Покупки в праздники: советы для розничных торговцев

Сезон праздничных покупок в самом разгаре, и магазины по всему миру готовятся к всплеску заказов. Важно подготовиться и расставить приоритеты в отношении рисков кибербезопасности. Ниже приведены советы по кибербезопасности, которым розничные торговцы должны следовать, чтобы продолжать оставаться в безопасности, продавая через Интернет.

Совет 1 Не забывайте обновлять ПО

- Включите автообновление для всего программного обеспечения.
- Каждое обновление содержит последние исправления и так называемые патчи, которые могут защитить вас от потенциально опасных угроз.
- **Перезагрузка компьютера** также является еще одним способом установки исправлений.

Совет 2 Определите свою политику кибербезопасности

- **Обучите всех своих сотрудников** политике кибербезопасности.
- Покажите сотрудникам важность кибербезопасности и роль, которую она играет в их личной и профессиональной жизни.
- **Зарегистрируйтесь в нашей бесплатной Программе киберготовности** и получите доступ к другим ресурсам CRI, чтобы выработать хорошие привычки киберготовности.

Совет 3 Откажитесь от USB-накопителей

- USB-накопители удобны для передачи файлов между компьютерами, но их также можно использовать для распространения **вирусов и вредоносных программ.**
- Настройте **сетевой компьютер, не принадлежащий компании,** который можно использовать для сканирования USB-накопителей на наличие вредоносных программ и удаление информации с дисков.
- Используйте **онлайн-систему или облачную систему обмена файлами с защищенным доступом,** чтобы вам не нужны были USB-накопители.

Совет 4 Берегитесь фишинга в праздники

- **Сохраняйте бдительность в отношении фишинга и вредоносных сообщений,** хакеры пытаются воспользоваться тем, что вы заняты и рассеянны.
- Проверьте адрес электронной почты отправителя и **внимательно просмотрите электронные письма,** чтобы убедиться, что отправитель является подлинным. Если это звучит слишком хорошо, чтобы быть правдой, возможно, так оно и есть!
- **Никогда не переходите по ссылкам**, не загружайте вложения и не передавайте информацию от неизвестных отправителей! Даже если вы знаете человека, всегда полезно написать или позвонить ему, чтобы проверить, прежде чем предпринять какие-либо действия.

Совет 5 Храните пароли в безопасности

- Убедитесь, что парольные фразы ваших учетных записей **надежны и уникальны**.
- При наличии включите **многофакторную аутентификацию (MFA)** во всех ваших учетных записях.
- Никогда никому не сообщайте свои пароли и **всегда меняйте их** после поездок или действий, когда вы вошли в учетную запись на чужом устройстве.