**ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ**

Развитие общества не стоит на месте. Компьютерные технологии и Интернет стремительно проникают во все сферы жизнедеятельности человека. Появляются новые виды преступлений. В настоящее время хищение денежных средств с банковских счетов является актуальной проблемой.

На сегодняшний день в молодёжной среде мы вряд ли найдем кого-либо, кто не был бы зарегистрирован «В Контакте», «Фейсбуке», «Инстаграмм», на каких-либо тематических форумах или иных площадках для виртуального общения. В целом это норма, ведь человек живет в обществе и стремится общаться. Однако некоторая неопытность, наивность и доверчивость порой приводит к негативным последствиям.

По данным статистики, дети начинают пользоваться Интернетом с 4 лет (в среднем). В возрасте до 12 лет около 85% подрастающего поколения активно использует Всемирную паутину для общения и развлечений.

Ежедневно около 4-х человек в области становятся в среднем потерпевшими от действий киберпреступников. Средний ущерб, причиненный киберпреступлениями, составляет 1151 рубль. Больше половины потерпевших – женщины. Большинство – со средним специальным и высшим образованием, в возрасте до 40 лет.

**Опасности в социальных сетях:**

1. *Заражение вирусом*– даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержанием;
2. *Нежелательный контент* - то есть информация, непригодная для возраста ребёнка (сцены насилия, жестокости, информацию о наркотиках, азартные игры, религиозные конфликты и т.д.);
3. *Интернет зависимость (игромания)*
4. *Опасности, связанные с общением:*

* *Ложное представление о собеседнике.*Основная проблема социальных сетей – это доверие к тем, кто находится по ту сторону монитора. Собеседники в Интернете чаще всего не видят друг друга. «Дружеский» стиль общения, распространенный в социальных сетях, обманчив – он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией. Это открывает двери для злоумышленников.
* *Эффект «онлайн-растормаживания»* (анонимность, виртуальность). Благодаря этому эффекту люди позволяют себе в Интернете такое поведение и высказывания, которые никогда бы себе не позволили в реальном мире. Считают, что останутся безнаказанными.
* *Троллинг* - на Интернет-сленге – это намеренно агрессивное, хамское, провокационное, оскорбительное поведение в Интернет-дискуссии. Цель тролля (тролль — это тот, кто занимается троллингом) — доведение собеседника до белого каления, разжигание склок в дискуссиях, провоцирование взаимных оскорблений и т. д.
* *кибербуллинг –*это когда ребенку в социальных сетях отправляют какие-то неприятные изображения, шантажируют, оскорбляют, создают целые группы, чтобы гнобить его. Зачинщики таким способом просто развлекаются. Главное правило — не кормить «троллей» своими эмоциями, не отвечать на их сообщения, не реагировать.

Ответственность за ТРОЛЛИНГ, КИБЕРБУЛИНГ:

* **Оскорбление** — умышленное унижение чес­ти и достоинства личности, выраженное в неприличной форме. Например, в сети гражданин получает сообщение, в котором содержится информация, унижающая его честь и достоинство, выраженное в неприличной форме, то есть содержит нецензурные выражения. Стоит обратить внимание, что сообщение может быть и правдивым, но выражено в грубой и неприличной форме. За такое деяние предусмотрен **штраф в размере до 20 базовых величин (статья 9.3 КоАП).**
* **Клевета**— распространение заведомо ложных, позорящих другое лицо измышлений. Например, в интернете гражданин получает сообщение, в котором содержится информация, не соответствующая действительности. Ответственность за такое действие предусматривает штраф в размере**до 30 базовых величин (статья 9.2 КоАП).**
* За оскорбление и клевету, осуществленные в публичной форме, например, сообщение размещено в свободном доступе в интернете и с ним могут ознакомиться посторонние граждане, лицо, его разместившее (распространившее), может быть привлечено к уголовной ответственности (**статья 188 и 189 УК Республики Беларусь**). В данном случае, нарушителю грозит не только штраф, но и исправительные работы на срок до 2 лет, или арест, или ограничение свободы до 3 лет. Также оскорблением или клеветой может быть признана информация, содержащаяся в видеороликах, карикатурах, демотиваторах, мемах и гифках.

*4. Лица, которые хотят эксплуатировать детей:*

* *дети могут выдать незнакомцам конфиденциальную (скрытую, личную) информацию о себе и родителях* (имя, адрес, номер счета или электронного кошелька)
* *знакомство со злоумышленниками*(для этого они обычно втираются в доверие, чтобы уже потом договориться с ребенком. Они могут назначить встречу, общаться о неподобающих вещах, манипулировать, шантажировать и т.д.)

*5. Опасные агрегаторы фото и видео*

Сейчас много сервисов, где люди выкладывают различные видео о своей жизни. Дети и подростки часто размещают там материалы неприличного характера. Этот поступок имеет отложенный эффект: если ребенок выложит такую информацию в 13−15 лет, то это может повлиять не только на его карьеру, но и на будущую жизнь. Важно понимать: все, что попадает в интернет, остается в интернете, даже если вы удалили свою публикацию, фото.

Ответственность за изготовление и распространение порнографических материалов или предметов порнографического характера (статья 343 Уголовного Кодекса РБ) Передача порнографической информации в основном осуществляется через социальные сети. Многие относятся к передаче фотографий или видеороликов порнографического характера как к игре. Но даже их демонстрация на экранах телефона или компьютера, размещение в социальных сетях, проставление «Лайка» является преступлением. Наказывается от 2 до 4 лет лишения свободы.

*6. Площадки-шпионы*

Существуют сообщества, которые собирают компрометирующие фото, видео, надписи в виде скриншотов. Мы не знаем, куда утечет выложенная нами информация, поэтому каждый раз нужно тщательно думать, нажимая кнопку «опубликовать».

*7. Неосознанные покупки в магазинах онлайн*

*8. Взлом пользовательских записей социальных ресурсов*. Источников утечки персональной информации о логинах и паролях лежит на самих пользователях, которые осуществляли авторизацию на иных ресурсах или в приложениях через свои учетные записи в социальных сетях, например для скачивания музыки или видеофайлов, получения мнимого выигрыша.

В случае обнаружения «взлома» аккаунта следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого, следует оповестить друзей и знакомых об инциденте, используя при этом иные социальные сети и мессенджеры. Специалисты по безопасности рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты, помимо этого в настройках страницы в разделе «Безопасность» подключить услугу «Подтверждение входа». При этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который автоматически будет выслан на указанный при регистрации страницы номер.

С каждым годом интернет-мошенники и взломщики становятся все моложе. Самым распространенным способом интернет мошенничество среди несовершеннолетних – использование банковских карт родителей (других членов семьи) при покупке донат.

Донат – в онлайн играх обычно обозначает оплату игроком дополнительных бонусов, уникальных предметов и прочих благ, не доступных обычным путем, без оплаты реальными деньгами. Чаще всего, в чистом виде, донат встречается в бесплатных играх. В платных же играх, как, например, WOW, под донатом подразумевается приобретение уникальных петов (животные, существа, привязанные к персонажу и сопровождающие его в игре) и маунтов (средство передвижения), доступных в игре только за наличные деньги. Дети сообщают данные банковских карт своих близки, с банковского счета снимаются деньги.

 Дети нарушают статью 212 Уголовного Кодекса РБ «Хищение путем использования компьютерной техники, либо путем введения в компьютерную систему ложной информации - наказывается лишением свободы до 3 лет. Те же действия, совершенные повторно, либо в группе по предварительному сговору – на срок до 5 лет.

Статья 349 Уголовного Кодекса РБ «Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, – наказывается штрафом или арестом. Те же действия, повлёкшие крушение самолета, аварию, катастрофу, несчастные случаи с людьми, отрицательное изменение окружающей среды или иные тяжкие последствия, – на срок до 7 лет.

*9. Вишинг*

Мошенники звонят, выдают себя за сотрудника банка. Под предлогом отмены какой-либо операции с деньгами или возврата случайно списанной суммы, выманивают у вас секретные данные: номер, срок действия и трехзначный код на обороте платежной карты. Используя эти сведения, переводят деньги себе на счет.

Или предлагают установить программу якобы для отмены таких операций и назвать код ее регистрации. На самом деле эта программа для удаленного доступа к вашему устройству. Она позволяет злоумышленникам войти в ваш мобильный банкинг и похитить деньги с вашего счета или даже оформить на вас онлайн-кредит.

Иногда к разговору подключаются сообщники, которые представляются сотрудниками милиции или следственных органов, и просят помочь разоблачить мошенника в банке. Для этого необходимо оформить в нескольких банках кредиты и полученные деньги временно перевести на якобы «специальный защищенный счет». При этом мошенники постоянно удерживают свою жертву «на крючке» – не дают закончить разговор, чтобы одуматься, позвонить или поговорить с родными, а также слышать, что происходит вокруг и постоянно держать человека в страхе и напряжении.

Чтобы не стать жертвой киберпреступников, в случае поступления звонка из банка, следует закончить разговор и самостоятельно перезвонить в банк по номеру на обороте платежной карты и уточнить все ли в порядке с вашим счетом.

*10. Фишинг*

Еще один способ, когда мошенники завладевают персональными данными и совершают хищение денежных средств.

Мошенник точно копирует настоящий и создает фишинговый сайт. Чаще всего подделывают почтовые сервисы (КУФАР, Белпочта, Европочта, СДЭК), но иногда и платежные системы банков (ОАО «Беларусбанк», ОАО «БелАгроПромБанк»), сервисов оплаты (билетов театра, аренды кальянной). Интернет-адрес в названии похож на настоящий, но есть отличие в названии или домене. Далее письма, содержащие фишинговую ссылку, рассылаются потенциальным потерпевшим.

Ссылки на поддельные страницы часто присылают в мессенджерах продавцам товаров с сайтов объявлений якобы для получения аванса за продаваемый товар или оформления доставки курьером. Фишинговые страницы содержат сведения о товаре, повторяют фирменный стиль и сервисы сайта, например. онлайн-консультант. Злоумышленник стремится получить все данные карты, в том числе трехзначный код с обратной стороны, а также смс-коды от банка или даже логины и пароли для входа в Интернет-банкинг. Эти данные позволяют ему перевести все деньги с карты владельца, а в случае передачи идентификационного (личного) номера паспорта оформить онлайн-кредит.

*Примеры фишинговых страниц: belpochta.by, bellpost.by, belpocht.by, belpost.be, europocha.be, kufar.cc, bel-bank.online.by и подобные.*

Чтобы не стать жертвой киберпреступников, перед совершением платежей самостоятельно зайдите на официальный сайт банка, уже с него перейдите в свой личный кабинет.

Переходите в интернет-банкинг только с официального сайта банка, а не по ссылкам, даже из поисковых систем.

Помните, что для получения оплаты никогда не требуется вводить трехзначный код с оборотной стороны карты.

В интернет-адресе белорусских организаций после последней точки обязательно должен быть домен BY, а за ним наклонная черта \*\*\*.BY/\*\*

**ПАРОЛИ.** Получив доступ к аккаунту пользователя в соцсети (методом подбора пароля или вредоносного программного обеспечения), **злоумышленник осуществляет рассылку сообщений интернет-друзьям и ждет отклика, убеждает под разными предлогами передать денежные средства или конфиденциальную информацию, например, фотографии или данные банковской карты.**

Устанавливайте сложные пароли, используйте цифры и буквы разного регистра.

Если вам пришло письмо от вашего друга с просьбой одолжить деньги, убедитесь, что это именно он прислал сообщение и нуждается в вашей помощи.

***ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ КИБЕРПРЕСТУПНИКОВ***

Никому не доверять по телефону и ни под каким предлогом не передавать номер банковской карты, срок действия, трехзначный секретный код на обороте, логины и пароли доступа к банкингу, смс-коды от банка.

Подключить услугу «3D Secure» (обязательное подтверждение операций в сети Интернет смс-кодами от банка) и никому не передавать коды (не вводить на страницах).

При поступлении звонка от работника банка или сотрудника милиции, закончить разговор и самостоятельно перезвонить в банк или милицию.

Не устанавливать программы по указанию незнакомых лиц.

Не переводить деньги по указанию, полученному по телефону даже от работников банка или милиции.

Установить в Вайбер защиту от нежелательных звонков. При поступлении звонка от абонента, не внесенного в телефонную книгу, вы увидите пропущенный звонок и, если нужно, сможете сами перезвонить. (Viber ® Еще ® Настройки ® Вызовы и сообщения ® Защита от лишних звонков).

Настроить ограничения по своей банковской карте: выставить запреты на проведение операций в Интернете, установить максимальные суммы расходов в день (неделю, месяц).

В адресе сайта белорусских организаций обязательно после имени сайта должен быть короткий домен (BY), а после него наклонная черта (\*\*\***.by**/\*\*\***).**

Тщательно проверять адрес сайта на наличие опечаток — это может быть копия официального ресурса, специально созданного для введения в заблуждение.













