# Профилактика киберпреступлений и мошенничеств, совершаемых с использованием информационно-коммуникационных технологий

*по материалам управления по противодействию киберпреступности криминальной милиции управления внутренних дел Могилевского областного исполнительного комитета*

Повсеместное внедрение и использование компьютерных информационных технологий, безусловно, создает возможности для более эффективного развития экономики, политики, общества и государства в целом. Однако совершенствование и применение высоких технологий приводит не только к укреплению информационного общества, но и появлению новых угроз, одной из которых является компьютерная преступность.

Как известно, Интернет не только содержит множество полезной информации и предоставляет выбор развлечений, но и таит массу угроз, которые могут повлиять и на материальное состояние семьи, и на психологическое здоровье детей.

Рассмотрим основные угрозы, которым подвергается население в современном киберпространстве.

## ВИШИНГ

**Вишинг** – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

При совершении звонков потерпевшим преступники используют, как правило, IP-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи. Кроме этого, зачастую злоумышленники используют мессенджеры Viber и WhatsApp, в которых существует возможность использования виртуальных номеров. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

Злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

## ФИШИНГ

**Фи́шинг** – вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой Интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: Kufar, Белпочта, службой доставки, банками, ЕРИП и т. д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.). Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, либо реквизиты своей БПК, то они становятся доступны мошенникам.

Стоит отметить, что применяемая злоумышленниками схема хищений характерна не только для Беларуси. Столь же системно эти преступления совершаются в отношении пользователей схожих ресурсов, ориентированных на иные государства СНГ: России (avito.ru), Украины (olx.ua), Казахстана (olx.kz) и др.

## СВАТИНГ

**Сватинг** – заведомо ложный вызов милиции, аварийно-спасательных служб, путем фальшивых (ложных) сообщений об опасности (например, о минировании, убийствах, захвате заложников).

Сватинг в первую очередь распространен в среде, где люди, чаще всего молодые, объединяются по каким-то целям. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» – когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о минировании какого-либо объекта.

В последние годы сватинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Общественная

опасность таких деяний состоит в том, что заведомо недостоверные сведения дезорганизуют нормальную работу объектов транспорта, предприятий, государственных органов и учреждений, организаций независимо от формы собственности. В свою очередь, это причиняет существенный экономический вред как субъектам хозяйствования, так и гражданам. При этом информация о возможном взрыве, поджоге либо иных действиях, предполагающих тяжкие последствия, способна посеять панику среди населения и внести неудобства в повседневную жизнь.

Стоит отметить, что ответственность за это преступление наступает с 14 лет. Наказание – штраф, арест, ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет. Если ребенку, сообщившему о ложном минировании, не исполнилось 14 лет, наступает административная ответственность родителей, а ребенка ставят на учет в инспекцию по делам несовершеннолетних.

## МОШЕННИЧЕСТВО В СОЦСЕТЯХ

В настоящее время особо актуальной становится проблема защиты аккаунтов в социальных сетях и противодействия различным формам и видам мошенничества. Наиболее типичные способы обмана в Интернете сегодня таковы:

**Предоплата:** злоумышленники размещают объявления о продаже каких-либо товаров по бросовым ценам, но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

**Шантаж и вымогательство:** в некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети – это ячейка персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в интернете.

**Онлайн-игры:** индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты БПК для покупки игровых

преимуществ и коллекционных предметов, которые игроки также нередко приобретают за реальные деньги.

## СОВЕТЫ ПО БЕЗОПАСНОСТИ

Существенную часть своей жизни современное общество проводят в интернете, а значит без базовых знаний в области кибербезопасности ему не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

**Советы родителям: е**сли ребенок хочет зарегистрироваться на каком-либо сайте, создать профиль в социальной сети и выложить свои фотографии, лучше уделите этому должное внимание. Взрослый человек сможет лучше проанализировать ситуацию и понять, опасен ли сайт, а также помочь выбрать снимки, которые можно выложить на всеобщее обозрение. Установите дистанционный контроль. Функция «родительского контроля» – это и как специализированное программное обеспечение, которое включает в себя: ограничение времени нахождения ребенка в сети; ограничение времени пользования компьютером; возможность создания графика с допустимыми часами работы в течение дня; блокировка сайтов с запрещенным контентом; ограничение на запуск приложений (например, игр и иных приложений) и установку новых программ. Беречь личные данные. Даже если ребенок думает, что хорошо знает человека, с которым общается онлайн, не нужно рассказывать подробности о себе и о родителях. Номер телефона, адрес, номер школы и класса, место работы родителей и их график, время, когда в квартире нет взрослых, а также данные из документов, номера банковских карт – такую информацию ни в коем случае нельзя передавать другим людям. Правило, приведенное выше, распространяется и на других людей. Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают. Нельзя показывать их фотографии – ни выкладывать их в своих профилях в социальных сетях, ни тем более в частной переписке. Если хочется выложить групповое фото с праздника или тренировки, сначала стоит обсудить это с теми, кто изображен на снимке. И лучше, если они сообщат родителям, что такое фото публикуется в Интернете.

**Советы всем пользователям сети Интернет:** надо научиться скептически относиться к любой информации, размещенной в Интернете, и не доверять слепо всему, что там пишут, т.к. мошенники активно используют Интернет в своих интересах. Они могут обманывать людей и манипулировать ими, давя на жалость или страх. Использовать сложные пароли, состоящие из букв и цифр. Определить четкий круг лиц, допущенных к важной информации и при кадровых

перестановках — менять пароли. По возможности не подключать компьютеры, содержащие важную информацию к сети Интернет, а если без этого не обойтись — не использовать для организации совместного доступа стандартные настройки службы удаленного рабочего стола. Обязательно создавать резервные копии важной информации на другие носители. Не посещать на компьютерах с важной информацией неизвестные сайты с подозрительным содержимым. Не запускать файлы, полученные из неизвестных источников. Не открывать файлы с активным содержимым, полученные по электронной почте от неизвестных источников, как бы они не назывались. Хранить номер карточки и ПИН–коды в тайне, а к своей основной карте в банке выпустить дополнительную, которой расплачиваться в Интернете, куда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее. Не перечислять деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если не убедились в благонадежности лица/организации, которым предназначаются средства; не переводить денежные средства на счета незнакомых лиц.