

Будь **#смарт-покупателем!**



Покупатели в Латвии все чаще совершают покупки в интернете.

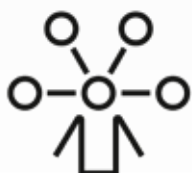


Но важно, чтобы с ростом покупок в интернете жители действовали как смарт-покупатели – распознавали надежные интернет-магазины и выбирали безопасные виды оплаты.



Повседневные покупки в интернете предоставляют удобство, надежность и контроль над тратами.

Кто такой **#смарт-покупатель?**



мыслит и действует в цифровом режиме



часто совершает повседневные покупки в интернете



использует различные платежные инструменты



может распознать надежные интернет-магазины

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Наиболее популярные виды атак – от чего себя защищать?

Вредоносное программное обеспечение



Вредоносные программы разного рода, которые устанавливаются на устройства без ведома пользователя. Атака этого вида позволяет начинать неразрешенные действия на компьютере или смартфоне, чтобы получить ценную информацию, отказать в доступе к хранящимся данным или вообще остановить работу устройства.



Злоумышленники могут использовать Ваши устройства, чтобы осуществлять свои атаки на других и скрывать следы своих действий. Это заставит правоохранительные органы подозревать Вас в совершении этих преступлений. Чаще всего вредоносное программное обеспечение распространяется в приложениях электронной почты, через нелегальные или зараженные веб-сайты, а также с использованием рекламы или ссылок.



Чаще всего мошенники используют приложения электронной почты, нелегальные или зараженные веб-страницы, а также создают заманчивые рекламы и ссылки, чтобы пользователи прошли по ним.

Фишинг



Способ, которым злоумышленники, выдавая себя за банк, коммерсанта, полицию или другое государственное учреждение, стараются получить от пользователя интернета личную, секретную информацию, включая данные кредитных карт или интернет-банка, имена пользователей, пароли доступа и т. д.



Чаще всего Вас посредством электронной почты, телефона или смс приглашают открыть ссылку на веб-сайт, где нужно ввести частные данные, или, например, присылается информация, что Вы получили посылку и нужно доплатить, чтобы ее получить.



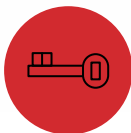
Помните, что банк никогда не попросит Вас отправить свои идентификационные данные по электронной почте, смс или по телефону. Никто не обязан раскрывать такие данные.



Если возникают подозрения, не происходит ли мошенничество во время разговора, немедленно прекратите разговор и свяжитесь с банком или учреждением, из которого якобы звонили.



Взлом или подбор паролей из взломанных баз данных



Самый простой вид взлома паролей – это его угадывание. Люди часто выбирают слишком предсказуемые пароли.



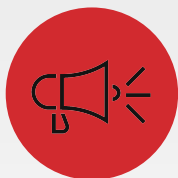
Чтобы получить доступ к паролям, злоумышленники могут взломать базу данных какого-либо веб-сайта и получить информацию о пользователях, также включающую в себя зашифрованные значения паролей, с теми же данными получить доступ к учетным записям пользователей на нескольких веб-сайтах, потому что нередко используется один пароль.



Сегодня просто пароль не считается надежным видом аутентификации. Для большей безопасности необходима многофакторная аутентификация. Для защиты менее уязвимой информации стоит рассмотреть возможность аутентификации с помощью профилей в социальных сетях.

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Наиболее популярные виды атак – от чего себя защищать?



Реклама в интернете

Часто используемым видом мошенничества является размещение рекламы в интернете, например, в популярных социальных сетях – Facebook и Instagram, – предлагающей приобрести продукты со значительной скидкой, например, на 80% дешевле. Обычно товар не доставляется вообще или доставляется неправильный товар.

Сообщения появляются от известных человеку людей (друзей), потому что мошенники разными способами могут находить решения, как разместить эти сообщения в профилях друзей на Facebook и в Instagram, поэтому у людей возникает ощущение, что скидка настоящая.

Мошенничество происходит через некоторое время, когда данные карты клиента используются для других сделок, а первая покупка была предназначена для кражи данных карты.



Инвестиционное мошенничество

Популярный вид мошенничества, когда агрессивным способом (обычно по телефону) покупателя убеждают инвестировать деньги, обещая неслыханную и надежную прибыль.

Клиент верит предложению мошенника, производит денежные переводы, не ознакомившись с фактическими условиями сделки и сервиса, таким образом сам давая согласие.

К сожалению, распространена практика, когда мошенники выманивают данные карт, обещая, что инвестируют от имени клиента и обеспечат большую прибыль за короткий промежуток времени. Когда мошенники получают данные карты, они используют их для приобретения различных товаров – мошенничества. В инвестиционном мошенничестве обычно наибольшие объемы денег.

Всегда будьте подозрительны, если обещаются надежные вложения с быстрой и невероятно хорошей прибылью.



Мошенничество с ложными займами

Людам, которые ищут заем (в объявлениях или иным способом), звонят и уверяют, что необходима проверка в базах данных Службы государственных доходов или, например, кредитных регистрах, и для этого необходимо назвать коды доступа к интернет-банку, подтвердить действия в мобильном приложении или назвать данные карт.

При первых подозрениях, что во время разговора происходит мошенничество, немедленно прекратите разговор и сами свяжитесь с учреждением, из которого Вы якобы получили вызов.



Поддельные лотереи

Очень распространенный вид мошенничества, при котором человеку предлагается принять участие в лотерее популярных смартфонов или других желанных брендов в социальных сетях или где-либо еще. Часто в таких поддельных лотереях требуются данные платежных карт пользователя.

Помните, свои пароли и банковские данные никому нельзя раскрывать!

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Как распознать безопасный интернет магазин?



Проверьте название веб-сайта и ссылку

нет ли в ней лишних знаков или символов, взятых из другого алфавита, например, «e», а на поддельном веб-сайте узнаваемое название написано с «ё». Именно поддельные веб-сайты, которые выглядят как официальный сайт организации, являются одним из наиболее частых способов, как мошенники пытаются обмануть покупателей, чтобы получить данные доступа или другую ценную информацию для перепродажи на черном рынке.



Убедитесь, что вы используете безопасное интернет-соединение

Об этом свидетельствует находящееся перед ссылкой обозначение HTTPS, а также иконка замка или щита в окне адреса. Но это не единственный аспект, на который нужно обращать внимание, так как злоумышленники становятся более изобретательными, и опасные веб-сайты тоже могут быть отмечены этим видом соединения. Безопасное соединение еще не свидетельствует о надежности веб-сайта.



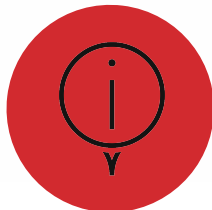
Проверьте репутацию предприятия и отзывы других покупателей перед совершением покупки

В надежном интернет-магазине будет легко доступная и понятная информация о предприятии, в том числе контактная информация в случае вопросов, и объяснение права вернуть товар. Нужно также обратить внимание на то, насколько старые указанные отзывы, не слишком ли они одинаковые, так как нередко фальшивые предприятия сами обеспечивают такого рода контент о себе. Безопаснее выбирать широко известные местные и зарегистрированные в Европейском союзе магазины.



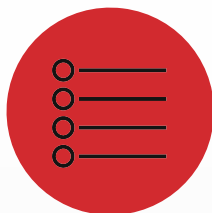
Не принимайте слишком заманчивые предложения, которые кажутся несоразмерно выгодными

Мошенники знают, что люди охотно используют возможность приобретать товары, особенно известных брендов, по более выгодной цене, поэтому стоит проявлять осторожность, если в рекламе рассказывает о предложении со скидкой, например, 90%.



Убедитесь,

указаны ли условия оплаты и доставки, право на отказ, предоставлено ли описание товара, а также обеспечена ли связь с клиентом.



Ознакомьтесь

с Черным списком и Списком подозрительных веб-сайтов Центра по защите прав потребителей (ЦЗПП).

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Надежные пароли для безопасности данных

Самый простой способ защитить свои данные – выбирать надежные и уникальные пароли для каждого веб-сайта.



Для дополнительной безопасности также рекомендуется использовать двухфакторную или строгую аутентификацию, которая требует подтверждать доступ еще каким-либо образом, например, отправкой смс с уникальным кодом подключения или использованием приложения для аутентификации.

Надежный пароль – длинный: не менее 14-16 символов, включая буквы, цифры, другие символы. Чтобы было легче запомнить, можно использовать так называемые парольные фразы, включающие в себя, например, известные тебе слова песни или стихотворения, цифры и символы.



Если длинный пароль трудно придумать и запомнить, эксперты рекомендуют использовать автоматически сгенерированные пароли. Менеджер паролей – это вид приложения, доступный на смарт-устройствах, в котором можно хранить разные пароли в зашифрованном виде, чтобы не забывать их.

Нужно помнить, что необходимо позаботиться о надежной защите хранимых паролей, установив соответствующую аутентификацию/шифрование на защищаемые пароли, а также на устройство.



ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Безопасные методы оплаты в интернете



Всегда используйте безопасные средства оплаты, например, банковскую карту или соединение с интернет-банком.



Совершайте покупки в интернет-магазинах, где для платежей используется надежная, или двухфакторная аутентификация. Это свидетельствует о том, что коммерсант высоко ценит безопасность платежей.



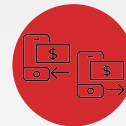
Если за товар нужно рассчитаться, произведя оплату счета до получения товара, подумайте дважды. В этом случае, если произойдет мошенничество, вернуть деньги с помощью банка Вы не сможете.



Платите только тогда, когда Вы подключены к безопасному интернет-соединению – избегайте использования открытой, публичной сети Wi-Fi.



Используйте для оплаты надежное устройство, обновления программного обеспечения которого были выполнены не ранее, чем в последние 3 месяца.



Следите за движением денежных средств на своем счету – для дополнительного контроля включите уведомления в мобильном приложении. По необходимости меняйте лимит оплаты.



Оплата картой

● Оплата картой является одним из любимых клиентов методов оплаты в интернете, безопасным и проверенным способом расчета. Mastercard – самые популярные в Латвии платежные карты. Более 80% всех выпущенных карт – именно Mastercard.

● О безопасности оплаты картами заботятся как эмитенты карт, так и банки, и коммерсанты. Каждый пользователь карты также должен заботиться о безопасности своей карты.

● Банки предлагают удобно подключать и отключать в интернет-банке платежи картой в интернете. Перед осуществлением покупки включите функцию безопасных электронных покупок, а затем отключите ее.

● На покупки платежной картой распространяется гарантия платежей картами, которая дает клиенту возможность обратиться в банк в случае несанкционированных и мошеннических платежей.

● С точки зрения оплаты наиболее безопасными в интернете являются те интернет-магазины, которые поддерживают для платежей картами надежную или двухфакторную аутентификацию, например, пароль и еще какой-либо дополнительный вид удаленной аутентификации. Это подтверждает, что продавец высоко ценит безопасность платежей и, вероятно, позаботился о других аспектах безопасности своих ИТ-систем.

● В электронной коммерции двухфакторная аутентификация для платежей, например, пароль и E-Mobile или SmartID, является знаком гарантии, что магазин надежен. Двухфакторная или строгая аутентификация – это как прослойка безопасности, помогающая предотвратить несанкционированные расчеты картами в интернете и защищающая от мошенничества. Пользователям карт Mastercard важно обращать внимание на наличие логотипа Mastercard Identity Check.



Соединение с интернет-банком (BankLink)

● Безопасное подключение к интернет-банку является одним из любимых клиентов методов оплаты в интернете, свидетельствует опрос жителей Латвии. Клиент после выбора товара или услуги направляется на уже заполненное платежное поручение в своем интернет-банке или мобильном приложении.

● BankLink обеспечивает, что коммерсант может подготовить платежное поручение непосредственно в интернет-банке покупателя, а клиент может незамедлительно подтвердить его.

● Нужно принимать во внимание, что перевод BankLink не гарантирует возврат денег в случае мошенничества. Если товар или услуга не поставлены, деньги нельзя будет вернуть с помощью банка.

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Как действовать, если товар не доставлен?



При использовании платежных карт вероятность вернуть деньги в случае мошенничества или некачественно доставленного товара выше.



Если товар не доставлен, сначала свяжитесь с продавцом. Возможно, есть некая объективная причина, почему доставка товаров задержалась.



Если ответа нет или не удастся договориться о решении, свяжитесь со своим банком, написав заявление и предоставив документальное доказательство осуществления покупки и общения с продавцом.



Если произошел несанкционированный платеж, т. е., пользователь платежной карты не давал согласия на его выполнение, банк должен вернуть деньги в течение одного дня. В свою очередь, если при осуществлении покупок в интернете услуга или товар не доставлен или поврежден, клиенту сначала следует связаться с коммерсантом. Если с продавцом не удастся договориться о возврате денег, клиент должен обратиться в свой банк. Банк будет оценивать каждый случай индивидуально – если покупка совершена платежной картой, клиент вернет деньги, возврат может занять до 90 дней.



Если есть подозрения в мошенничестве, сообщите полиции. Обычно при оценке индивидуального случая банк рекомендует или даже просит обратиться в полицию.

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.

Советы для безопасных покупок в интернете



#1

Будьте осторожны при выборе интернет-магазина. Убедитесь, указаны ли: название, регистрационный номер, юридический адрес, контактный телефон, адрес электронной почты предприятия для быстрой связи. Посмотрите отзывы других покупателей и оцените, предоставлена ли ясная и понятная информация о товаре.

Остерегайтесь рекламы, которая обещает чудо-продукты или невероятно низкие цены на товары или услуги.



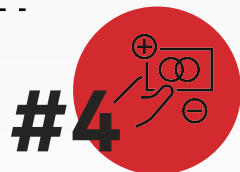
#2



#3

Совершайте покупки в интернет-магазинах, использующих надежную, или двухфакторную аутентификацию. Это свидетельствует о том, что коммерсант заботится о безопасности платежей.

Следите за движением денежных средств на своем счету – для дополнительного контроля включите уведомления в мобильном приложении. По необходимости меняйте лимит оплаты.



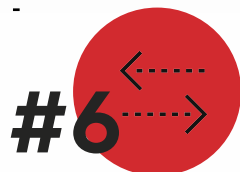
#4



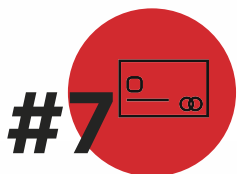
#5

Убедитесь, что соединение является безопасным (http и https). Не используйте устройство, обновления программного обеспечения на котором не выполнялись дольше 3 месяцев.

Выясните, каковы правила возврата товаров.



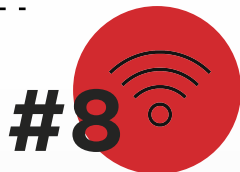
#6



#7

Всегда используйте безопасные средства оплаты, например, банковскую карту или подключение к интернет-банку (BankLink).

Платите только тогда, когда Вы подключены к безопасному интернет-соединению – избегайте использования открытой, публичной сети Wi-Fi.



#8

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНЫЕ УСТАНОВКИ, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ. ПЕРЕД ТЕМ, КАК ЗАКАЗЫВАТЬ ТОВАР В ИНТЕРНЕТЕ, ВЫ ДОЛЖНЫ САМОСТОЯТЕЛЬНО ОЦЕНИТЬ ИНТЕРНЕТ-МАГАЗИНЫ, КОТОРЫЕ ВЫ ВЫБИРАЕТЕ.