vied pircējs

ПУТЕВОДИТЕЛЬ ПО ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В ИНТЕРНЕТЕ

FINANŠU NOZARES ASOCIĀCIJA

mastercard

ВВЕДЕНИЕ

Покупатели в Латвии все чаще совершают покупки в интернете. Реагируя на изменение привычек покупателей, предприниматели начали все чаще предлагать товары и услуги в интернете – это обеспечивает удобство, безопасность и контроль бизнеса. Важно, чтобы предприниматели также заботились о цифровой безопасности, таким образом защищая своих клиентов и бизнес.

Кибербезопасность в интернете включает в себя технологии, процессы или действия, разработанные для защиты сетей, оборудования, программ и данных от атак, повреждений и несанкционированного доступа.

Количество, качество и объем кибератак по всему миру с каждым годом увеличивается. Данные показывают, что независимо от размера предприятия оно может быть подвержено риску кибератак. Однако именно малые и средние предприятия менее готовы предотвращать эти атаки. Большинство, а именно 60%, кибератак нацелены именно на малые и средние предприятия. В то же время потребители ожидают, что сохраненная на веб-сайте информация будет в безопасности. Важно оправдать это доверие – 31% респондентов указывают, что никогда не будут пользоваться услугами предприятия снова, если из него произошла утечка информации или оно было взломано, свидетельствуют собранные Cyber Readiness Institute данные.

Эта электронная книга предоставляет информацию и практические советы, которые следует знать каждому предпринимателю, планирующему или уже имеющему интернет-магазин, а также тем, кто хочет больше узнать о цифровой безопасности. В том числе информацию о видах атак, методах оплаты, решениях, которые помогут современному предприятию опознать риски и защититься, а также обобщает полезные инструменты и ссылки. Сейчас самое время ознакомиться с содержанием данного путеводителя!

ОГЛАВЛЕНИЕ

Какие виды атак существует в интернете? 1

Как защитить свой интернет-магазин? 4

Безопасные методы оплаты в интернете 7

Что делать, если происходит кибератака? 9

Что важно помнить? 10

Дополнительные ресурсы 11

vied pircējs FINANŠU NOZARES ASOCIĀCIJA mastercard

КАКИЕ ВИДЫ АТАК СУЩЕСТВУЕТ В ИНТЕРНЕТЕ?

Вредоносное программное обеспечение

- Разного рода вредоносные программы, 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.
- Вредоносное программное обеспечение чаще всего распространяется через вложения электронной почты, нелегальные или зараженные веб-сайты, а также при использовании рекламы или ссылок.

Взлом или подбор паролей из взломанных баз данных

- Один из самых простых способов – это взлом или подбор паролей из уже утекших баз данных паролей. Доказано – штобы разгадать 6-значный пароль, состоящий только из цифр, мощному компьютеру требуется всего пара секунд.
- Другой вид атаки для доступа и использования паролей – это получение информации о пользователях, включая пароли, из базы данных веб-сайта, доступ с этими же данными к учетным записям пользователей на других веб-сайтах, так как нередко пользователь использует один и тот же пароль на нескольких порталах. Поэтому особенно важно заботиться о безопасности данных, доверенных клиентом.
- 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.

Фишинг

- Способ, которым злоумышленники пытаются получить от пользователя интернета личную, секретную информацию, включая данные карт или интернет-банка, имена пользователей и пароли доступа и т. д. Злоумышленник может также притвориться сотрудником банка, Службы государственных доходов или полиции. Помните, что банк никогда не попросит Вас отправить свои идентификационные данные по электронной почте, sms или по телефону. Никто не обязан раскрывать такие данные.
- Такая атака может осуществляться с помощью телефонного звонка, sms, электронной почты, разных чатов, предлагая открыть ссылку на веб-сайт, который выдает себя за знакомый веб-сайт и выглядит как он, или файл в приложении в котором просят ввести, например, банковские данные предприятия.

Атака нулевого дня

- Все системы подвержены атакам. Атакой нулевого дня называется атака, например, на веб-сайт, когда она произошла впервые. Такую атаку невозможно предсказать, так как с развитием систем развиваются и техники злоумышленников.
- Злоумышленники находят в системе или программе уязвимость, о которой ее разработчик ранее не знал или которую не успел устранить, и получает доступ к информации на устройствах.
- Обычно возможность осуществить атаку такого рода приберегается для особых целей, где потенциальный выигрыш особенно ценен.
- Сайты электронной коммерции обычно страдают от атак, использующих уязвимости, исправления для которых доступны уже месяцами или даже годами, и их можно было избежать.

Атака DDoS

- Также называется Distributed Denial of Service, или распределенной атакой типа «отказ в обслуживании».
- В случае такой атаки несколько компьютеров используются для перегрузки веб-сайта путем отправки большого количества запросов. Это перегружает системы или оборудование, мешая их работе.

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.

- Можно реализовать более простые атаки DoS, или атаки типа «отказ в обслуживании», которые нацелены на определенные места компьютерной системы, которые являются особенно чувствительными и перегрузка которых вызывает общее нарушение работы системы.

Социальная инженерия

- Информация об индивидууме и предприятии часто широко доступна в интернете, поэтому злоумышленник может попытаться выдать себя за того, кем на самом деле не является.
- Разного рода атаки, осуществляемые с помощью взаимной коммуникации людей, психологически обманывающие собеседника, чтобы он раскрыл уязвимую информацию или совершил некое действие. Например, выдавая себя за другого человека или используя общие контакты, чтобы заслужить доверие.

Помните!

Данные опроса свидетельствуют, что **40% тех, кто столкнулся с мошенничеством, не смогли его распознать и попались.** Ваше понимание, знание о рисках, ответственное отношение коллег, очень важно для обеспечения кибербезопасности Вашего предприятия.

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 ЗАЩИТИТЬ СВОЙ ИНТЕРНЕТ-МАГАЗИН?

Выбирайте готовые и надежные решения для содержания и создания интернет-магазина

- Таким образом можно будет избежать недостатков веб-сайта и быть уверенным, что осуществляются необходимые изменения, соответствующие стандартам безопасности.
- Выбор такого решения займет меньше времени на его внедрение. Есть несколько веб-сайтов, обеспечивающих такие услуги, среди них, например, Mozello, Shopify, Wix и др.

Используйте надежные и уникальные пароли и двухфакторную аутентификацию

- Это поможет избежать доступа посторонних лиц к системам предприятия. Статистика показывает, что до 63% всех кибератак произошло из-за слабых или украденных паролей.
- 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.
- Альтернативой является использование менеджеров паролей, автоматически генерирующих пароли и хранящих их в зашифрованном виде.
- Для дополнительной безопасности также рекомендуется использовать двухфакторную, или строгую аутентификацию, которая требует подтверждать доступ еще каким-либо образом, например, отправкой sms с уникальным кодом подключения или возможностью дополнительной авторизации в приложении.

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.

Регулярно обновляйте программное обеспечение

Большая часть этих обновлений разрабатывается с целью устранения уязвимостей в системе и повышения ее безопасности.

Сотрудничайте с профессиональными поставщиками услуг, которые готовы принять ответственность за свою работу.

- Хранение информации на профессионально содержащихся **виртуальных серверах** (в облаке) является одним из способов защиты информации от недоброжелателей.
- Рекомендуется хранить данные в зашифрованном виде, что означает, что алгоритм преобразует их в формат, непонятный пользователю без ключа доступа. Нужно помнить, что ключи доступа должны храниться в безопасности. Если кто-то получает к нему доступ, это может привести к несанкционированному доступу к данным, в свою очередь, если он утерян, все данные будут безвозвратно утрачены.
- Серверы должны находиться удаленно – в охраняемых помещениях, где к ним не могут получить доступ посторонние лица. Также рекомендуется создавать резервные копии данных, что в случае атаки, когда доступ к информации запрещен, может предотвратить то, что ценная информация будет утрачена. В то же время нужно помнить и следить за стандартами Payment Card Industry (PCI), которыми устанавливается, как коммерсантам, принимающим оплату картой, нужно защищать информацию.
- Payment Card Industry Security Standards Council также предлагает анкету самооценки, которая поможет понять текущую ситуацию и, если необходимо, осуществить соответствующие улучшения. Больше информации можно найти в разделе Дополнительные ресурсы.

Создавайте резервные копии данных

В случае атаки, когда доступ к информации запрещен, копия может предотвратить то, что ценная информация будет утрачена. Таким образом можно обеспечить непрерывную работу предприятия.

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.

Следите за защитой веб-сайта

Чтобы убедиться, что веб-сайт и предприятие защищены от рисков атаки, доступны различные **тесты безопасности и автоматические сканеры**, проверяющие систему и сообщающие о возможных уязвимостях. В конце этой электронной книги доступен список ресурсов, в который также включены примеры тестов безопасности и другие решения для поддержания безопасности.

Помните!

Важно заботиться о цифровой безопасности ежедневно – регулярно менять пароли, обновлять программное обеспечение и сохранять резервные копии данных. Убедитесь, что на предприятии об этом проинформированы все!

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

Проведенный в мае 2020 года опрос о покупательских привычках жителей Латвии свидетельствует – если при приобретении товаров или услуг в интернете дается возможность выбора, предпочтение будет отдано оплате платежной картой и подключению к интернет-банку. Кроме того, почти для 70% жителей Латвии важно, чтобы товары и услуги предприятий можно было приобрести в интернете.

Помните!

Безопасный метод оплаты поможет оптимизировать время покупки и даст гарантию оплаты покупки.

Оплата картой

- Оплата картой является одним из полюбившихся клиентам методов оплаты в интернете, безопасным и проверенным способом. Mastercard – самые популярные в Латвии платежные карты. Более 80% всех выпущенных карт – именно Mastercard.
- Прием оплаты картой в интернет-магазине повышает общее доверие к веб-сайту, так как пользователь карты получает дополнительную защиту, поддерживающую надежную, или двухфакторную аутентификацию, например отправку sms с уникальным кодом подключения или использование аутентификации в интернет-банке.

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.

- В электронной коммерции двухфакторная аутентификация для платежей, например, пароль и E-Mobile или SmartID, является знаком гарантии, что магазин надежен.
- Коммерсант, присоединившись к системе двухфакторной аутентификации платежей, может разместить в своем интернет-магазине логотип программы, подтверждая, что платформа электронной коммерции проверена и готова к безопасным платежам. Таким гарантийным знаком, например, является логотип Mastercard Identity Check.

Соединение с интернет-банком (BankLink)

- Безопасное подключение к интернет-банку является одним из наиболее полюбившихся клиентам 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, не осуществляя лишних дополнительных действий.
- Одним из основных выигрышей коммерсанта является то, что деньги сразу поступают на счет.

Консультации с банком

Чтобы выяснить, соответствует ли уже выбранная предприятием платежная система принятым стандартам, рекомендуется связаться с представителями банка. Банк предоставит консультации о лучшем способе, как защитить себя и своих клиентов, порекомендовав безопасные и проверенные методы оплаты.

Помните!

В электронной коммерции **двухфакторная аутентификация платежей**, например, пароль и E-Mobile или SmartID, является знаком гарантии, что магазин надежен.

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.

ЧТО ДЕЛАТЬ, ЕСЛИ ПРОИСХОДИТ КИБЕРАТАКА?

Если на предприятии обнаружена атака в цифровой среде, прежде всего **нужно закрыть веб-сайт,** чтобы не допустить дальнейшей утечки данных и заражения пользователей. В то же время необходимо незамедлительно **проинформировать пользователей** о произошедшем, чтобы у них была возможность защитить себя в дальнейшем.

Когда веб-сайт будет закрыт и пользователи будут проинформированы, **нужно привлечь специалиста по безопасности**, который поможет провести анализ ситуации, определит размер атаки и даст рекомендации о том, как избежать атак в будущем.

Возобновлять работу веб-сайта можно только после того, как будут выяснены обстоятельства ситуации и приняты необходимые меры безопасности.

Четыре шага, если произошла атака

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.

ЧТО ВАЖНО ПОМНИТЬ

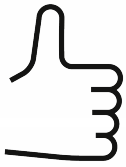
Интернет-магазин находится на предусмотренной в его целях платформе или был создан профессионалом.

Используются уникальные пароли доступа длиной не менее 14-16 символов, известные только пользователю.

Программное обеспечение обновляется регулярно, не реже одного раза в 3 месяца.

Для всех данных доступны резервные копии, хранящиеся отдельно.

К интернет-магазину подключен надежный метод оплаты.



Не наблюдается подозрительных действий или частых жалоб от клиентов.

Проведены тесты безопасности.

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.

ДОПОЛНИТЕЛЬНЫЕ РЕСУРСЫ

РАЗНЫЕ

Вопросы и ответы о внедрении требований платежей в интернете

- https://www.fktk.lv/mediju-telpa/nozares-temati/stingra-autentifikacija-maksajumiem-interneta/jautajumi-un-atbildes-par-jauno-interneta-maksajumu-drosibas-prasibu-ieviesanu/

Установлен дополнительный период, предусмотренный для внедрения строгой аутентификации для сделок платежными картами в электронной коммерции

- https://www.fktk.lv/jaunumi/pazinojumi-medijiem/noteikts-papildu-periods-kas-paredzets-stingras-autentifikacijas-ieviesanai-maksajumu-karsu-darijumiem-e-komercija/

Request for input on the preparedness to meet the requirements on strong customer authentication (информация на английском языке)

- https://www.financelatvia.eu/wp-content/uploads/2020/01/EBA_Questionnaire_PSPs_acquiring.pdf
- https://www.financelatvia.eu/wp-content/uploads/2020/01/EBA_Questionnaire_PSPs_acquiring.pdf

Анкета самооценки Payment Card Industry (информация на английском языке)

- https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

Как уменьшить киберриски? (информация на английском языке)

- https://gcatoolkit.org/smallbusiness/

РЕСУРСЫ БАНКОВ

Вебинар банка Citadele «Как учредить э-Предприятие: от А До Я»

- https://www.facebook.com/watch/?v=2615556711998222

Luminor: От бизнеса к э-бизнесу!

- https://www.luminor.lv/lv/e-komercijas-atbalsts

Э-академия банка SEB

- https://eakademija.seb.lv/#985

Swedbank: Узнайте, как удобно открыть интернет-магазин

- https://www.swedbank.lv/business/campaign/ecommerce?language=LAT&WT.mc_id=202006_ EcommerceCombiningForces_GDN_search_lv_lat