Как совершать безопасные онлайн-покупки: 10 главных правил

Сегодня все большее количество россиян предпочитает делать покупки в интернете. Во-первых, это удобно. Можно выбрать нужный товар, не выходя из дома. Во-вторых, онлайн покупки обходятся, как правило, дешевле. Имеется и еще одно преимущество: в интернете люди нередко приобретают качественные товары «с рук» за небольшие деньги. Существенным недостатком онлайн-шопинга является возможность потери денежных средств по вине злоумышленников.

Мошенники используют самые изощренные приемы, чтобы получить доступ к персональным данным пользователей и завладеть чужими финансами. Важно знать правила безопасной покупки в интернете, не забывать о бдительности при совершении расчетов с онлайн магазинами и оплате различных услуг.

В наш список включены 10 правил, соблюдение которых поможет снизить риск столкновения с мошенничеством.

1. **Для того чтобы онлайн покупки были безопасными, требуется обязательно установить в компьютере или смартфоне надежную антивирусную программу и регулярно ее обновлять. Важно использовать современный браузер последней версии.**

При осуществлении расчетов за покупки с помощью смартфона безопаснее всего использовать банковские приложения для дистанционного обслуживания клиентов («мобильный банкинг»).

1. **Прежде чем оплачивать выбранный товар, необходимо убедиться в подлинности сайта, предлагающего совершить покупку. Мошенники нередко используют сайты-двойники, копируя подлинный дизайн. Подмену заметить непросто, так как «липовый» адрес обычно отличается от настоящего одной**

буквой или дополнительным знаком.

При входе на продающий сайт желательно ввести адрес вручную, проверив его подлинность с помощью поисковых систем. Только после этого можно заносить в заявку данные своей банковской карты. Если воспользоваться скопированной ссылкой, можно попасть на мошеннический сайт.

Желая обмануть доверчивого покупателя, злоумышленники зачастую размещают на фиктивных сайтах сверхвыгодные предложения с нереально большими скидками на покупку товаров, оплату услуг. Такие предложения необходимо оставлять без внимания, так как желанная экономия может обернуться большими неприятностями. Продавец, уверенный в своем товаре и знающий ему цену, не станет необоснованно занижать ее, рискуя потерять доверие клиентов.

Чтобы узнать, безопасна ли интернет покупка в данном онлайн магазине**,** необходимо обратить внимание на предложенные способы оплаты. Если она производится, например, картой одного вида, доверять такому продавцу нельзя.

1. **Рекомендуется делать покупки на серверах, защищенных с использованием протокола https. В отличие от серверов, помеченных в адресной строке символом http, данные пользователей на https сайтах передаются в зашифрованном виде.**

Защищенный сайт можно узнать по значку в виде закрытого замка. Он размещается в начале адресной строки. Если нажать на этот значок, открывается окно с пунктом проверки сертификата безопасности.

1. **Чтобы совершать безопасные покупки в интернете, важно позаботиться о создании надежных паролей для входа в банковскую систему. Они должны составляться из букв разного размера, чередующихся с цифровыми знаками.**

Не рекомендуется использовать одни и те же пароли для входа в электронную почту, социальные сети и онлайн банк. Существуют специальные приложения для создания и хранения секретных ключей, такие как LastPass, RoboForm. Используя подобные «менеджеры паролей» можно обезопасить свои данные, не забивая голову сложными сочетаниями знаков. Пароли разного назначения вносятся в программу-хранилище, для доступа в которое требуется знать ключевой «мастер-пароль», известный только владельцу. Его надо тщательно скрывать от посторонних.

Нельзя использовать такой «ключ» для входа на какие-либо другие сайты.

1. **Важно сохранять конфиденциальность своих персональных данных. Если для входа на продающий сайт требуется регистрация с сообщением адреса проживания, номера паспорта и телефона, это должно насторожить. Зачем разглашать личную информацию, не зная, будет ли совершена покупка вообще?**

Не следует оплачивать покупки с чужого компьютера. Отсутствие должной антивирусной защиты может стать причиной похищения личной информации или ее искажения с помощью вирусных программ.

Мошенники могут легко рассекретить пароли, если покупки совершаются с общественной системы Wi-Fi.

Не рекомендуется входить в систему онлайн банкинга через социальные сети. Следует правильно использовать настройки конфиденциальности, чтобы недобросовестные продавцы не могли получать доступ к профилям клиентов в сетях Facebook , «Одноклассники», «В Контакте» и т. д.

1. **Не следует переходить по неизвестным рекламным ссылкам с предложениями «купить», «продать», «скачать» что-либо. Нередко мошенники используют такие ссылки, чтобы установить на чужой компьютер вредоносные программы, взламывающие или уничтожающие важные данные. Переход по незнакомой ссылке чреват подключением платного приложения, автоматически снимающего деньги с банковской карты.**

Для внедрения вредоносного ПО злоумышленники часто используют электронную почту. Открывая ссылки и документы, содержащиеся в письмах от незнакомых лиц, можно завести в компьютер мошеннические программы.

1. **Не следует соглашаться на предварительную оплату покупок, не имея гарантий на возврат денег в случае отказа от товара, не подошедшего по размеру, качеству или другим параметрам. На некоторых продающих сайтах с хорошей репутацией появилась функция «Безопасная сделка». Продавец получает доступ к деньгам, внесенным на его счет, только после того, как покупатель получает товар и подтверждает согласие на его приобретение.**
2. **Специалисты по интернет-маркетингу, отвечая на вопрос, как безопасно оплачивать покупки в интернете, советуют использовать виртуальные карты, которые оформляют многие популярные банки.**

Удобны и безопасны в использовании обычные карты, защищенные по технологии 3-D Secure. Деньги снимаются с них лишь после того, как владелец подтвердит осуществление операции путем введения SMS кода, приходящего на его телефон. При этом значительно осложняется похищение средств мошенниками в случае попадания к ним реквизитов карты (ее номера, срока действия и кода CVC2/ CVV2). Такие данные, а также приходящие на телефон SMS коды нельзя никому сообщать, так же как и аккаунты электронных кошельков.

Наилучшим вариантом является использование для интернет-расчетов отдельной карты, а не той, на которую перечисляется зарплата, и где содержатся сбережения. Для того чтобы предотвратить похищение всех денег, необходимо установить лимит их максимального выведения с карты.

Безопасные онлайн платежи можно также производить с электронных кошельков.

Непосредственно перед шопингом на такой кошелек или на карту для покупок переводится определенная денежная сумма.

После совершения онлайн-расчетов за покупки желательно сохранять квитанцию. Она может пригодиться при возникновении спорной ситуации, например, в случае повреждения или утери товара при перевозке.

1. **Перед внесением платежей надо предварительно изучить отзывы покупателей, чтобы совершать действительно безопасные онлайн покупки. Если высказываются претензии по поводу качества и доставки товара, лучше не рисковать, приобрести его дороже, но у более надежного продавца.**

Нередко владельцы онлайн магазинов размещают на своих сайтах фиктивные отзывы, написанные за деньги специально привлеченными людьми. О том, что отзывы не настоящие, можно судить по некоторым признакам, таким как: однотипный стиль изложения, преобладание общих слов, а не конкретных фактов.

1. **Необходимо обращать внимание на контактные данные продавца. Магазины, внушающие доверие, всегда размещает их на своих интернет-страницах. Если указан номер телефона, то рекомендуется позвонить по нему и убедиться в том, что магазин реально существует.**