vied pircējs

Путеводитель по предпринимательской деятельности в Интернете

FINANŠU NOZARES ASOCIĀCIJA

mastercard

vied pircējs

Введение

Латвийские покупатели все чаще делают покупки в Интернете. Реагируя на смену покупательских привычек, предприниматели начали предлагать товары и услуги онлайн, что обеспечивает им удобство, безопасность и контроль над бизнесом. Важно отметить, что предприниматели заботятся и о цифровой безопасности, тем самым защищая своих клиентов и бизнес.

Кибербезопасность в онлайн-среде включает в себя технологии, процессы или действия, разработанные для защиты сетей, оборудования, программ и данных от нападений, повреждений или несанкционированного доступа.

С каждым годом во всем мире растет как количество совершенных кибератак, так и количество пострадавших от них. Данные показывают, что любое предприятие, независимо от своего размера, может быть подвержено риску кибератаки. Однако осведомленность и готовность к нарушениям кибербезопасности особенно важны для малых и средних предприятий, поскольку им зачастую не хватает ресурсов для инвестиций в инструменты безопасности и обучение. Такие предприятия менее подготовлены к предотвращению кибератак: лишь 38 % малых и средних предприятий по всему миру утвердительно ответили на вопрос о готовности к кибер-инцидентам, свидетельствуют данные, собранные Cyber Readiness Institute в 2021 году.

В данном электронном путеводителе собрана информация и практические советы для предпринимателей, которые планируют открыть или уже открыли онлайн-магазин, а также для желающих подробнее узнать о цифровой безопасности, в том числе информацию о видах атак, способах оплаты, решениях, помогающих современному предприятию защититься и распознать риски, а также подборку полезных инструментов и ссылок. Сейчас самое время прочитать это руководство!

vied pircējs

Предметный указатель

1 Какие существуют виды атак в Интернете?

4 Как защитить свой интернет-магазин?

7 Безопасные методы расчетов в Интернете

9 Что делать, если произошла кибератака?

10 О чем важно помнить?

11 Дополнительные ресурсы

FINANŠU NOZARES ASOCIĀCIJA

mastercard

vied pircējs

Какие существуют виды атак в Интернете?

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

- Различные вредительские программы, которые устанавливаются на устройства без ведома пользователя.
- При нападении такого рода начинают выполняться запрещенные действия в компьютере или смартфоне в целях получения ценной информации, лишения доступа к хранящимся данным или полной остановки работы устройства.
- Чаще всего вредоносное программное обеспечение распространяется в виде приложений к электронным письмам, посредством нелегальных или зараженных интернет-страниц, а также рекламы или ссылок.

ФИШИНГ

- Это способ злоумышленников завладеть как личной информацией, в том числе данными платежных карт или интернет-банка, именами пользователей и паролями, так и имеющимися в распоряжении предприятий данными клиентов.
- Зачастую злоумышленники выдают себя за работников банка или служб доставки.
- Такое нападение может осуществляться посредством SMS-сообщения, электронной почты, различных чатов, побуждающих открыть прилагаемый файл или ссылку на фальшивую интернет-страницу, которая выдает себя за известную и предлагает ввести, например, банковские данные предприятия.

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНОЕ РУКОВОДСТВО, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ.

FINANŠU NOZARES ASOCIĀCIJA
mastercard

vied pircējs

ВЗЛОМ ИЛИ ПОДБОР ПАРОЛЯ ИЗ ВЗЛОМАННЫХ БАЗ ДАННЫХ

- Один из простейших способов – взлом или подбор пароля из попавших в общий доступ хранилищ паролей. Доказано: чтобы разгадать 6-значный пароль, состоящий только из цифр, мощному компьютеру потребуется лишь пара секунд.

- Другой вид атаки для получения и использования паролей – извлечение информации о пользователях, включая их пароли, из базы данных в Интернете, и использование этих данных для доступа к учетным записям пользователей на других страницах, поскольку нередко пользователь использует один и тот же пароль на нескольких порталах. Поэтому особенно важно заботиться о безопасности доверенных клиентом данных.

- В наши дни один лишь пароль не может считаться надежным способом аутентификации. Для более высокого уровня безопасности необходима многофакторная аутентификация. Для защиты менее чувствительной информации стоит рассмотреть возможность предлагать клиентам аутентифицироваться посредством профиля в социальных сетях.

DDOS-АТАКА

- Также называется Distributed Denial of Service, или распространенный отказ услуги из-за перегрузки атаками.

- В случае такой атаки используется несколько компьютеров, чтобы перегрузить интернет-страницу одновременной отправкой большого количества запросов. В результате наступает перегруженность системы или установки, нарушающая ее работу.

- Существует возможность реализовать более простые DoS, или атаки с отказом сервисов, нацеленные на определенные места компьютерной системы, которые особенно чувствительны и перегрузка которых вызывает общее нарушение работы системы.

vied pircējs

АТАКА НУЛЕВОГО ДНЯ

- Все системы подвержены атакам, однако атакой нулевого дня называется атака, например, на домашнюю страницу, которая произошла впервые. Предвидеть такую атаку невозможно, поскольку наряду с развитием систем безопасности развиваются и техники злоумышленников.

- Злоумышленники находят уязвимость в системе или программе, о которой ее разработчик не знал или не успел устранить, и завладевают информацией, хранящейся на устройствах.

- Обычно возможность совершения такого нападения сохраняется для достижения особых целей, когда вероятная выгода особенно велика.

- Как правило, интернет-страницы э-коммерции страдают от атак с использованием уязвимостей, для которых уже несколько месяцев или даже лет существуют исправления, позволяющие избежать нападений.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Информация о физическом лице и предприятии обычно доступна в Интернете, поэтому злоумышленник может пытаться выдать себя за того, кем на самом деле не является.

- Различные атаки осуществляются с помощью личной коммуникации, когда на человека воздействуют психологически, для того, чтобы он разгласил конфиденциальную информацию.

Помните!

Понимание и знания о рисках, имеющиеся у Вас и ваших коллег, важны для обеспечения кибербезопасности вашего предприятия.

vied pircējs

Как защитить свой интернет-магазин?

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

- Таким образом вы сможете избежать недочетов и быть уверены во внесении необходимых изменений, соответствующих стандартам безопасности.
- Выбор такого решения потребует меньше времени на его внедрение. Существует несколько страниц, предоставляющих подобные услуги, например: *Mozello, Shopify, Wix* и другие.

Используйте надежные и уникальные пароли, а также двухфакторную аутентификацию

- Это поможет избежать проникновения посторонних в системы предприятия. Статистика[1] показывает, что вплоть до 63 % всех кибератак происходит из-за слабых или украденных паролей.
- Надежный пароль длинный – не менее 14–16 символов, включая буквы, цифры, другие знаки. Чтобы их было легче запомнить, можно использовать так называемые парольные фразы, включающие, например, слова известной вам песни или стихотворения, цифры и символы.
- В качестве альтернативы можно использовать менеджеры паролей, которые автоматически генерируют пароли и хранят их в зашифрованном виде.
- Для дополнительной безопасности также рекомендуется использовать двухфакторную, или строгую, аутентификацию, которая требует подтверждать доступ еще каким-либо способом, например путем отправки SMS-сообщения с уникальным кодом подключения.

[1] Данные *Cyber Readiness Institute*

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНОЕ РУКОВОДСТВО, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ.

FINANŠU NOZARES ASOCIĀCIJA
mastercard

vied pircējs

Регулярно обновляйте программное обеспечение

- Большая часть таких обновлений разрабатывается с целью устранить уязвимости в системе и повысить ее безопасность.

Сотрудничайте с профессиональными поставщиками услуг, готовыми нести ответственность за свою работу

- Хранение информации на поддерживаемых профессионалами **виртуальных серверах** (в облаке) – один из способов защитить данные от недоброжелателей.

- Рекомендуется хранить данные в зашифрованном виде, т. е. преобразованном алгоритмом в формат, который непонятен пользователю без ключа доступа. Необходимо помнить и о безопасном хранении ключа доступа. Завладевший им получит доступ к данным, а в случае утери ключа все данные будут необратимо утрачены.

- Серверы должны находиться в охраняемых помещениях, исключающих доступ к ним посторонних лиц. В то же время необходимо помнить и соблюдать стандарты *Payment Card Industry* (PCI), в которых предусматривается, что информацию должны охранять торговцы, принимающие платежи картами.

- В *Payment Card Industry Security Standards Council* также предлагается анкета самооценки, которая поможет разобраться в сложившейся ситуации и при необходимости внести соответствующие улучшения. Подробную информацию можно найти в разделе «Дополнительные ресурсы».

Создавайте резервные копии данных

- В случае атаки, если доступ к информации будет закрыт, копия поможет предотвратить потерю ценной информации. В результате будет обеспечена непрерывность деятельности предприятия.

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНОЕ РУКОВОДСТВО, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ.

vied pircējs

Следите за защитой интернет-страницы

- Чтобы убедиться в том, что страница и предприятие защищены от рисков атаки, существуют различные **тесты безопасности и автоматические сканеры**, которые выполняют проверку системы и сообщают о возможных недочетах. В конце данной электронной книги приводится перечень ресурсов, содержащий также примеры тестов безопасности и других решений для поддержания безопасности.

Помните!

Важно заботиться о цифровой безопасности ежедневно – регулярно менять пароли, обновлять программное обеспечение и сохранять резервные копии данных. Проследите за тем, чтобы об этом знали все работники предприятия!

vied pircējs

Безопасные методы расчетов в Интернете

Проведенный в январе 2022 года опрос о покупательских привычках жителей Латвии свидетельствует, что, если при покупке товаров или услуг в Интернете предоставляется возможность выбора, предпочтение отдается платежам с подключением к интернет-банку и платежной картой. При этом для 78 % жителей Латвии важна возможность приобрести товары и услуги предприятий в Интернете.

Помните!

Безопасный метод расчетов поможет оптимизировать время покупки и обеспечит гарантию ее оплаты.

ПОДКЛЮЧЕНИЕ К ИНТЕРНЕТ-БАНКУ (*BANKLINK*)

- Согласно опросу жителей Латвии, надежное подключение к интернет-банку – один из самых популярных среди клиентов способов оплаты в Интернете. После выбора товара или услуги клиента перенаправляют на заполненное платежное поручение в его интернет-банке или мобильном приложении.
- Banklink обеспечивает торговцу возможность подготовить платежное поручение именно в интернет-банке покупателя, а клиенту – немедленно подтвердить его без выполнения каких-либо дополнительных действий.
- Одна из основных выгод для торговца заключается в том, что деньги поступают на счет сразу.

.

FINANŠU NOZARES ASOCIĀCIJA
mastercard

vied pircējs

ПЛАТЕЖИ КАРТАМИ

- Платежи картами – один из популярных среди клиентов методов оплаты в Интернете, надежный и проверенный способ. Mastercard – самые популярные платежные карты в Латвии. Более 76 % выданных карт составляют именно Mastercard.

- Прием платежей картами в интернет-магазине повышает общее доверие к интернет-странице, поскольку пользователь карты получает дополнительную защиту, поддерживая безопасную, или двухфакторную, аутентификацию, например путем отправки SMS-сообщения с уникальным кодом подключения или использования приложения для авторизации.

- Присоединившись к системе двухфакторной аутентификации платежей, торговец может разместить в своем интернет-магазине логотип программы в качестве подтверждения того, что платформа э-коммерции проверена и готова к осуществлению безопасных платежей. К примеру, таким знаком гарантии является логотип Mastercard Identity Check.

КОНСУЛЬТАЦИИ С БАНКОМ

- Чтобы выяснить, соответствует ли выбранная предприятием платежная система принятым стандартам, рекомендуется обратиться к представителям банка. Они предоставят консультацию о наилучшем способе защитить себя и своих клиентов и порекомендуют надежные и проверенные способы платежей.

Помните!

Использование в э-коммерции **двухфакторной аутентификации для подтверждения платежа** обеспечивает покупателю уверенность в том, что его платежные данные будут в безопасности.

vied pircējs

Что делать, если произошла кибератака?

Если на предприятии произошло нападение в цифровой среде, прежде всего нужно **закрыть интернет-страницу**, чтобы не допустить дальнейшую утечку данных и заражение пользователей. В то же время необходимо немедленно **сообщить пользователям** о случившемся, чтобы те могли в дальнейшем защитить себя и срочно сменить пароли от своих учетных записей.
Когда интернет-страница закрыта, а пользователи проинформированы, нужно привлечь **специалиста по безопасности**, который поможет проанализировать ситуацию, определит масштаб атаки и даст рекомендации о том, как избежать атак в будущем.

Возобновить работу интернет-страницы разрешается только после того, как обстоятельства ситуации выяснены и приняты необходимые меры безопасности.

Четыре шага, которые нужно предпринять в случае атаки

1

ЗАКРОЙТЕ ИНТЕРНЕТ-СТРАНИЦУ!

2

СООБЩИТЕ ПОЛЬЗОВАТЕЛЯМ И БАНКУ!

3

ПРИВЛЕКИТЕ СПЕЦИАЛИСТА ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ!

4

ВОЗОБНОВИТЕ РАБОТУ ИНТЕРНЕТ-СТРАНИЦЫ!

FINANŠU NOZARES ASOCIĀCIJA
mastercard

vied pircējs

О чем важно помнить?

- [x] **Интернет-магазин размещен на созданной для этой цели платформе или создан профессионалом**
- [x] **Используются уникальные пароли доступа, состоящие минимум из 14–16 символов и известные только пользователю**
- [x] **Программное обеспечение регулярно обновляется – минимум раз в 3 месяца**
- [x] **Имеются резервные копии всех данных, которые хранятся отдельно**
- [x] **К интернет-магазину подключен надежный способ оплаты**
- [x] **Интернет-магазин прошел тесты безопасности**
- [x] **В интернет-магазине не наблюдается подозрительных действий или частых жалоб клиентов**

ПОЖАЛУЙСТА, ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ИНФОРМАТИВНОЕ РУКОВОДСТВО, А НЕ ПРОФЕССИОНАЛЬНЫЕ РЕКОМЕНДАЦИИ.

FINANŠU NOZARES ASOCIĀCIJA
mastercard

vied pircējs

Дополнительные ресурсы

РАЗНОЕ

Установлен дополнительный срок для внедрения системы строгой аутентификации сделок с платежными картами в э-коммерции *(информация на латышском языке)*

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

Анкета самооценки Payment Card Industry
(информация на английском языке)

Как уменьшить киберриски? *(информация на английском языке)*

РЕСУРСЫ БАНКОВ

Как удобно открыть интернет-магазин?

Как защитить свое предприятие от попыток мошенничества?

Вебинар «Как учредить э-предприятие: от А до Я»
(информация на латышском языке)

От бизнеса – к э-бизнесу! *(информация на латышском языке)*

Э-академия *(информация на латышском языке)*