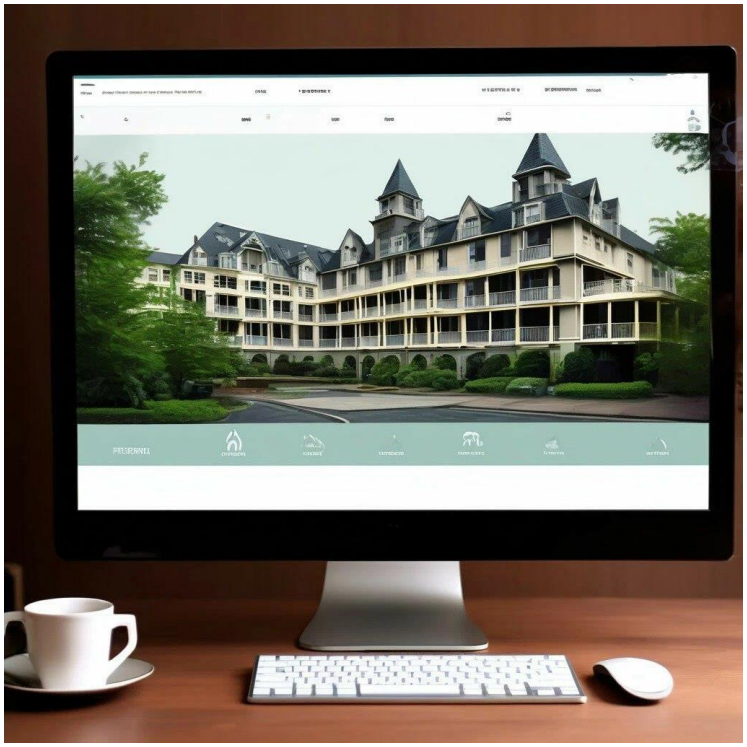
ПАМЯТКА «Меры безопасности при бронировании отелей»

Как не испортить себе отпуск?

В период отпусков и высокого спроса на жилье люди часто поддаются эмоциям и хотят быстрее забронировать отель, чтобы не упустить выгодное предложение. Этим пользуются мошенники, рассчитывая на чью-нибудь спешку и невнимательность. Основные схемы, используемые мошенниками:

Фейковый сайт отеля

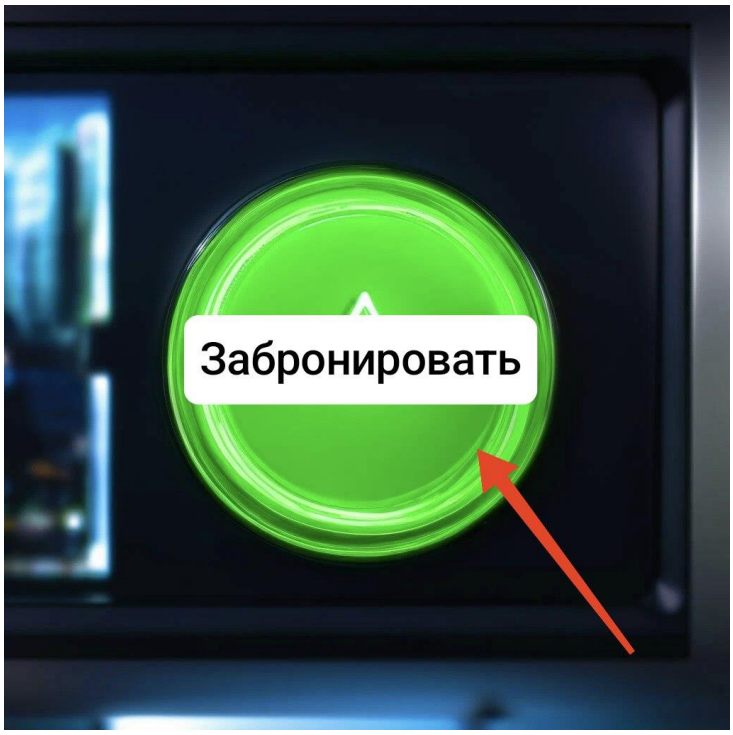


Злоумышленники копируют дизайн сайта какого-то отеля, описывают преимущества, добавляют отзывы, как будто от довольных гостей. Посетителю сайта предлагают оформить бронирование по выгодной цене. Такая «акция», как правило, имеет ограниченный срок и думать нужно быстро. Иногда мошенники, наоборот, ставят цены выше рыночной, чтобы получить больше денег с одной жертвы.

Человек переводит предоплату, а «отельеры» сразу пропадают или некоторое время еще поддерживают связь, чтобы усыпить бдительность. Когда наступает запланированный отпуск, выясняется, что в реальном отеле брони нет, либо по указанному адресу находится какой-нибудь бизнес-центр.

«Проверка» карты

Мошенники создают на известном агрегаторе фейковую страницу отеля. При этом адрес может быть и реальным. Посетителю предлагают бесплатно оформить бронь с опцией отмены.

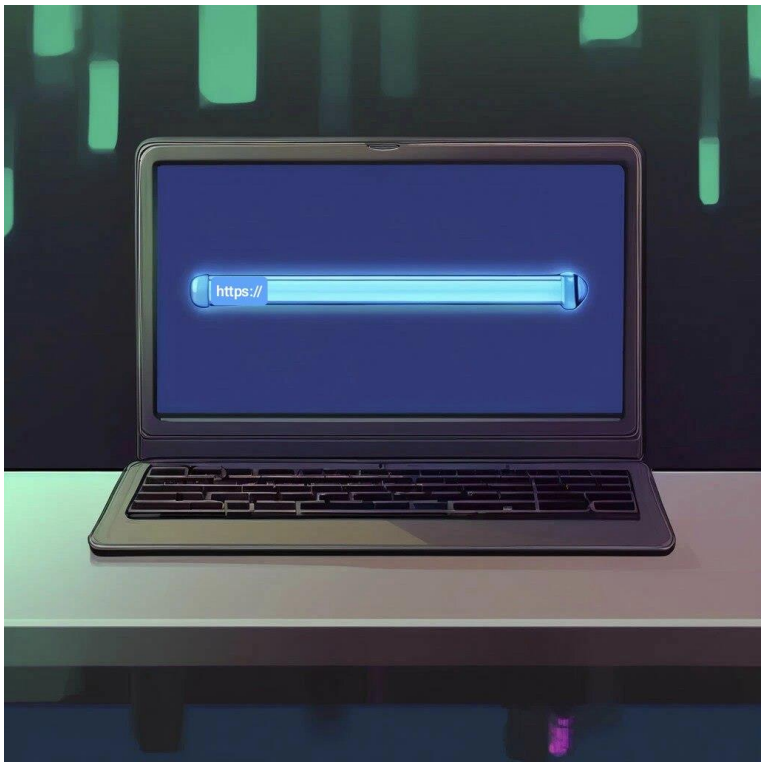


После оформления с ним связываются мошенники и говорят, что сервис не может проверить его банковскую карту. Чтобы завершить оформление брони, нужно пройти по ссылке в письме и ввести данные карты. Они спишут маленькую сумму и сразу ее вернут. Если человек поверит и введет свои данные, то после небольшого списания якобы для проверки, начнутся более крупные.

Агрегаторы действительно могут так проверять карты при бесплатном бронировании: списывают символическую сумму и тут же зачисляют обратно. Но если при проверке возникнут проблемы, то сервис просто отменит бронь, а не будет звонить клиенту или присылать письма со ссылками.

Чтобы снизить риски неприятностей:

- При бронировании отеля обязательно обращайте внимание на наличие защищенного соединения (SSL). В адресной строке браузера должен отображаться замок и адрес сайта должен начинаться с "https://". Например, "https://ostrovok.ru". Это гарантирует, что все данные, включая вашу личную информацию и данные кредитной карты, будут передаваться в зашифрованном виде и защищены от несанкционированного доступа.



- Пользуйтесь проверенными сервисами бронирования. Если вам приглянулся малоизвестный отель, проверьте, можно ли забронировать номер через эти сервисы. Если бронь возможна только на сайте отеля, это может указывать на мошенничество.

- Общайтесь с представителями компаний в чате официального сайта или приложения. Там служба безопасности отслеживает переписку и блокирует подозрительные ссылки. Насторожитесь, если вас уводят в сторонние мессенджеры.

- Перед тем, как оплачивать заказ, попробуйте узнать больше о компании или ИП. Можно проверить информацию о юридическом лице с помощью запроса электронной выписки из Единого государственного реестра юридических лиц

или поиска сведений на сайте Федеральной налоговой службы.

- Проверьте, есть ли у сервиса служба поддержки и насторожитесь, если нет, или линия все время занята. Служба поддержки может быть и поддельной, поэтому смотрите и на другие аспекты.

- Не переводите оплату по номеру карты или на электронные кошельки. Не переходите по ссылкам и не вводите данные банковской карты на незнакомых ресурсах
- Будьте внимательны, если отель предлагает цену существенно ниже или выше рыночной. Проверяйте информацию, если встретили ее в соцсетях или на форумах. Новые страницы в соцсетях можно создавать и удалять хоть каждый день, и мошенники этим пользуются.

ОБКУ УМВД России по Липецкой области.