С активным внедрением в общественную жизнь современных технологий активно развиваются и новые виды преступной деятельности, направленные на обман и мошенничество граждан с применением информационно-коммуникационных технологий. Одной из форм мошенничества выступает создание и использование злоумышленниками сайтов-двойников. Фишинговый сайт – это платформа для интернет-мошенничества, на которой злоумышленник получает доступ к конфиденциальным данным граждан, таким как логины и пароли, номера и коды безопасности кредитных карт. Не владея достаточными знаниями, пользователь не всегда может отличить фишинговый сайт от настоящего в связи с тем, что поддельный ресурс визуально похож на оригинальный сайт. Под видом предоставления несуществующих услуг или имитируя веб-ресурс организации (учреждения) которому держатель доверяет, злоумышленники получают доступ к конфиденциальной информации и используют ее в мошеннических целях. Особенно опасны поддельные сайты социальных сетей, банковских и финансовых организаций, организаций, оказывающих государственные услуги, принимающих оплату штрафов, налогов, услуг ЖКХ. Следует внимательно проверять реквизиты оплаты штрафов, налогов, услуг ЖКХ, в том числе приходящих на личную электронную почту, якобы направленных из государственных органов или организаций. Обезопасить себя от преступлений в указанной сфере возможно путем внимательного изучения адреса сайта, на котором находится пользователь. При поиске в браузерах желательно самостоятельно набирать фразу «Официальный сайт» и название сайта, магазина, организации, которая требуется. Изначально появится оригинальный сайт, на который можно будет перейти, либо ознакомиться с правильностью написания адреса в браузере. При наличии сомнений, рекомендуется позвонить в организацию, сайт которой требуется пользователю, и уточнить правильное написание. Также рекомендуется тщательно изучать содержание сайта. Грамматические ошибки, низкое качество графики могут являться признаками «фишинга». Цены на предлагаемые товары или услуги значительно ниже среднерыночных, а также отсутствие фотографий предлагаемого товара являются признаками мошеннических сайтов. Мошенники, как правило, редко обновляют свои сайты и их разделы, поэтому гражданам надлежит внимательно изучить даты сообщений и новостей. Особое внимание стоит обратить на интерактивные гостевые книги и форумы посетителей сайта, отсутствие активности, либо удаление направленных сообщений – признак подделки веб-ресурса. Стоит отметить, что на мошеннических сайтах практически никогда не указываются контактные данные, нет формы обратной связи, либо она не работает. Максимальное внимание стоит уделить к разделу услуг доставки, предлагаемых на сайтах. Для проверки указанных услуг рекомендуется связаться с компанией-перевозчиком и перепроверить реквизиты платежа. Не стоит также переходить по сомнительным ссылкам. Оказание услуг неуполномоченными лицами и организациями через сайты-двойники, является незаконным и влечет предпосылки к мошенническим действиям, несоблюдение правового режима оборота персональных данных. Противодействовать фишинговым интернет ресурсам возможно путем обращения в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) которая после проверки блокирует в сети «Интернет» сайты содержащие информацию, распространение которой в Российской Федерации запрещено. Органами прокуратуры также осуществляется мониторинг сети «Интернет» и в случае выявления сайтов на которых содержится недостоверная информация в рамках исполнения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», направляют информацию в досудебном порядке в службу Роскомнадзора либо обращаются с заявлением в суд об ограничении доступа к сайтам и (или) страницам сайтов в сети «Интернет». Роскомнадзор включает заблокированные интернет-ресурсы в единую автоматизированную систему «Единый реестр доменных имен, указателей сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» с целью ограничения доступа к ним вне зависимости от действий операторов связи. Старший помощник Кирово- Чепецкого городского прокурора Н.С. Кокорева