Элементарные правила цифровой безопасности.

Все пользуются Интернетом. Но Интернет – это не только развлечения. Какие опасности могут вас подстерегать в сети.

Цель киберпреступников – похитить деньги у тех, кто не очень внимательно относится к сохранению своих персональных данных – полных реквизитов банковской карты, логина и пароля к сервисам, идентификационного номера паспорта, кодов из СМС.

Для вывода похищенных денежных средств мошенникам необходимы промежуточные счета. Для этого они через мессенджеры подбирают людей, готовых предоставить за вознаграждение свои личные данные – реквизиты банковских карт или данные доступа к личному кабинету в банке.

Мошенники уверяют, что такие деяния не влекут ответственности, однако это не так. В банковском договоре указано, что предоставлять личные данные запрещено.

НАПРИМЕР. 14-летний ученик Витебской школы попросил на некоторое время в пользование у своего 15-летнего одноклассника его банковскую платежную карту. Парень уже имел аккаунт на криптовалютной бирже. Неизвестные лица связались с ним в мессенджере и предложили заработать. Молодой человек предоставил реквизиты банковской карты друга, на которую он получил 10 000 рублей, после чего для них с этой карты купил криптовалюту на всю сумму. В ходе проведения проверки установлено, что полученные деньги были похищены у пенсионера из Витебска.

Таким образом, школьник оказал услуги по покупке-продаже криптовалюты третьим лицам, что влечет ответственность за незаконную предпринимательскую деятельность по ч.3 ст. 13.3 КоАП Республики Беларусь.

В настоящее время решается вопрос о привлечении его законных представителей к административной ответственности.

ЕЩЕ ПРИМЕР. 16 подростков из двух учреждений среднего специального образования области, связавшись с заказчиком из Интернета, оформляли на свое имя банковские карты и за вознаграждение от 15 до 50 рублей передавали их или их реквизиты неустановленному лицу для использования. С помощью этих банковских карт и счетов киберпреступники переводили похищенные деньги. В отношении 8 подростков возбуждены уголовные дела, в отношении остальных – проводится проверка и решается вопрос о возбуждении уголовных дел.

Надо знать, что легких денег не бывает, а сомнительный заработок в сети может повлечь за собой ответственность за незаконную предпринимательскую деятельность или незаконный оборот средств

платежа по ст. 222 УК. (Профилактический ролик расположен по адресу: https://t.me/cifgram/492)

Иногда киберпреступники охотятся за деньгами взрослых.

Чтобы сохранить деньги родителей нельзя передавать кому бы то ни было в сети личные данные.

1. НАПРИМЕР. «Вконтакте» переписывались девочки, хотели помочь приюту для животных. Одна по просьбе другой передала данные фотографии маминой карты с двух сторон.

Чтобы защитить свои деньги от расчетов в сети, нельзя никому передавать данные карты с оборотной стороны, и на всякий случай, необходимо подключить услугу 3-D Secure.

2. Используя телефон родителей никому нельзя передавать цифры из СМС и устанавливать приложения, даже если собеседники представились сотрудниками госорганов и предлагают сохранить деньги от мошенников.

НАПРИМЕР. Девочка 10 лет в Витебске ответила на звонок в мессенджере и согласилась на предложение помочь маме сохранить деньги. Она передала личный номер из паспорта и цифры из СМС. В итоге мошенники смогли оформить на маму кредит и теперь семья его выплачивает.

3. В других случаях, злоумышленники по звонку из Viber побуждали детей ВЫПОЛНЯТЬ ОПАСНЫЕ ДЕЙСТВИЯ.

Так, в июле 2023 года в Полоцке мужчина, представившийся сотрудником службы поддержки Viber для обновления «посоветовал» 10-летней девочке скачать определенное приложение, которое предоставляет ему возможность управлять ее устройством, а удостоверившись в том, что она дома одна, убедил положить фольгу, а потом куриные яйца в микроволновую печь, каждый раз включая ее на 2 минуты.

В августе 2023 года в Верхнедвинске 6-летней девочке мужчина представился сотрудником милиции, сказал, что для проверки исправности газовых плит необходимо включить газовую конфорку, выйти из кухни на 30 минут, после чего вернуться и зажечь огонь.

Для включения функции «**Защита от лишних звонков**» необходимо в Viber последовательно нажать следующее: Еще→Настройки→Вызовы и сообщения→Защита от лишних звонков (установить галочку).

4. Нельзя использовать чужую банковскую карту.

НАПРИМЕР. Так в Орше школьники по дороге в школу нашли утерянную банковскую карту и воспользовались ею в ближайшем магазине – купили угощения, а также недорогие сувениры.

Такие действия также влекут уголовную ответственность с 14 лет.

5. Нельзя использовать чужую банковскую карту, даже в Интернете

НАПРИМЕР. В банкомате мужчина забыл свою банковскую карту. Другой ее обнаружил и сфотографировал с двух сторон, но себе не забрал, а обратно вставил в тот же банкомат. Первый мужчина обнаружил пропажу и вернулся за картой, забрал ее и продолжал пользоваться ей.

Так как данные его карты уже были скомпрометированы вторым мужчиной, через некоторое время он воспользовался данными и совершил оплату в Интернет-магазине с найденной банковской карты. Действия второго мужчины повлекли уголовную ответственность. За такие деяния также предусмотрена уголовная ответственность с 14 лет.

А вот у первого мужчины если бы в настройках карты была подключена услуга 3-D Secure, он бы был предупрежден через СМС от банка об операциях по его карте в Интернете и смог бы остановить оплату.

Нельзя никому давать фотографировать банковскую карту.

С 14 лет уже можно получить в банке и использовать собственную банковскую карту. Чтобы никто случайно не смог зафиксировать сведения о карте, безопасно привязывать карту к мобильному приложению и рассчитываться телефоном с функцией бесконтактной оплаты.

6. Нужно сохранять в тайне свои личные данные для игр.

НАПРИМЕР. В Полоцке школьник играл в Танки. Другой игрок предложил ему «прокачать» оружие, передав на время доступ к аккаунту. После передачи доступа второму игроку в аккаунте был изменен пароль и привязан другой номер телефона, а мальчик потерял свои достижения в игре, приобретенные за реальные деньги.

В этом преступлении злоумышленник установлен и привлечен к уголовной ответственности.

7. Через компьютерные игры дети иногда доказывают сою значимость. Но иногда игры переходят в реальную жизнь.

Среди подростков существует мнение, что можно отомстить обидчику, добавив ему проблем. Так иногда подростки на электронную почту организации направляют сообщения о том, что она заминирована. В письме иногда просят перевести деньги, иногда пишут данные отправителя письма с расчетом, что за это его привлекут к ответственности.

Надо помнить, что все действия в сети сохраняются и рано или поздно отправитель письма будет установлен, а уголовная ответственность за такие деяния наступает с 14 лет.

НАПРИМЕР. В Орше отвергнутый молодой человек, желая отомстить новому другу бывшей девушки, отправил от его имени электронное письмо с заведомо ложным сообщением об опасности. Ранее

другой подросток из области направлял аналогичные письма, чтобы сорвать уроки в школах. В настоящее время в отношении парней возбуждены уголовные дела, им грозит вплоть до 7 лет лишения свободы. Все материальные затраты на работу спецслужб при эвакуации людей придется компенсировать им или их родителям.

8. Пароли в СОЦ СЕТИ. Все смотрят ролики блогеров, они получают за просмотры деньги, это их заработок.

Для того чтобы хакеры не завладели деньгами, необходимо соблюдать цифровую гигиену – устанавливать сложные пароли к аккаунтам, в Интернете использовать отдельную виртуальную карту, привязывать аккаунт к номеру телефона.

Иногда родители могут совершать ошибки в Интернете. Многие привязывают свои зарплатные карты к приложениям такси, доставки пиццы, суши, торговых площадок. Иногда, хакеры взламывают приложения и продают данные карты родителей. В сети используйте отдельные виртуальные карты и не храните на них много денег.

Научите родителей использовать в Интернете отдельную виртуальную карту и активировать на ней услугу 3-D Secure.

9. НАПРИМЕР. Хакеры взламывают аккаунты в социальных сетях, устанавливают сведения о вас, о ваших родителях, бабушках и дедушках, или ваших друзьях, а потом начинают переписываться с вами, просят отправить им что-то личное. Нельзя указывать в Интернете свои реальные данные и данные родителей. Киберпреступники могут даже шантажировать вас, если у них найдется компрометирующая вас информация – фото или сообщения. Они могут требовать деньги или отомстить за невыполнение требований, например, от вашего имени заминировать школу или другой объект.

10. Киберпреступники могут представляться ровесниками и сами начать общение с вами, а потом просить отправить им в Интернете ваши личные фотографии, обещая заплатить за это деньги. После получения первых просят отправлять все больше и больше фотографий, а потом могут вас заставлять делать опасные вещи или просить деньги взрослых, пугая, что покажут эти фотографии одноклассникам или родителям. Такие факты действительно существуют, поэтому, нельзя доверять незнакомцам в соцсети – любой может оказаться не тем, кем представляется.

11 В «Instagram» часто продают недорогие вещи. Нужно тщательно проверять информацию о магазине и оплачивать покупки только после получения на почте. Иногда мошенники преднамеренно получают предоплату, позже сообщают, что доставка товара не возможна, и предлагают вернуть деньги обратно, при этом покупателю направляют

фишинговую ссылку, на которой требуется ввести полные данные карты, включая трехзначный код на обороте, предназначенный только для расходных операций. Под предлогом возврата денег, покупатели иногда становятся дважды обманутыми киберпреступниками.

12. Нельзя никого оскорблять в соцсети, ответственность за это, как и в обычной жизни. Если вы не достигли возраста наступления ответственности, то за ваши поступки будут отвечать родители.

Управление по противодействию киберпреступности
криминальной милиции
УВД Витебского облисполкома