Информационно-справочные материалы по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Официальная статистика МД России по обращениям о мошенничествах в разрезе праздничных периодов отдельно не ведется. Однако существует такое понятие, как «четкая закономерность» - когда спрос рождает предложение.

В преддверии праздников и распродаж люди массово ищут выгоду, активно покупают подарки, билеты на культурные мероприятия и следят за акциями.

Злоумышленники этим активно пользуются, так как психологическая готовность человека к выгодной покупке значительно снижает его бдительность.

Какие именно схемы обмана становятся самыми популярными у злоумышленников?

Фишинг – это одна из ключевых угроз, но не единственная. Что именно делают злоумышленники, подстраивая свои схемы под потребительские тренды:

- резко наращивают объемы фишинговых рассылок с фейковыми акциями и ссылками на сайты-клоны;

- создают поддельный страницы популярных маркетплейсов, в том числе осуществляющих реализацию билетов, предлагая «неслыханные» скидки;

- активнее используют схемы с предзаказом дефицитных товаров, играя на ажиотаже.

Таким образом, среди ***основных «трендов» мошенничества в сфере продажи билетов, которых стоит опасаться в предверии новогодних праздников и зимних каникул, можно выделить следующие способы:***

1. Создание злоумышленниками сайтов – двойников (копий официальных сайтов известных касс).

Для создания фейковых сайтов-клонов мошенниками используются шаблоны и автоматизированные скрипты, которые позволяют развернуть точную копию легального сайта буквально за несколько часов.

С этой целью регистрируются доменные имена, похожие на имя известного бренда, с различными опечатками. «Жизненный цикл» такого сайта короток – от нескольких часов до 2-3 суток.

Этого времени достаточно, чтобы собрать достаточное количество жертв, после чего мошенники его бросают и запускают новый.

2. Размещение в сети Интернет рекламы несуществующих билетов по «низкой» цене до начала официальной продажи, а также продажа несуществующих или уже использованных бумажных билетов.

3. Продажа копий/скриншотов электронных билетов. Один билет продается десяткам людей. Первый, кто придет на мероприятие, пройдет, остальные останутся у входа.

4. Использование легальных площадок перепродаж (к примеру Авито, Юла), когда злоумышленник после предоплаты блокирует покупателя.

5. Генерация поддельных QR-кодов, которые не будут считываться сканером или ведут на фишинговый сайт при «проверке».

6. Предложение «вернуть» деньги за отмененное мероприятие по фальшивой ссылке.

Что делают власти и организаторы?

1. МВД России и Роскомнадзор блокируют фишинговые сайты.

2. Организаторы и площадки внедряют именные билеты с паспортным контролем.

3. Банки улучшают системы Антифрод для отслеживания подозрительных операций.

4. Легальные площадки создают официальные площадки для безопасной перепродажи по фиксированной цене.

***Но осторожность и осведомленность покупателя остаются основными инструментами защиты.***

Самой современной и эффективной стратегией кибербезопасности **является принцип нулевого доверия.**

**Если говорить коротко, его суть можно выразить одной фразой «Никогда не доверяй, всегда проверяй».**

**Советы покупателям:**

1. Покупайте билеты только у официальных распространителей. Проверяйте список на сайте артиста, организатора или мероприятия. Основные легальные площадки: Кассир.ру, Яндекс.Афиша, Ticketland.ru и др.

2. Верифицируйте сайт. Проверяйте домен (адрес сайта), наличие SSL-сертификата (замочек в строке браузера), юридических данных компании.

3. Остерегайтесь предоплаты переводом на банковскую карту физическому лицу. Используйте безопасные способы оплаты, которые можно оспорить (к примеру, сервисы официальных касс).

4. Тщательно проверяйте продавцов на вторичном рынке, а именно:

- смотрите рейтинг, давность аккаунта, историю других продаж, требуйте оригинал чека из официальной кассы;

- для электронных билетов – договоритесь о встрече у кассы мероприятия для совместной активации или проверьте билет через официальное мобильное приложение кассы (оно сканирует QR и показывает валидность).

5. Не поддавайтесь на уловку мошенника и используемую им технологию психологического давления: «билеты заканчиваются».

6. Подозрительно относитесь к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься», «купи»), с темами про финансы, в том числе со ссылками, особенно если они длинные или наоборот, использовались сервисы сокращения ссылок.

7. Не переходите по ссылкам из письма, если они заменены на слова. Также на фишинговом сайте часто есть орфографические ошибки и некорректно работающие элементы.

**Но если все же попались на удочку мошенника, алгоритм действий должен быть таким:**

1. Немедленно позвоните в свой банк по номеру с обратной стороны карты и заблокируйте ее, либо сообщите что осуществлена операция без согласия клиента. Блокировку банковской карты можно также осуществить в мобильном приложении банка.

2. Обратитесь с заявлением в полицию.

3. Если вы ввели логины и пароли от каких-либо сервисов, немедленно смените их, а также включите двухфакторную аутентификацию.

Главное – не паниковать, а действовать быстро. Ваши первые действия определяют шансы вернуть денежные средства.

Следственный департамент МВД России