ЦИФРОВАЯ БЕЗОПАСНОСТЬ:
КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕР-ПРЕСТУПНИКА

(областная тема)

Почему и как совершаются преступления?

Условием, способствующим распространению числа имущественных преступлений, учтенных по линии ПК, является широкое распространение различных видов криптовалют и иных цифровых активов, операции с которыми зачастую не поддаются регулированию.

Правоохранители отмечают, что, учитывая, что основная масса преступлений, регистрируемых по линии киберпреступности, совершается с использованием различных методик социальной инженерии, то такие правонарушения могут совершаться только при условии, когда достаточно большие массы населения не владеют основами цифровой безопасности. Соответственно, доведение правоохранителями этой информации позволяет людям избежать подобных преступлений.

Важно отметить, что информатизация очень быстро распространяется во всех сферах деятельности. Учитывая активность подрастающего поколения и их желание испробовать каждую новинку, они более широко, чем люди старшего возраста, используют компьютерные технологии. Соответственно, во многом то, что им кажется невинной шалостью, на самом деле может образовывать состав преступления.

Какие киберпреступления самые распространенные?

Вишинг – один из методов мошенничества, когда 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.

Фиишинг – 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.

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

ДДОС-атаки – это атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен. В настоящее время DoS и DDoS-атаки популярны тем, что позволяют довести до отказа практически любую систему.

Груминг – это вхождение взрослого человека в доверие к ребенку с целью сексуального самоудовлетворения. Злоумышленник дистанционно нащупывает связь с ребенком через социальные сети, мессенджеры, онлайн-игры, электронную почту. Затем может вынудить ребенка прислать фотографии интимного характера, вовлечь в изготовление порнографических материалов, склонить к интимной встрече в реальности.

Кибербуллинг – травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди. Эта форма психологического террора может принимать разные обличия: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве; физическая агрессия и так далее. Причины кибербуллинга: зависть, чувство превосходства над соперником, чувство собственной неполноценности, самореализация.

Угроза нового времени – так называемые **группы смерти**. И хотя обычно создателями таких групп являются сами подростки (цель – «хайп», жажда острых ощущений, желание доминировать и управлять другими), в подобных группах создается благоприятствующая атмосфера для культивирования суицидальных намерений.

Как избежать уловок мошенников?

– Не вводите данные карты (особенно – срок действия и CVV-код) на сайтах, куда перешли по ссылкам от незнакомцев. Не соглашайтесь

уходить с торговой площадки и продолжать переписку в другом приложении.

– Не переходите ни по каким ссылкам из письма (даже если они якобы ведут к результатам игры). Через поисковик узнайте, действительно ли розыгрыш был проведен, есть ли другие призеры.

Помните, что визуально заметить подмену сложно, но есть характерные маркеры:

– замочек слева от адресной строки не замкнут или есть надпись «Не защищено»;

– электронный адрес ненастоящий или буквы в нем перепутаны (bel-post.by вместо belpost.by, bealrusbank.by вместо belarusbank.by).

– Не переходите по ссылкам на незнакомые ресурсы: с их помощью мошенники пытаются заразить ваш компьютер или телефон вирусом и украсть ваши личные данные.

– Не высылайте денег человеку, с которым вы лично не знакомы, и уж тем более не называйте ему личную информацию, способствующую взлому банковских данных и краже денежных средств.

– Если у вас есть сомнения в личности покупателя, лучше созвонитесь с ним, желательно по видеосвязи. Или, если это возможно, предложите личную встречу.

Как не стать жертвой при осуществлении финансовых операций в сети Интернет

Что сегодня может быть проще, чем купить в интернете понравившийся товар? Совершить такую покупку может даже ребенок или пользователь, не вполне уверенно владеющий навыками работы с персональным компьютером. Этот процесс обусловлен тем, что большинство людей сегодня все чаще испытывает дефицит свободного времени и тратить его на походы по магазинам, особенно в поисках обычных товаров, стало для многих недоступной роскошью. Кроме этого, купить или продать товар в сети Интернет стало очень просто благодаря огромному числу торговых площадок, которые делают этот процесс максимально быстрым и удобным, предоставляя возможность оплаты с использованием банковских платежных карт и доставки товара в любой уголок мира.

Наиболее распространены способы совершения преступлений:

1. «Предоплата» (обман продавца)

Суть данного способа заключается в том, что злоумышленник выступает в роли покупателя. На одной из интернет-площадок с объявлениями он находит продавца и копирует его контактные данные. После чего ищет его в мессенджерах (социальных сетях), представляясь покупателем. В ходе переписки, злоумышленник сообщает, что товар ему

понравился, и он хочет его приобрести в связи с чем уже якобы совершил предоплату (зачастую высылается скриншот электронного карт-чека о перечислении средств). Для того, чтобы получить данные средства продавцу высылают ссылку на поддельную страницу (она выглядит как один из разделов официального сайта интернет-площадки или банковского учреждения), где продавцу нужно ввести номер своей карты, имя держателя, срок действия, CVV-код указанный на оборотной стороне карты (информацию, содержащуюся в СМС-сообщении, поступившем из банка, для подтверждения получения предоплаты). После получения конфиденциальных сведений, злоумышленник совершает хищение средств.

2. «Доставка» (обман покупателя)

Злоумышленник размещает объявление на интернет-площадке о продаже товара по крайне выгодной цене. После того, как потенциальный покупатель начинает вести переписку во внутреннем чате площадки, злоумышленник под различными предлогами убеждает его продолжить общение в мессенджере или социальной сети. Во время общения мошенник уговаривает покупателя внести предоплату или оформить доставку, и чтобы развеять сомнения покупателя, сообщает о якобы новой услуге удержания (холдирования) средств, которая появилась на торговой площадке, т.е., если доставка не произойдет, то торговая площадка автоматически вернет средства на карту. При этом покупателю высылается ссылка на поддельную страницу, которая имитирует официальную страницу торговой площадки или интернет-банкинга, где нужно ввести данные карты (далее осуществляются действия по схеме обмана продавца).

3. Использование социальных сетей

Осуществив несанкционированный доступ к персональным аккаунтам пользователя сети Интернет, злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон).

4. Звонок от «представителя» банка с просьбой срочно предоставить необходимую информацию

Преступники от имени сотрудников банка сообщают, что необходимо осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. Для маскировки преступники используют функцию «подмены номера», как следствие у потерпевшего на экране мобильного телефона может отображаться совершенно любой абонентский номер телефона, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным. Получив необходимую информацию о реквизитах карты, преступники осуществляют хищение.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

– вести общение с покупателями (продавцами) только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);

– ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);

– очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;

– уточнить у собеседника номер телефона, если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);

– использовать отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;

– избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки;

– если Вы все же перешли по подобной ссылке и видите уведомление о том, что в системе имеется денежный перевод и для его получения необходимо ввести данные банковской платежной карты, ни

при каких обстоятельствах не вводите запрашиваемые сведения, так как это прямой путь к утрате собственных средств;

– если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо в срочном порядке произвести блокировку карты, позвонив в банк либо самостоятельно в интернет-банкинге;

– если Вам поступил звонок из «банка», ни при каких обстоятельствах никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме;

– уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы;

– если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения.