия.

Также банки стимулируют клиентов пользоваться услугами их онлайн-банкинга, и за это дают специальные бонусы — **кешбэк** — в виде баллов или денег. С каждой операции и покупки они накапливаются, и ими потом можно будет расплатиться в магазине или пополнить баланс. Все перечисленные возможности доступны не всем пользователям. У разных банков разный функционал в онлайн-банкинге, особенно для детей, на чьё имя открыта банковская карта.

Финансовые мошенники в интернет-пространстве

Все же помнят, что у каждой медали есть обратная сторона? В онлайн-банкинге это персональная безопасность ваших данных.

От вашей осторожности при проведении финансовых онлайн-операций зависит сохранность средств на счёте.

С развитием дистанционного банкинга начали активно вести свою работу и финансовые мошенники, которые придумывают и внедряют различные схемы обмана людей, чтобы получить онлайн-доступ к их деньгам. Немало людей пострадало от действий таких преступников, когда все деньги автоматически списывались со счёта при переходе клиента банка по незнакомой ссылке, при ненадёжном пароле мобильного приложения и так далее.

Сами банки, конечно же, предпринимают всевозможные меры для защиты своих систем от взломов киберпреступников, сохранения безопасности данных клиентов. Но во многом безопасность в онлайн-режиме зависит и от самих пользователей банкинга. Зачастую они сами разглашают и публикуют секретные данные: полные реквизиты своей платёжной карты, в том числе код на оборотной стороне, SMS-код, пин-код и другие личные сведения.

Какие обычно схемы используют мошенники?

Злоумышленники могут предлагать свои товары или услуги в интернете на различных сайтах по невысокой цене и с обещанием быстрой доставки. Клиент «клюёт» на приманку, его просят перевести онлайн частичную или полную предоплату на счета, которые обычно оформлены на третьих лиц. Ну а после получения предоплаты заказы не выполняются. Найти таких преступников очень сложно, так как покупатель не знает, с кем он именно общался, его данные.

Часто мошенники звонят клиентам различных банков, представляясь сотрудниками службы безопасности. Они сообщают, что по карте клиента якобы происходят подозрительные финансовые операции и чтобы их заблокировать, нужен трёхзначный номер на обороте платёжной карты. Получив эти три цифры, преступники подключаются к интернет-банкингу и за считаные минуты похищают все деньги с онлайн-счетов клиента. Ведь чтобы использовать карту клиента в своих целях, мошенникам нужно узнать её номер, имя владельца, срок действия, номер *CVC* или *CVV* (это те самые три цифры на обороте любой платёжной карты — они расположены в поле для подписи владельца карты или рядом с ним).

Финансовые мошенники могут позвонить или отправить *SMS*-ку: мол, ваш абонентский номер победил в конкурсе компании. Приз предлагают забрать из другого города или получить деньгами на банковскую карту. Конечно, большинство выбирает второй вариант. Мошенники, опять же, запрашивают личные данные человека, просят скачать разные приложения, позволяющие подключить на их устройстве интернет-банкинг, и похищают деньги.

Ещё одна распространившаяся в наши дни схема — преступники притворяются покупателями. Они отправляют на телефон продавца ссылки, ведущие на фишинговые сайты, чтобы он ввёл там данные для оплаты товара.

И тогда деньги могут автоматически списаться с его счёта без ведома владельца платёжной карточки.

Дети для таких мошенников — лёгкая нажива. Используя различные психологические приёмы, злоумышленники могут выведать у детей конфиденциальные данные их родителей: ИИН, ФИО, данные карты и другую информацию — и оформить на взрослых онлайн-кредиты.

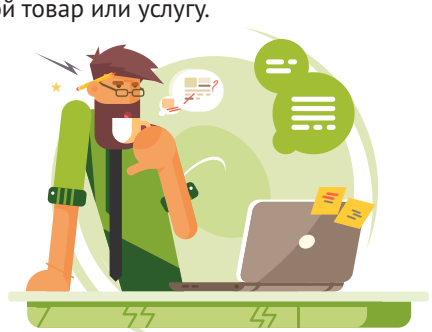
Как обезопасить себя и не стать жертвой мошенников?

В первую очередь, ни в коем случае нельзя никому сообщать персональные данные свои или родителей, в том числе реквизиты пластиковых карт. Не передавайте коды и кодовые слова.

Нельзя доверять непроверенным и сомнительным источникам информации, особенно в интернете. Мошенники могут выдавать себя за вашего ровесника, чтобы войти в доверие. Всегда проверяйте любую информацию, которая касается денежных вопросов, всегда советуйтесь со взрослыми, своими родными и близкими.

Без проверки нельзя производить предоплату за товар — договоритесь об оплате после его получения.

Если вы сомневаетесь в том, что покупатель или продавец с вами искренен, если вам кажется, что он пытается вас обмануть, то доверьтесь своей интуиции и приостановите или отмените сделку. Всегда можно подождать. Пока деньги у вас, вы хозяин положения, и вам решать, стоит или нет покупать тот или иной товар или услугу.



Никогда не переходите по сомнительным ссылкам. Повторимся: деньги со счетов могут автоматически снять мошенники, используя ваши личные данные. Не перезванивайте на незнакомые номера. Все неизвестные вам сайты проверяйте через интернет, смотрите отзывы, анализируйте информацию.

Если вам говорят, будто вы что-то выиграли или с вашей карты случайно банк списал деньги, и нужно назвать свои данные, чтобы заблокировать операцию, сразу же завершите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты. Или попросите сделать это взрослых.

Чаще меняйте пароли доступа к услугам своего онлайн-банкинга, попросите родителей установить антивирус на гаджете.

Регулярно проверяйте движение денег на своих счетах — сколько средств и когда поступило и израсходовано.

Если вы покупаете что-то через интернет, никому не сообщайте секретный код для подтверждения операций. Обычно он приходит по *SMS*.

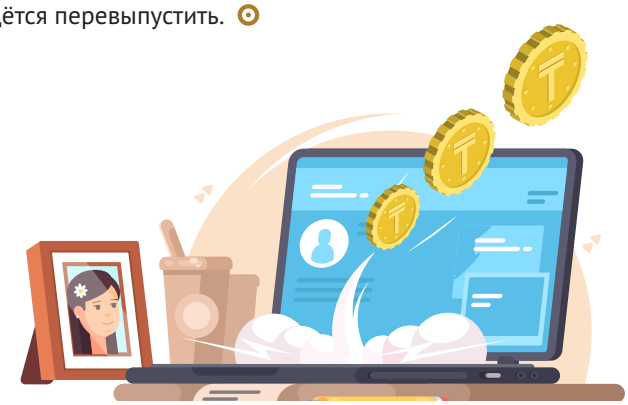
Если вдруг вам пришло *SMS* якобы от банка о зачислении средств на ваш счёт, а затем вам звонит неизвестный человек и говорит, что по ошибке зачислил вам деньги, и просит вернуть, то не спешите этого делать. Скорее всего, это мошенники. Деньги, скорее всего, на самом деле вам не поступили, а *SMS* — поддельное. Сразу проверьте все свои счета, посмотрите выписку в онлайн-банке, или пусть это сделают ваши родители в своём онлайн-банкинге.

Если вам приходит уведомление «Подтвердите покупку» и код на телефон, а потом вам также звонит неизвестный человек, говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, то ни в коем случае не делайте этого.

Преступникам нужен ваш код, чтобы списать с вашего счёта деньги или подписать вас на ненужный платный сервис.

Обычно в банковских приложениях, к которым привязана детская карточка, установлен лимит суммы, которую ребёнок может потратить на онлайн-покупки и перевести кому-либо (например, не более 30 тысяч тенге в месяц). Это сделано в целях безопасности, чтобы сохранить ваши деньги.

Если мошенники пытались взломать ваши личные пароли, использовали ваши личные данные или вы потеряли свою платёжную карту, то сразу нужно проинформировать об этом своих родителей и обратиться в банк. Можно попросить банк временно заблокировать вашу карту, в этом случае её придётся перевыпустить.



КАК СОЗДАТЬ НАДЁЖНЫЕ ПАРОЛИ К СВОИМ АККАУНТАМ В СЕТИ?

Надёжный пароль поможет вам защитить ваши личные данные, сохранить конфиденциальность своих писем, файлов и других материалов и уберечься от мошенников, которые могут попытаться взломать ваш аккаунт.

1. Пароль должен содержать не менее 12 символов. Это может быть любая комбинация букв, цифр и других знаков. Чем длиннее пароль, тем он надёжнее. Это может быть: строка из песни или стихотворения; цитата из фильма или речи известного человека; цитата из книги; значимая для вас фраза; аббревиатура (как вариант — из первых букв каждого слова в предложении).

2. Не используйте пароли, которые легко угадать. Если человек знает вас, то может легко подобрать пароль — например, по данным из ваших соцсетей.

3. Не устанавливайте слишком простой пароль типа *Danik123*, не указывайте в нём своё имя и год рождения. Избегайте личных данных и общеупотребительных слов. Лучше всего установить такую комбинацию, которую вам было бы легко запомнить, но посторонние не могли бы угадать. Чаще меняйте пароли.

4. Храните записанные пароли в надёжном безопасном месте. Если вам требуется записывать пароли, чтобы не забыть их, не оставляйте их в свободном доступе — на столе или мониторе компьютера, в заметках телефона.

Будьте всегда бдительны, совершая какие-либо финансовые операции онлайн. Аккуратнее относитесь к совершению покупок в Сети. И слушайтесь родителей, которые всегда желают вам самого лучшего.

Повышайте свою финансовую грамотность с детства!