**Меры профилактики киберпреступлений**

Как правило, схемы мошенничества однотипны. Чаще всего жодинцы становятся жертвами фишинга и вишинга. Первый способ помогает мошенникам узнать конфиденциальные данные пользователей с помощью фишинг-ссылок. Так, злоумышленник в переписке убеждает человека перейти на сайт и ввести персональную информацию, например, логин, пароль или данные карты. Чаще всего фишинг используют в почтовых рассылках, на платформах с досками объявлений о купле-продаже или в переписках в мессенджерах. В свою очередь, вишинг – вид мошенничества, при котором жертву пытаются убедить раскрыть личные данные во время телефонного разговора. Злоумышленники при этом играют определенную роль, например, сотрудников банка или специалистов по борьбе с киберпреступностью. Обычно звонок поступает с иностранного номера в мессенджере. Большинство подобных дел раскрыть сложно или даже невозможно, потому что злоумышленники тщательно шифруют свои данные.

Недавно в ГОВД обратилась 67-летняя женщина. Ей позвонил уже привычный «сотрудник банка», но попросил аферист не данные карты, а данные учетной записи в интернет-банкинге – приложении для управления счетами и осуществления банковских операций через интернет. Пенсионерка выдала заветную информацию мошеннику, после чего с ее карты списали около двух тысяч рублей. Но преступник на этом не остановился. Используя украденные данные, он взял онлайн-кредит на четыре тысячи рублей, которые также списал с карты доверчивой женщины. В результате пострадавшая лишись не только своих накоплений, но и осталась с нешуточным долгом.

В последнее время популярным видом преступлений в сети Интернет стало вымогательство. В большинстве случаев потерпевшие с использованием мобильных устройств или персональных компьютеров осуществляли выход в Интернет, посещали сайты социальной сети «ВКонтакте». Знакомство происходило по инициативе девушки: либо девушка первой присылала личное сообщение, либо ставила оценку профилю потерпевшего, после чего он начинал общение с ней. После непродолжительного общения на вышеуказанных интернет-площадках от девушки поступало предложение начать общение в интернет-мессенджере «Skype». Далее девушка предлагала молодому человеку заняться «виртингом» - так называемым «виртуальным сексом». В процессе «виртинга» видеотрансляция обрывалась и потерпевшим поступали текстовые сообщения, в которых неустановленное лицо сообщало, что все действия потерпевшего зафиксированы на видео, после чего начинался шантаж: предъявлялись требования о перечислении денежных средств (как правило, на электронные кошельки какой-либо международной платежной системы) под угрозой распространения интимной видеозаписи среди знакомых в социальных сетях.

Также в некоторых случаях неустановленное лицо предлагало обменяться с потерпевшим фотографиями интимного характера, после чего поступали требования о перечислении денежных средств за их нераспространение в сети Интернет, а иногда осуществлялся несанкционированный доступ к аккаунтам потерпевших, где размещалась информация интимного содержания, которая впоследствии копировалась преступником и становилась предметом торга под угрозой распространения в социальных сетях.

В результате угроз некоторые потерпевшие перечисляли денежные средства, другие - нет.

В структуре преступности по-прежнему преобладают мошенничества в сети Интернет.

В ходе анализа преступлений указанной категории преобладают факты не поставки оплаченных товаров, когда потерпевший осуществляет перевод денежных средств на банковскую карту имитированную банком, осуществляющим деятельность на территории Республики Беларусь, что усыпляет бдительность покупателя, который рассчитывает, что продавец находится на территории Республики Беларусь и это дает гарантию того, что товар будет доставлен, а в действительности выясняется, что владельцы указанных банковских карт являются лишь посредниками при переводе денежных средств и не подозревают, что участвуют в мошеннической схеме. Аналогичная ситуация складывается и в предоставлении со стороны продавца якобы своих паспортных данных гражданина Республики Беларусь (фотография паспорта), которыми мошенник завладевает в ходе переписки с иными добросовестными покупателя, указывая, что их анкетные данные необходимы для осуществления сделки.

Еще одним из способов завладеть денежными средствами граждан является поступающая просьба от якобы знакомого одолжить денежные средства. При этом преступник создает «фейковую» страницу или осуществляет несанкционированный доступ к аккаунту знакомого потерпевшего, после чего от пользователя данного аккаунта рассылает сообщения с просьбой одолжить денежные средства.

Также в последнее время участились случаи обращения граждан по факту завладения денежными средствами под предлогом получения кредита без поручителей и справки о доходах или же с целью быстро заработать деньги, когда потерпевший переводит определенную сумму для оплаты услуги за перевод ему денежных средств, после чего с ним переписка прекращается, и никакие денежные средства в его адрес не поступают.

Поэтому, чтобы не стать жертвой преступников, не доверяйте незнакомым людям и избегайте общения с подозрительными собеседниками, а также не предоставляйте доступ к своим аккаунтам и персональным данным неизвестным лицам; не храните конфиденциальную информацию в свободном доступе; при получении сообщения с просьбой перевести денежные средства перепроверьте данную информацию, позвонив своему знакомому; при осуществлении звонка в ваш адрес со стороны якобы работника банка не предоставляйте ему конфиденциальную информацию, а сами связывайтесь с работниками банка по имеющимся контактным номерам на банковской карте или по номерам указанным на официальном сайте банка.

В текущем году киберпреступники в своей противоправной деятельности активно используют информационно-коммуникационные технологии. Ключевыми факторами, способствующими успеху преступной деятельности в сети Интернет, являются легкомыслие и излишняя доверчивость граждан, чрезмерная отзывчивость, а иногда и отсутствие элементарной бдительности.

Из общего числа зарегистрированных преступлений основная масса связана с несанкционированными доступами злоумышленников к персональным страницам популярных социальных сетей, в ходе которых, последние, мошенническим путем получают все необходимые данные для последующего хищения денежных средств. Не редко злоумышленники, изучив личную информацию (переписка, фотографии и тщ.), которую владелец неосмотрительно хранил у себя на персональной странице и хотел оставить в тайне, используют для вымогательства.

Как правило, злоумышленники осуществляют распространение ссылок на «фишинговых», поддельных, сайтах социальных сетей, где пользователи собственноручно вводят «логин» и пароль. Поддаться соблазну: перейти по ссылке, граждан подталкивают различные заманчивые предложения, такие как получение бесплатного «стикера», участие в розыгрыше дорогостоящего устройства и т.п.

По-прежнему актуальными остаются действия киберпреступников по шифрованию информации, хранящейся на компьютерном оборудовании и в локальных сетях юридических и физических лиц.

Внедрение новых финансовых инструментов и способов получения денежных средств с одной стороны упрощают взаимодействие граждан с банками и кредитно-финансовыми организациями, однако с другой стороны создает благоприятную среду для совершения различных мошеннических схем.

Так под благовидным предлогом, например, за небольшое вознаграждение в связи с оказанием помощь в получении кредитов, граждане передают данные для доступов в системы «Интернет-банкинг», фотографии с изображением страниц паспорта, 5М5-сообщения получаемые на свой мобильный телефон, тем самым не осознавая последствия таких действий, позволяют злоумышленникам совершить хищения.

**Как же не стать жертвой киберпреступника?**

Для этого нужно запомнить и руководствоваться следующими рекомендациями:

* Использовать сложные (уникальные) и различные пароли доступа к своим учетным данным (электронным почтовым ящикам, аккаунтам в социальных сетях, личным кабинетам системы «Интернет-банкинг»);
* Не переходить по сомнительным (фишинговым) ссылкам и запускать загруженные из сети Интернет-файлы без предварительной их проверки на специализированных сетевых ресурсах;
* Использовать специальное программное обеспечение (антивирус, расширение для веб­браузеров), чтобы избежать посещения сомнительных ресурсов;
* Подключить и использовать двухфакторную аутентификацию;
* Обмениваться сообщениями в социальных сетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагировать на сомнительные просьбы и предложения;
* Хранить в тайне ПИН-код к банковской платежной карте;
* Никому ни под каким предлогом не передавайте реквизиты и пароли от банковских карт, в том числе CVV-код – трехзначное число на обратной стороне карты. Тем, кто не пользуется онлайн-оплатой, стоит приобрести карту без CVV-кода.
* Никогда не используйте один и тот же пароль для всех веб-ресурсов. Старайтесь создавать уникальные сочетания. Если мошенник узнает один из паролей, он не сможет получить доступ к остальным интернет-аккаунтам.
* Не устанавливайте подозрительные приложения. Особенно, если ссылку на него прислал незнакомец. Вообще, старайтесь не переходить по сомнительным ссылкам на сторонние сайты и ресурсы. Это правило актуально, например, для электронной почты и платформы Kufar.
* Вы часто совершаете покупки в интернете? Создайте дополнительную карту, на которую вы сможете переводить незначительные суммы. В случае хищения данных, это убережет от масштабных потерь.
* Поставьте лимит на сумму списания и перевода средств с карты. Это можно сделать в интернет-банкинге или обратившись в банк.
* Будьте внимательны с прикрепленными файлами в интернет-письмах от незнакомцев. Старайтесь проверять вложения на наличие вирусов. Также никогда не заполняйте формы и анкеты в интернете, полученные по электронной почте от неизвестных.
* Не отправляйте никому личные данные или денежные средства, если вы не уверены в надежности человека или организации.
* При необходимости проверяйте «сотрудника банка» или «родственника». Вы всегда можете перезвонить им напрямую, чтобы уточнить, связывались ли они с вами накануне. Не стоит доверять иностранным номерам и аккаунтам, звонящим в мессенджерах. Помните, что сотрудник банка никогда не будет спрашивать у клиента реквизиты банковской карты, тем более посредством звонка в мессенджере!
* Мошенники стараются, чтобы вы нервничали и действовали необдуманно. Сохраняйте самообладание. Без ваших личных данных злоумышленники не смогут провернуть ни одну схему. Будьте внимательны и осторожны в интернете!