Профилактика киберпреступности среди несовершеннолетних.

С каждым годом интернет-мошенники и взломщики становятся все моложе. Современные подростки проводят в интернете большую часть своего времени, но возможности Всемирной паутины каждый использует по-разному. Около 92% родителей Беларуси не знают о потенциально опасных активностях своих детей в интернете. При этом 58% несовершеннолетних скрывают от родителей, чем на самом деле они занимаются в сети.

За 10 месяцев текущего года в Гомельской области было совершено 4 киберпреступления несовершеннолетними.

Самым распространенным способом киберпреступлений 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 — увеличенная скорость прокачки, уникальная и мощная экипировка, хитрая валюта за которую можно купить в игре что-то ядреное, вкусности, оружие и т.д. В платных же играх, как например World of Warcraft, под донатом подразумевается приобретение уникальных петов или персонажей (животные, существа, привязанные к персонажу и сопровождающие его в игре) и маунтов (средство передвижения доступное персонажу), доступных в игре только за наличные деньги.

Родителям также рекомендовано с использованием сети Интернет изучить игровой сленг, на котором общаются подростки, для того чтобы понимать о чем идет речь при общении с ребенком. Также ребенку очень нравится, когда его родители спрашивают, что означает то или иное слово. Таким образом, устанавливаются с ребенком доверительные отношения.

Многие родители не зная, что их ребенок геймер тратит свои карманные деньги на донат игр, становиться зависим от этого. Ребёнок геймер донатит, чтобы казаться лучше других игроков и иметь преимущество над ними в игре.

Дети, совершая оплату своих персонажей чужими банковскими картами, нарушают ст. 212 Уголовного Кодекса РБ (хищение имущества путем модификации компьютерной информации).

Под данную статью уголовного кодекса попадают следующие действия несовершеннолетних:

1) С использованием найденной банковской карты осуществляют снятие денег в банкомате либо оплачивают с использованием платежного терминала покупки в торговых точках (магазины, кафе и т.д.).
2) С использованием украденной банковской карты производят оплаты в Интернет-магазинах (Aliexpress, Joom и т.д.).
3) Активируют на мобильном телефоне другого человека услугу, предоставляемую компанией А1, «А1-банкинг» и переводят на свой абонентский номер телефона деньги, которые предоставляет компания в качестве кредита в размере 100 рублей.

Несовершеннолетние **за совершение таких киберпреступлений** несут уголовную ответственность с 14 лет!

По статьи 212 УК Республики Беларусь:

1. Хищение имущества путем модификации компьютерной информации –
наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, –
наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, –
наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без

штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, –

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Кроме этого в поле зрения правоохранителей попадают несовершеннолетние, совершающие несанкционированный доступ к компьютерной информации (ст. 349 УК Республики Беларусь).

Данные действия заключаются в следующем:

Несовершеннолетние осуществляют несанкционированный доступ к электронной почте, учетным записям на различных сайтах, игровых платформах, в том числе в социальных сетях, а также к информации, содержащейся на компьютере, в смартфоне, с использованием различных программ удаленного доступа, методов социальной инженерии, таких как «вишинг» и «фишинг» (когда получаешь логины и пароли путем обмана и введение в заблуждение владельца информацией). Как правило, несанкционированный доступ к компьютерной информации влечет за собой совершение ряда киберпреступлений, таких как ст. 350 (уничтожение, блокирование или модификация компьютерной информации) или ст. 208 УК (вымогательство).

Чаще всего несанкционированный доступ осуществляют к учетным записям социальных сетей «ВКонтакте» и «Instagram».

Несовершеннолетние **за совершение таких киберпреступлений** несут уголовную ответственность с 16 лет!

Максимальный срок наказания по ст. 349 УК составляет 7 лет лишения свободы, по ст. 350 УК – 10 лет лишения свободы, по ст. 208 УК – 15 лет лишения свободы.

Рекомендации по профилактике киберпреступлений среди несовершеннолетних.

Первое и самое главное правило «Установите с ребенком доверительные отношения и **положительный** эмоциональный контакт в вопросе использования сети Интернет».

Для детей от 10 до 13 лет.

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;

- используйте средства фильтрации нежелательного контента;

- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета;

- поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;

- расскажите об ответственности за недостойное поведение в сети Интернет.

На данном этапе могут активно использоваться **программные средства родительского контроля**, к которым можно отнести следующие инструменты:

- услуга родительского контроля провайдера, оказывающего услугу доступа в сеть Интернет, позволяющая ограничить доступ к Интернет сайтам, содержащим нежелательный контент;

- функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);

- функции родительского контроля, встроенные в некоторые антивирусы (напримерKasperskyInternetSecurity, NortonInternetSecurity), позволяющие контролировать запуск различных программ, использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержимого, пересылку персональных данных;

- специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например, КиберМама, KidsControl, TimeBoss и другие.

Подростки в возрасте 14-17 лет.

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;

- настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета;

- напоминайте о необходимости обеспечения конфиденциальности личной информации;

- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.

В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации классному руководителю, социальному педагогу учреждения образования, в правоохранительные органы по месту жительства.