CYBER READINESS
INSTITUTE

Ой-ой, только не это!

Советы по киберготовности для розничных торговцев в период праздников

Сезон праздничных покупок в самом разгаре, но, как и многие привычные нам действия, **в этом году шоппинг будет отличаться из-за пандемии COVID-19.**

Все больше людей совершает покупки в Интернете, чем когда-либо прежде. По данным McKinsey, от 30 до 60% потребителей во всем мире планируют совершать покупки в Интернете во время праздников. Розничным торговцам пришлось предпринять шаги, чтобы облегчить процесс покупки товаров Интернете и предложить покупателям новые доставки товаров. В новых условиях многие розничные торговцы должны были заключить договоры на услуги по доставке. Это означает, что им нужно делиться информацией о клиентах с третьими сторонами. Весь процесс покупки от начала до конца все больше зависит от передачи информации между продавцами и их клиентами, которые пользуются компьютерами и смартфонами. Современные передовые технологии позволили розничным торговцам, даже небольшим, быстро перевести большую часть своего бизнеса на цифровую платформу. Это отличная новость для решения бизнес-задач, которых стало больше из-за пандемии. Плохая новость заключается в том, что преступники также совершили переход в цифровой мир.

Киберпреступники знают, что все больше людей совершают покупки в Интернете и что розничные продавцы собирают и делятся более ценной информацией о своих покупателях, включая номера кредитных карт, адреса и удостоверения личности с фотографией для самовывоза. Произошло огромное увеличение числа фишинговых атак по электронной почте и текстовых сообщений — попыток обманом заставить вас нажать на ссылку или отправить информацию — и атак программ-вымогателей, когда преступники держат вашу компьютерную систему и данные «в заложниках» до тех пор, пока не получат оплату. ФБР сообщило о 400-процентном увеличении количества жалоб на кибератаки по сравнению с периодом до COVID-19. В то время как Интерпол отслеживает «тревожный уровень кибератак», направленных на предприятия всех масштабов, правительства и критически важную инфраструктуру в период пандемии. Мы знаем, что это напряженное время года, и что вы сосредоточены на обслуживании своих клиентов. Мы понимаем, что вы можете нанимать сезонных работников или начать сотрудничать с новыми службами доставки и партнерами.

Но преступники тоже это знают и рассчитывают на то, что вы можете отвлечься и пренебречь необходимостью в киберподготовке.. К сожалению, по данным Национального альянса кибербезопасности, 60% малых предприятий прекращают свою деятельность в течение 6 месяцев после серьезного киберинцидента.

guide@cyberreadinessinstitute.com

Возможно, вы думаете, что ваш бизнес слишком мал, чтобы служить мишенью, однако вы можете быть легкими пропуском к более крупной желаемой цели. Вот несколько советов, которые помогут вам быть киберготовыми в сезон праздничных покупок:

Нужно

- Немедленно обновите свои пароли использовать в них до 15 символов — Используйте парольные фразы, их легче запомнить. (например, слова из песни, строки из книги)
- Включите автообновление для всех программ
- Используйте многофакторную аутентификацию в любое время, когда она доступна
- Убедитесь, что резервное копирование ваших компьютеров и данных выполняется в отдельной сети, и регулярно проверяйте резервное копирование.
- Имейте четкие киберправила, которые представлены всем сотрудникам
- Обучите сотрудников тому, как безопасно и надежно получать и обрабатывать онлайн-заказы

Нельзя

- Не нажимайте на ссылки и никогда не предоставляйте финансовую информацию по электронной почте
- Не сообщайте свои пароли или учетные данные для входа
- Не оставляйте компьютер без присмотра и/или разблокированным
- Не думайте, что ваши партнеры киберготовы (например, службы доставки, платежные системы, мелкие поставщики)

Помните, что поведение людей имеет решающее значение в предотвращении кибератак.

Убедитесь, что все ваши сотрудники и сезонные работники обучены вашим политикам кибербезопасности, что они знают важность кибербезопасности и свою роль в ней. Помогите им выработать хорошие привычки киберготовности. Чтобы получить более подробную информацию, пожалуйста, зарегистрируйтесь в Программе киберготовности и ознакомьтесь с другими нашими руководствами по выработке хороших привычек киберготовности.

Об Институте кибербезопасности

Институт кибербезопасности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов для обмена ресурсами и знаниями, которые используются с целью разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Изучите основы хорошей кибербезопасности с помощью нашего Стартового набора или создайте культуру киберготовности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше, посетите сайт www.BeCyberReady.com.

guide@cyberreadinessinstitute.com