**ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ**

*Материал подготовлен Хотимским районным отделом внутренних дел*

Киберпреступность является новой и одной из быстроразвивающихся формой транснациональной преступности. Сеть Интернет стала практически незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники не могут этим не пользоваться. Два миллиарда пользователей Интернета по всему миру создают идеальную среду для совершения преступлений, где можно действовать анонимно и получать доступ к любой персональной информации, которую мы, желая того или нет, размещаем в сети. В последние годы безопасность в сети Интернет подвергается более серьезным угрозам, и от преступлений в глобальном киберпространстве страдают более 431 миллиона взрослых пользователей.

**Что такое киберпреступление**

В настоящее время при характеристике компьютерных преступлений используется целый ряд понятий: *«информационное преступление», «киберпреступление», «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий», «виртуальное преступление».*

Согласно действующему законодательству Республики Беларусь, в содержание понятия ***«компьютерная преступность»*** включают:

1) преступления против информационной безопасности (модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

2) хищения путем использования средств компьютерной техники;

3) изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего;

4) иные преступления, так или иначе связанные с использованием компьютерной техники: доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет; разглашение врачебной тайны; незаконное собирание либо распространение информации о частной жизни; клевета; оскорбление; распространение ложной информации о товарах и услугах; заведомо ложное сообщение об опасности; шпионаж; умышленное либо по неосторожности разглашение государственной тайны; умышленное разглашение служебной тайны и др.

Таким образом, к компьютерным преступлениям относятся правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

**Персональные данные в социальных сетях: важные правила безопасности**

Неотъемлемым элементом нашей повседневной коммуникации становятся социальные сети и мессенджеры.

Вместе с позитивными изменениями соцсети и технологии больших данных способствуют возникновению нового общества наблюдения, которое создает угрозы конфиденциальности. В большинстве случаев условием получения интересующих услуг выступает указание своих персональных данных, предоставление согласия на их обработку, согласие с политиками конфиденциальности. Все это подвергается анализу и используется для самых разных целей.

Страницы в соцсетях, куда люди добровольно выкладывают личную информацию и фотографии, смотрят не только друзья (исключение – закрытый профиль).

Часто – это безграничный источник сведений для мошенников.

Приведём несколько примеров.

Фото из отпуска оповещают, что вас нет дома.

Хвалебные посты о дорогостоящих покупках сориентируют других на предмет Вашего финансового состояния.

Метка геолокации на фото в соцсети, сделанном по месту проживания, позволяет установить дом, в котором живёт лицо, опубликовавшее фотографию.

Размещая личный номер мобильного телефона или электронной почты в сетях, Вы рискуете получить шквал ненужных Вам звонков, сообщений, рассылок с рекламными предложениями, а можете попасться «на удочку» аферистов.

Предупрежден – значит вооружен. Напомним о базовых правилах безопасного оборота Ваших персональных данных в социальных сетях.

1. Читайте политику конфиденциальности соцсети. Важно знать, кто будет обрабатывать Ваши персональные данные, как хранить и использовать.

2. Делитесь сокровенными моментами своей жизни только с близкими, а для этого уделите внимание настройкам конфиденциальности в соцсетях, закройте страницы. В настройках профиля есть раздел «Приватность». В нём Вы можете ограничить круг тех, кто сможет писать вам сообщения, оставлять комментарии или видеть основную информацию Вашей страницы. Следуйте правилам безопасности, если Вы решили оставить профиль открытым и видимым для всех.

3. Установите в соцсетях и мессенджерах двухэтапный вариант проверки, который позволяет создать персонализированный PIN-код для большей безопасности от нарушений и хакеров.

4. Не публикуйте в открытом доступе избыточную информацию: адреса, номера телефонов, даты рождения. Это же касается и сведений о родных и близких, не публикуйте чужие фото и видео (даже совместные) и иную личную информацию без согласия на то человека. Вы просто не имеете на это права.

5. Не используйте геолокацию, когда размещаете в соцсетях фото дома, не отмечайте на нем адрес. Зачастую по умолчанию к каждому снимку, который Вы делаете, привязывается местоположение. Оно сохраняется в метаданных изображения. Функция вполне удобная: можно открыть карту и посмотреть, в каких местах Вы делали фотографии. Но зачем это знать посторонним людям?

6. Получили новый паспорт, водительское удостоверение? Не публикуйте фото с документами, где видны данные. Это же касается билетов на самолет.

7. Не пересылайте и не храните в соцсетях и мессенджерах документы, пароли, коды, реквизиты банковской карты и счетов. Это очень чувствительные данные.

8. Не рекомендуем входить и авторизироваться на сторонних сайтах через учетную запись соцсети. Не всегда перед входом можно проверить «надежность» ресурса, а это, в свою очередь, чревато тем, что доступ у управлению страницей могут перехватить.

9. Используйте проверенные антивирусные службы и лицензионное ПО.

10. Следует воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

11. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт по просьбе пользователей сети Интернет.

12. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам необходимо использовать сложные пароли, исключающие возможность их подбора. Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).

Настройте уникальные и надежные пароли для всех своих учетных записей. Использование одних и тех же паролей многократно увеличивает риск их взлома.

Помните, информация, размещенная в социальных сетях, остается там навсегда. Прежде чем публиковать очередной пост или что-то писать в комментариях, необходимо подумать, проверить и убедиться в необходимости такой публикации. И хотя всегда можно удалить нежелательные сообщения, Вы не знаете, кто собрал эту информацию и Ваши персональные данные раньше и что с этими данными намеревается делать, в том числе, возможно, использовать против Вас.

*Справочно:*

*По состоянию на 15 июля 2024 года в Хотимском районе зарегистрировано 8 преступлений, связанных с мошенническими действиями в сети интернет.*

*К примеру:*

*9 февраля 2024 года возбуждено уголовное дело по признакам преступления, предусмотренного ч.1 ст.209 УК Республики Беларусь в отношении неустановленного лица.*

*Неустановленное лицо, имея умысел на завладение денежными средствами обманным путем, в неустановленное время, на странице «DebosH» в социальной сети «Instagram» в сети «Интернет» разместило объявление о продаже мужской одежды и обуви, после чего 14.11.2023 вступило в переписку с гражданином Н, в ходе которой они договорились о покупке двух мужских курток, двух пар мужских кросовок, двух мужских шапок, двух мужских спортивных штанов, двух мужских спортивных кофт. Затем 22.11.2023 за указанную одежду гражданин Н со своей банковской карты на банковскую карту продавца перевел денежные средства в общей сумме 270 руб. После чего, вышеуказанную одежду гражданину Н никто не выслал и денежные средства в общей сумме 270 рублей не вернул.*

*29 февраля 2024 года возбуждено уголовное дело по признакам преступления, предусмотренного ч.1 ст.209 УК Республики Беларусь в отношении неустановленного лица.*

*Неустановленное лицо, находясь в неустановленном месте, имея умысел на противоправное безвозмездное завладение имуществом гражданина Т 27.02.2024 по средством мессенджера «Skype» осуществили звонок с абонентского номера РБ представившись специалистом службы безопасности ОАО «Белагропромбанк», путем обмана, убедили последнего перевести денежные средства в сумме 1900 рублей на расчетный счет ОАО «БНБ-Банк».*

*11 апреля 2024 года возбуждено уголовное дело по признакам преступления, предусмотренного ч.1 ст.209 УК Республики Беларусь в отношении неустановленного лица.*

*Неустановленное лицо, находясь в неустановленном месте, 05.04.2024 получив несанкционированный доступ к анкете в мессенджере «Telegram», принадлежащей гражданки А, имея единый умысел на хищение денежных средств, путем обмана, под предлогом оказания материальной помощи, в ходе переписки, убедила гражданина Е перевести денежные средства в сумме 370 рублей и 200 рублей, которые последняя перевела на указанную неустановленным лицом банковскую платежную карту, причинив тем самым потерпевшей материальный ущерб на общую сумму 570 рублей.*

*09 июля 2024 года возбуждено уголовное дело по признакам преступления, предусмотренного ч.3 ст.209 УК Республики Беларусь в отношении неустановленного лица.*

*Неустановленное лицо, с использованием учетных записей месенджера Viber, Telegram в период времени с 17.06.2024 по 04.07.2024 путем обмена текстовыми сообщениями и живого общения под предлогом инвестирования в акции компании «Газпром» убедило гражданина Г осуществить переводы в период времени с 24.06.2024 по 04.07.2024 на предоставленные банковские платежные карты (БПК) и счета: в сумме 339 рублей с БПК на БПК, в сумме 11189 рублей посредством инфокиосков ОАО «Беларусбанк» и ОАО «Белагропромбанк» на банковский счет, совершив хищение денежных средств гражданина Г на общую сумму 11 528 рублей.*

Киберпреступность принимает самые различные формы, чаще всего – преступлений, связанных с персональными данными. Они могут совершаться при помощи *"фишинга"* (обмана пользователей сети Интернет с целью заставить их сообщить свои персональные данные), вредоносных программ (программного обеспечения, устанавливаемого без ведома пользователя и собирающего персональные данные) и взлома (незаконного получения удаленного доступа чужому компьютеру). Как правило, подобные методы применяются мошенниками для кражи данных кредитных карт и денежных средств. Кроме того, через Интернет все чаще совершаются преступления, связанные с нарушением авторских прав и прав интеллектуальной собственности, а также распространением материалов с детской порнографией и сценами насилия.

**Как не стать жертвой киберпреступления?**

1. Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

***ВНИМАНИЕ: помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp).***

2. При составлении платежных документов важно проверять платежные реквизиты получателя денежных средств.

3. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек не следует отвечать на подобные сообщения, а необходимо связаться с данными пользователями напрямую посредством иных средств связи.

4. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

5. Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров; не переходить по ссылкам в сообщениях о призах и выигрышах.

6. Необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

7. Следует ознакомить с перечисленными правилами безопасности своих родственников и знакомых, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.