Как защитить свои данные

Привет,
это команда Нетологии!

«Мне нечего скрывать» — в прошлом стандартный ответ на вопрос о защите персональных данных в интернете. Этот принцип больше не работает. Средне-статистический пользователь проводит в интернете 6 часов 43 минуты в день: за это время человек заходит на десятки сайтов, заполняет формы регистрации, выкладывает фотографии в соцсети и скачивает файлы.

Если не следить за своими действиями в интернете, данные могут попасть не в те руки: в лучшем случае к маркетологам, которым они помогут продать больше товаров, а в худшем — к мошенникам, которые смогут украсть деньги у вас и ваших близких.

Этот гайд — проводник в мир безопасности в интернете. В нём мы подробно разберём, какие угрозы существуют и как их избежать. А заодно расскажем, как правильно делать покупки в интернете.

Что внутри

Мы на связи:

Часть

01

Угрозы

Почему следить за своими данными важно

Данные хранятся на подключённых к интернету серверах, их покупают, продают, используют разно-образными способами, а иногда и воруют. Вот что случится с разными типами личных данных, если они окажутся в руках мошенников.

1. Получили данные карты

Реквизиты банковской карты — секретная информация, которую нельзя сообщать друзьям, покупателю на «Авито» и даже сотруднику банка. К реквизитам относится всё, что написано на карте: номер из 16 цифр, фамилия и имя владельца, срок действия и трёхзначный код на обратной стороне карты, CVC. В их число входят и СМС, которые приходят от банка.

Что может случиться, если эти данные окажутся у мошенников? Меньшая проблема — банк заблокирует карту, как только узнает, что реквизиты попали в чужие руки.

Дальше всё зависит от того, какие именно данные получили хакеры. Рассмотрим возможные ситуации по порядку:

- номер карты и ФИО владельца — ничего;
- номер карты, ФИО и срок действия — совершить покупки в некоторых интернет-магазинах (например, на Amazon);
- номер карты, ФИО, срок действия и CVC — купить билеты на автобус или самолёт, забронировать отель на Booking.com или airbnb, привязать карту к платёжной системе (например, google play), оплатить заказ на Aliexpress или eBay;
- номер карты, ФИО, срок действия, CVC и код из СМС — совершить любую покупку в интернете и перевести деньги.

2. Знают личные данные

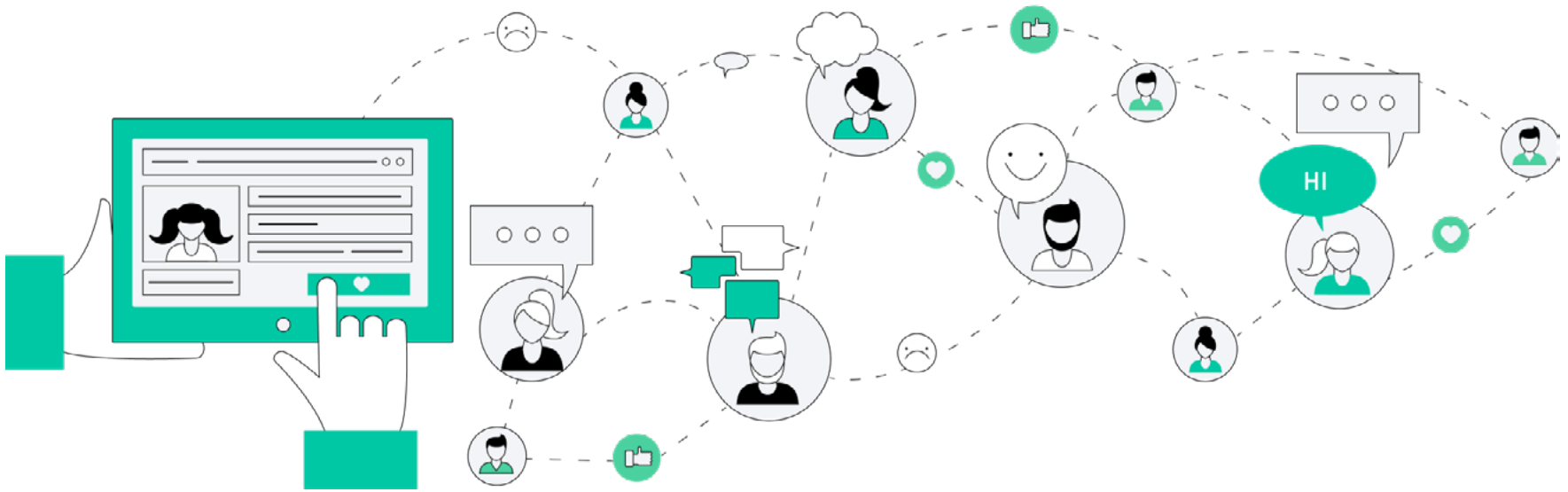
Личные данные — это дата рождения, ФИО, данные паспорта и других документов, селфи, фотографии билетов, домашний адрес, клички домашних животных и другая информация о вас.

Люди постоянно делятся этими данными в интернете: когда оставляют заявку на кредит, регистрируются в социальной сети или получают скидочную карту в супермаркете. И их кража не менее опасна, чем похищение данных карты.

Хакеры могут поменять пароли. Если у мошенников есть достаточно личной информации о вас, они могут сбросить пароли в соцсетях, ответив на секретные вопросы и назвав девичью фамилию вашей матери или предыдущий адрес, по которому вы проживали. Иногда взломщики предлагают вернуть доступ к аккаунту за деньги: в противном случае они обещают опубликовать конфиденциальную информацию о вас, ваших близких или друзьях.

Притвориться вами. Для этого мошенникам достаточно получить доступ к вашему имени, фамилии и отчеству, дате рождения, информации о привычках и фактам биографии. Они могут «украсть личность»: другими словами, войти в доверие к друзьям или родственникам, попросить у них деньги или услуги.

Запустить фишинг от вашего имени. Если злоумышленники знают адрес вашей электронной почты, они могут создать похожий и писать с него письма со ссылками на заражённые сайты от вашего имени друзьям и родственникам. Жертвой можете стать и вы сами — мошенники смогут отправлять персонифицированные письма с вредоносным кодом или ссылками на заражённые вирусом ресурсы, например, от лица знакомого или компании, клиентом которой вы являетесь.



3. Следят за вашими профилями в социальных сетях

Если вы выкладываете в социальные сети фотографии документов, билетов и снимки, по которым можно легко определить местоположение вашего дома, то назойливая реклама и звонки от незнакомцев с предложением услуг — самое безобидное, что может случиться.

Рекламные модули в мобильных приложениях и на сайтах собирают много информации о владельце устройства: от истории браузера до геолокации. Это помогает рекламодателю повысить эффективность рекламы, которая массово показывается пользователю, и продавать больше.

Иногда личная информация может использоваться для динамического ценообразования: когда один и тот же товар для разных людей стоит по-разному. Например, сервис заказа такси Uber знает, что вы согласитесь заплатить больше, если у вашего телефона садится батарея. Компании умалчивают факты динамического ценообразования, поэтому понять, насколько широко оно используется, сложно. Важно знать, что этот феномен существует.

Мошенники могут воспользоваться информацией, чтобы совершать противоправные действия с недвижимостью, взять кредит от вашего имени или просто предоставить информацию третьим лицам, которые могут вмешаться в вашу личную жизнь.

Три самых распространённых угрозы

Надеемся, что теперь вы относитесь к безопасности своих данных серьёзнее. Разберёмся, какие категории угроз существуют — это поможет понять, с каким видом мошенничества вы столкнулись и найти самый эффективный способ защиты.

1. Сайты-клоны

Мошенники создают точные копии известных сайтов — например, банков, сервисов по поиску работы, отелей или интернет-магазинов, — и используют их для кражи данных и денег у случайных пользователей.

Адрес сайта-клона часто очень похож на оригинальный — например, sber.bank.ru вместо sberbank.ru. Поэтому важно внимательно читать адрес.

Например, осенью 2020 года злоумышленники создали 1,5 тысячи копий сайта издания «РБК» (rbc.ru) с доменами в виде rbk-***.ru. На их главных страницах был опубликован материал со ссылкой на мошеннический сайт — там пользователю предлагали заработать на торговле нефтью и газом. Перед покупкой акций нужно было заполнить форму с личными данными.

Сколько пользователей стало жертвами мошенничества, неизвестно, но такие схемы кражи данных и денег распространены достаточно широко, чтобы их стоило опасаться

2. Фишинг

Эксперты по кибербезопасности считают, что сейчас фишинг переживает свой расцвет: суммы, которые мошенникам удаётся украсть с помощью рассылки писем со ссылками на вредоносные ресурсы или поддельных СМС от банка, растут с каждым годом.

Цель фишинга — кража личных данных пользователя. Например, когда человеку звонят и сообщают, что с его карты сняли какую-то сумму денег, но операцию можно отменить, если он назовет данные карты, — это фишинг, а звонящий — мошенник. То же касается писем о выигрыше в лотерею или наследстве в другой стране. Обе ситуации возможны, но встречаются крайне редко, поэтому важно проверять информацию и не совершать поспешных действий.

Если речь идёт о письме, сверьте адрес электронной почты с официальным. Если о звонке из банка, перезвоните в банк сами.

3. Овердоход

В эту категорию входят все предложения о вложении денег на определённый срок, выгода которых слишком велика.

В 2020 году средняя доходность рублёвых вкладов в России не превышает 7% годовых, в долларах и евро составляет не более 4% годовых. Если вы видите предложение с гарантированной доходностью выше — это повод задуматься. Если доходность около 100% и более, перед вами финансовая пирамида или иной вид мошенничества.

Вот реальные схемы обмана в интернете:

Прежде чем перейти к методам защиты личных данных, закрепим знания об угрозах на нескольких реальных схемах обмана в интернете. На эти уловки ведутся даже опытные пользователи, — а кто предупреждён, тот вооружён.

Пройдите опрос (и получите 5000 рублей)

За последний год доходы россиян значительно сократились. Мошенники воспользовались ситуацией, чтобы под видом лёгкого заработка собирать личные данные и деньги.

Схема выглядит так: в рекламном посте пользователя приглашают принять участие в опросе, а взамен предлагают 3 000 или 5 000 рублей. В опроснике нужно указать имя и фамилию, адрес регистрации и фактического проживания, дату рождения, почту и другие личные данные, а также ответить на несколько общих вопросов.

В конце организатор предлагает перечислить небольшую сумму денег — «пошлину» — или совершить тестовый платёж в размере 269 рублей. Вознаграждение никто не получает, а пользователи теряют деньги и личные данные.

Ложный покупатель на «Авито»

На «Авито», «Юле» и других платформах для продажи б/у вещей на объявления часто откликаются мошенники. Они задают несколько поверхностных вопросов о товаре, а затем пишут, что живут далеко и сами забрать заказ не смогут, поэтому пришлют за ним курьера или таксиста. Деньги обещают перевести на карту.

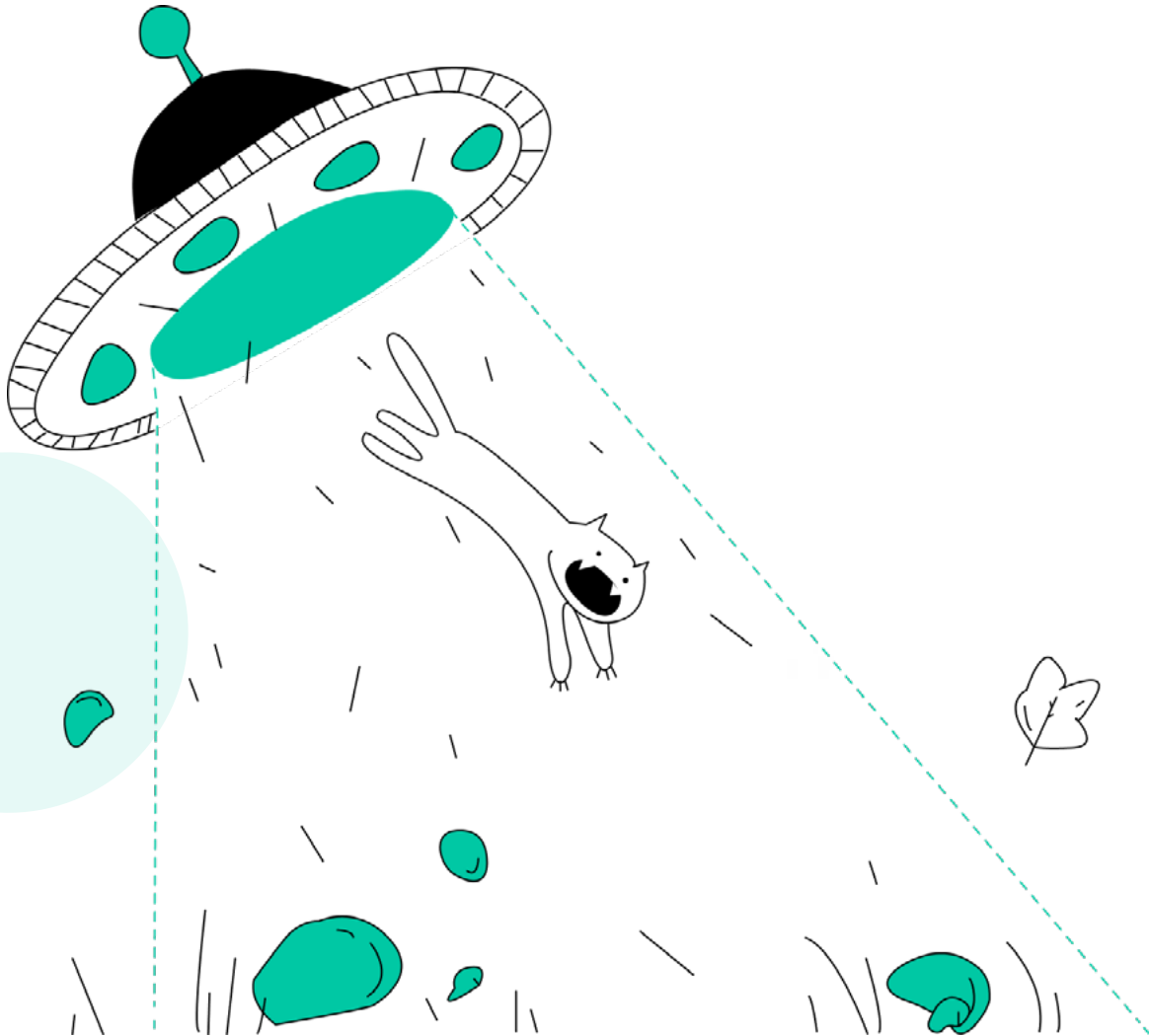
Когда курьер приезжает за заказом, покупатель просит реквизиты карты для перевода денег: но не только номер, но и дату выдачи, имя владельца и код из СМС от банка. Часто это происходит в условиях спешки, когда рядом стоит раздражённый таксист или курьер. В результате мошенник покупает товар и распоряжается данными с вашей карты на своё усмотрение.

Родственник в беде

Вот что бывает, когда мошенники узнали пароль соцсетей или смогли ответить на контрольные вопросы. На странице пользователя появляется сообщение, что близкий родственник серьёзно болен, попал в аварию или арестован. Срочно нужны деньги — перевести их можно на карту, указанную мошенниками в конце поста.

Тесты и вакцины от COVID

Один из трендов пандемии — объявления с поддельными наборами для тестов на COVID в домашних условиях и продажей несуществующих вакцин. Кроме того, мошенники могут попытаться украсть персональные данные пожилых людей под видом заполнения опросника на участие в испытаниях вакцины от коронавируса.



Часть 02

Как защититься?

Во второй главе расскажем, как защитить себя в интернете. Сначала речь пойдёт об общих принципах защиты, а затем разберёмся, как правильно покупать в интернете и что делать, если вашу технику взломали мошенники.

Общие меры

Защитите почту

При регистрации на сайтах и в социальных сетях пользователя всегда просят указать электронную почту. Это означает, что с её помощью можно получить доступ к учётным записям: сбросить пароли и изменить их. Иногда для этого даже не нужно отвечать на контрольные вопросы.

Кроме социальных сетей, к почте привязан мобильный банк — то есть кроме личных данных вы можете лишиться и денег. Лучший способ защитить свою основную почту — создать специальный аккаунт, который будет использоваться для регистрации на сомнительных сайтах, приложениях для знакомств и других сервисах, которым вы доверяете не до конца.

Установите сложные и разные пароли

Сложные пароли — один из лучших способов защитить свои данные. В 2019 году самым популярным в мире паролем был «123456», на втором месте — «12345678». Не используйте их, а также дату рождения, имя и фамилию, имена близких и домашних животных.

Оптимальный пароль — тот, который вы сможете запомнить, но его трудно угадать мошенникам или алгоритмам для подбора паролей. Лучше всего подойдёт длинная фраза: например, nomonkeyisnotagoodpassword («нетобезьянаэтоплохойпароль»).

Хорошо, если в пароле есть цифры, буквы и специальные знаки — двоеточие, восклицательный знак, точка, дефис и другие. Такой пароль можно сгенерировать; выглядеть он будет, например, так: P#JOfnPBd. Да, такой набор символов сложно запомнить. Для этого существуют сервисы хранения паролей: например, 1Password, Bitwarden или Dashlane.

Не стоит использовать один и тот же пароль для всех аккаунтов. Лучше всего придумать собственный для каждого аккаунта или хотя бы защитить надёжными почту и мобильный банк.

Используйте двухфакторную идентификацию

При двухфакторной идентификации кроме пароля для входа в учётную запись нужны дополнительные данные: например, код из СМС или ответ на секретный вопрос.

Такие меры сильно осложняют задачу мошенникам, которым удалось украсть ваш пароль. Скорее всего, они не будут тратить время на ваш аккаунт и займутся взломом менее защищённых.

Установите антивирус

Пользуйтесь антивирусными программами — они защитят ваш компьютер или смартфон лучше, чем самые надёжные пароли. Бесплатные версии есть у «Касперского», Avast, Dr. Web и Avira.

Доверяйте своей антивирусной программе. Если она считает, что открывать сайт или скачивать файл не стоит, лучше всего так и поступить.

Обновите приложения и проверьте разрешения

Приложения и сервисы периодически требуют обновлений: с их помощью разработчики исправляют ошибки и устраняют недочёты, которыми мошенники могут воспользоваться для сбора личных данных.

Каждое приложение обновляется в разное время — за этим может проследить ваш смартфон, если включить на нём автообновление. Отсутствие обновлений — одна из причин отказаться от использования пиратских программ.

Важно обращать внимание на разрешения приложений: некоторые из них запрашивают данные об электронной почте или доступ к камере, фотогалерее и микрофону. Не давайте разрешений автоматически — следите за тем, какую информацию запрашивает приложение. В некоторых случаях разумнее вообще отказаться от его использования, чтобы не передавать личные данные о себе неизвестным лицам.

Не рассказывайте о своих планах и не публикуйте документы

Публиковать фотографии документов, билетов и чеков — плохая идея. То же касается рассказов о планах уехать в отпуск или пойти в ресторан.

Мошенники могут воспользоваться этой информацией: по данным из посадочного талона можно зайти в личный кабинет на сайте авиакомпании и получить доступ к паспортным данным, а потом взять на них онлайн-кредит. Обычных домушников ваша открытость тоже наверняка обрадует — они смогут точно узнать, когда вас не будет дома.

Как правильно покупать в интернете

Каким магазинам доверять, а каким — нет?

Лучше всего покупать на сайтах интернет-магазинов, которые вам знакомы — например, у них есть офлайн-магазины («М.Видео», «Спортмастер», «Связной» и другие) или это крупные онлайн-ритейлеры (Ozon, Lamoda или «Яндекс.Маркет»).

Иногда цена в малоизвестном магазине сильно отличается от цены у крупного ритейлера. В этом случае стоит обращать внимание на отзывы. Лучше всего смотреть их не на сайте магазина, а на сторонних сервисах: например, на «Отзовик» и «IRecommend».

Стоит обратить внимание как на количество отзывов (если их мало, лучше купить в проверенном месте), так и на мнение других покупателей о качестве товаров, условиях доставки, возврата товара и денег.

Убедитесь, что магазин — тот, за кого себя выдаёт

Мошенники часто подделывают сайты интернет-магазинов в надежде, что пользователь не заметит подвох и введёт реквизиты своей карты. Несколько советов, как не попасться на такую уловку:

1. **Внимательно читайте адрес сайта.** Часто мошенники меняют одну или несколько букв в домене — мы уже рассказывали об этом в первой главе. Если сомневаетесь, скопируйте адрес сайта в поисковую строку — поддельный сайт в поисковой выдаче будет располагаться ниже, чем оригинальный.
2. **Следите за замком.** На настоящем сайте интернет-магазина установлен протокол безопасности https — он защищает данные пользователей от утечек и краж. О наличии шифрования свидетельствует значок замка — чаще всего он расположен слева от строки с адресом сайта. Важно отметить, что само по себе наличие значка не означает, что сайт безопасен — мошенники уже нашли способ получать их.
3. **Проверьте информацию о продавце.** Этот пункт самый скучный, но не менее важный. У добросовестных продавцов в разделе «Контакты» всегда есть номер телефона для связи, указаны юридический и фактический адреса, а также сведения о компании. Если по телефону вам ответили на вопросы, а по адресу почты вы нашли достаточно отзывов, сайту можно доверять.

Как защитить свою карту

Бывает, что сайты взламывают, а собранные ими данные попадают в руки мошенников. Это касается и реквизитов банковских карт. Поэтому для покупок в интернет-магазинах можно завести отдельную карту и отправлять на неё только небольшие суммы денег для совершения конкретной покупки.

Если мошенники получат доступ к этой карте, они не смогут ничего снять или потратить — ведь деньги на ней не хранятся. Ваша основная карта остаётся в безопасности.

Как выбрать продавца на маркетплейсе

Маркетплейсы — например, Ozon, «Авито» или Aliexpress — отдельная категория магазинов: на них есть множество продавцов, каждый из которых продаёт определённые товары. Разные продавцы могут продавать один и тот же товар — цена и качество у них могут сильно отличаться. Вот несколько советов, как не ошибиться при покупке.

Читайте отзывы. Универсальный совет при покупках в интернете, напомнить о котором никогда не лишне. Если речь идёт о платформах для продажи б/у товаров, можно посмотреть, какие предметы продавал человек и как часто он это делал. Если о классических маркетплейсах, стоит следить за количеством продаж и отзывами на товары.

Будьте осторожнее с предоплатой за товар. Если на маркетплейсах оплачивать покупку заранее вполне безопасно, то на платформах для продажи б/у товаров нужно настаивать на наложенном платеже. Другими словами, вы оплатите товар, как только получите его и убедитесь, что он физически существует. Мошенник, скорее всего, откажется от такого предложения.

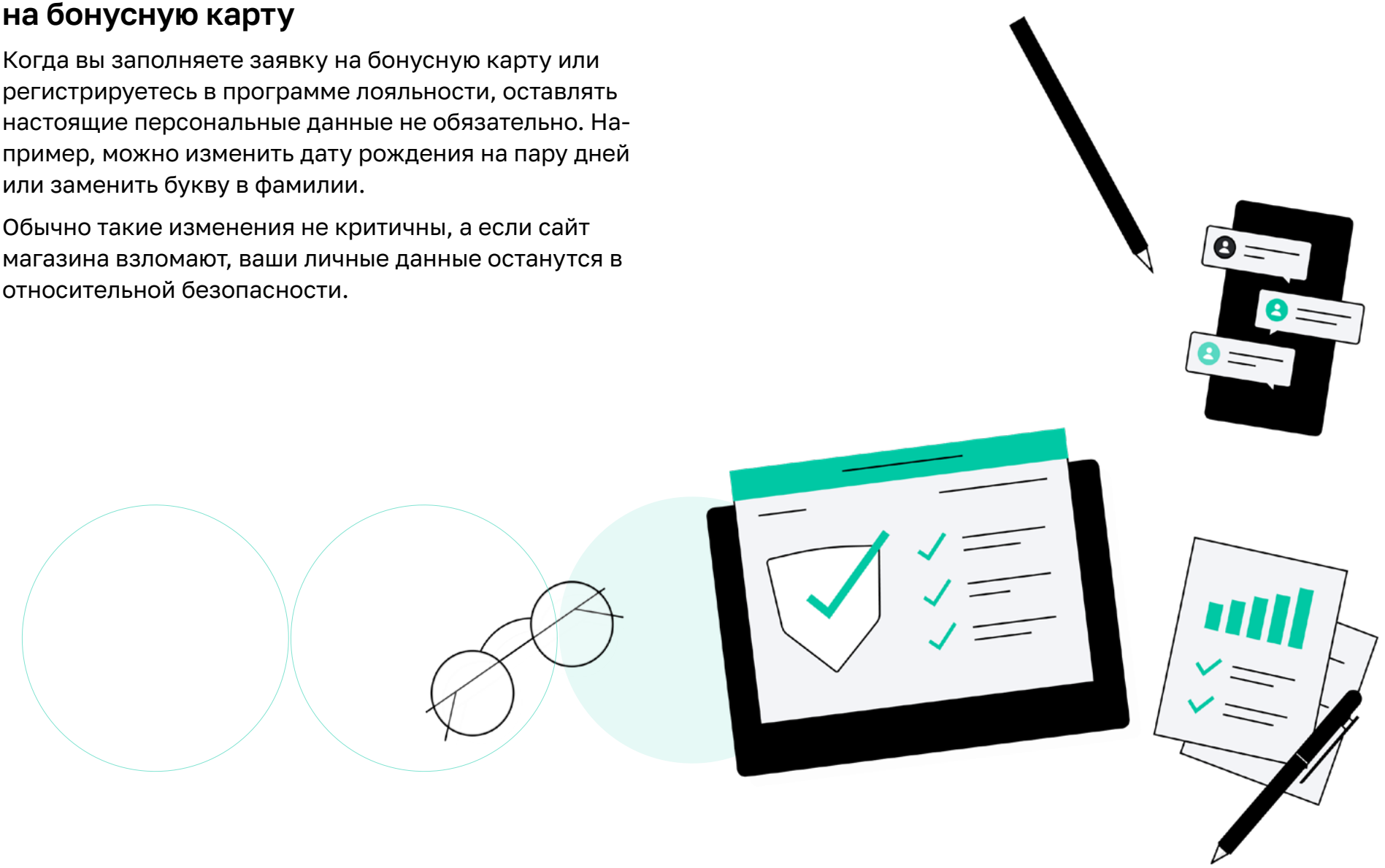
Никому не сообщайте реквизиты банковской карты. Об этом мы тоже рассказывали выше. Окончательно закрепим: для перевода денег достаточно номера карты; сообщать другие реквизиты не нужно.

Не отправляйте деньги на кошелёк «Киви». Мошенники часто пользуются этой платёжной системой из-за её особенности — проводить платежи на небольшие суммы на ней можно без регистрации. Другими словами, найти получателя потом будет очень сложно: даже платёжная система почти ничего о нём не знает.

Как заполнять заявку на бонусную карту

Когда вы заполняете заявку на бонусную карту или регистрируетесь в программе лояльности, оставлять настоящие персональные данные не обязательно. Например, можно изменить дату рождения на пару дней или заменить букву в фамилии.

Обычно такие изменения не критичны, а если сайт магазина взломают, ваши личные данные останутся в относительной безопасности.



Что делать, если взломали соцсеть, смартфон или компьютер

Смартфон заблокирован, взломщик требует выкуп. *Такая проблема чаще всего возникает у владельцев iPhone: на экране появляется баннер, который блокирует любые действия с телефоном. Чтобы разблокировать устройство, взломщик просит перевести выкуп — от 2 000 до 5 000 рублей.*

Платить хакеру не нужно: скорее всего, телефон после этого не разблокируется, а вы зря потеряете деньги. Если речь идет об iPhone, звоните в поддержку Apple по номеру +7 495 580-95-57 — оператор задаст контрольные вопросы и поможет разблокировать устройство. То же самое касается ноутбуков MacBook.

Если баннер появился на компьютере с Windows, придётся переустановить операционную систему.

Взломали аккаунт в социальной сети, собирают деньги на лечение. *Частая история — мошенники получили доступ к вашему аккаунту и просят перевести деньги на срочную медицинскую помощь после аварии, лечение родственника, на билет или другие нужды. Если это произошло, нужно обратиться в поддержку социальной сети и ответить на контрольные вопросы, чтобы вернуть доступ к аккаунту. Кроме того, стоит позвонить родственникам и друзьям — предупредить, что аккаунт взломан и деньги переводить не нужно.*

Часть

03

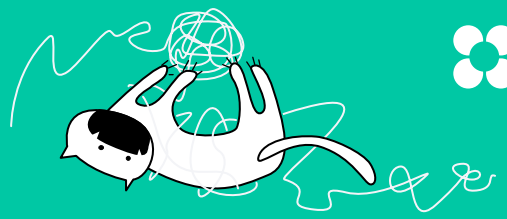
Проверка знаний

Проверьте себя

Небольшое бинго
по кибербезопасности.

Бинго

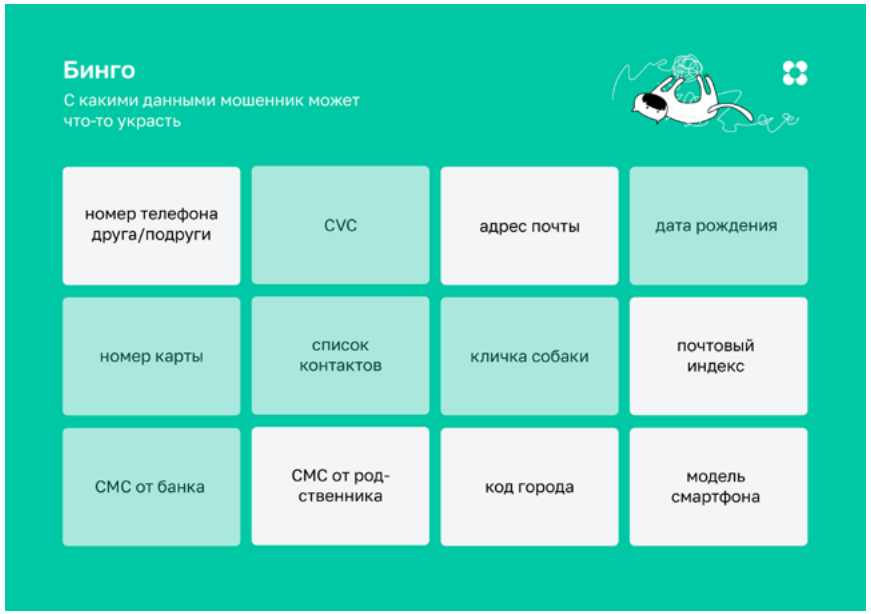
С какими данными мошенник может что-то украсть



номер телефона друга/подруги	CVC	адрес почты	дата рождения
номер карты	список контактов	кличка собаки	почтовый индекс
СМС от банка	СМС от родственника	код города	модель смартфона

Ответы:

CVC, дата рождения; номер карты; список контактов; кличка собаки; СМС от банка



Для подготовки гайда мы использовали следующие источники:

- Мошенничество в интернет-магазинах: как работают основные мошеннические схемы и как от них защититься
- Что хакеры могут узнать о вас по номеру телефона
- Cookie monsters: why your browsing history could mean rip-off prices
- Что такое интернет-мошенничество

Редакторы: Олег Сабитов

Дизайн: Анастасия Волкова