



БЫТЬ ХАКЕРОМ: не развлечение, а преступление!



Уголовная ответственность за киберпреступления наступает:



Статья 212 УК Беларуси

с 14
лет



Хищение путем использования компьютерной техники или введения в компьютерную систему ложной информации наказывается вплоть до лишения свободы на срок **до 3 лет**.



Те же действия, совершенные повторно или группой лиц по предварительному сговору, наказываются лишением свободы на срок **до 5 лет**.



Если хищение крупное, то предусмотрено наказание в виде лишения свободы на срок **до 7 лет**.



За хищение, совершенное организованной группой или в особо крупном размере, грозит **до 12 лет** лишения свободы.

Статья 349 УК Беларуси

с 16
лет



Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, наказывается вплоть до лишения свободы на срок **до 2 лет**.



За несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, грозит наказание вплоть до лишения свободы на срок **до 7 лет**.

Памятка о безопасности в интернете

ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом или арестом на срок до шести месяцев.

2. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Модификация компьютерной информации

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Модификация компьютерной информации, сопряженная с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, - наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 351. Компьютерный саботаж

1. Умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, - наказывается лишением свободы на срок от трех до десяти лет.

Статья 352. Неправомерное завладение компьютерной информацией

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, - наказываются общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети - наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами -

наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, повлекшие тяжкие последствия, - наказываются лишением свободы на срок от трех до десяти лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, -наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, -наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, -наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Наиболее распространенные методы работы злоумышленников



выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов знакомых в социальных сетях



ЛЖЕПОКУПАТЕЛЬ - под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошеннический сайт, визуально похожий на официальный сайт банка



ВИШИНГ - представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты конфиденциальную информацию (ее реквизиты, а также номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды)



НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные



ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка



Для защиты денежных средств клиентов у банка есть вся необходимая информация



Работники банка по телефону не должны спрашивать ни реквизиты карты, ни паспортные данные



Не давайте никому свой мобильный телефон и предупредите об этом ваших близких, особенно детей и лиц пожилого возраста

Источник: Национальный банк Беларуси.

© Инфографика

Опасные картиннки

Практически каждый из нас является счастливым обладателем мобильного телефона, а многие – и компьютера.

В школе, транспорте, дома – ты всегда на связи и готов к общению. И не только к общению. Как же хочется поделиться какими-нибудь новыми картинками, фотографиями или видео, скачанными из Интернета с друзьями, одноклассниками и просто знакомыми!

А теперь ответь себе на вопрос: «Как часто я задумываюсь о том, какую картинку, фотографию или видео посылаю другому лицу и будет ли мне что-нибудь за это?». Думаю, что ответ не заставит себя долго ждать.

Вместе с тем, не всегда такие картинки, фотографии или видео столь безобидны, а их передача другому лицу – безнаказанна.

Дети, подростки, молодежь часто хотят знать информации намного больше, чем им могут предоставить родители, школа или общедоступные Интернет-ресурсы. И их любопытство порой оказывается на грани, а иногда и за гранью дозволенного.

Признайся себе, ведь хоть раз в жизни ты, тихонечко, прячась от родителей смотрел в Интернете «особые» картинки, фотографии или видео? И у тебя может даже возникала мысль, что круто бы было показать «это» своим друзьям, одноклассникам, просто знакомым? И вот ты сохраняешь эти картинки, фотографии и видео на свой мобильный телефон или любимый компьютер и...

Вот тут и начинается история, у которой может и не быть счастливого конца.

История 1. Молодая девушка Екатерина дома с помощью ноутбука скачала 3 порнографических изображения и через несколько дней разместила их в сети Интернет на одном из сайтов для общего доступа.

История 2. Александр, Дмитрий и Вадим передали хранящиеся в их мобильных телефонах порнографические материалы через Bluetooth одной девушке.

История 3. Юрий скачал в Интернете видеоролик порнографического содержания и разместил его на своей странице в социальной сети «ВКонтакте», где его мог просмотреть неограниченный круг пользователей.

История 4. Александр, используя личный компьютер и сеть Интернет разместил в своей анкете в одной из социальных сетей порнографическое изображение, в результате чего оно стало доступно для просмотра и копирования другими пользователями.

История 5. Молодой человек со своего электронного ящика отправил девушке одно порнографическое изображение.

История 6. Молодой человек с использованием сети Интернет через сайт «ВКонтакте» переслал (распространил) порнографический материал на мобильный телефон другого лица.

Всех этих молодых людей объединяет одно - в отношении каждого из них было впоследствии возбуждено уголовное дело.

В Уголовном кодексе Республики Беларусь есть ст.343, которая предусматривает ответственность за изготовление и распространение порнографических материалов или предметов порнографического характера.

Изготовление либо хранение с целью распространения или рекламирования либо распространение, рекламирование, трансляция или публичная демонстрация порнографических материалов, печатных изданий, изображений, кино-, видеофильмов или сцен порнографического содержания, иных предметов порнографического характера наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом (ч.1 ст.343 УК Республики Беларусь).

Те же действия, но совершенные, в том числе, с **использованием глобальной компьютерной сети Интернет**, иной сети электросвязи общего пользования либо выделенной сети электросвязи, а равно распространение, рекламирование, трансляция или демонстрация заведомо несовершеннолетнему порнографических материалов, печатных изданий, изображений, кино-, видеофильмов или сцен порнографического содержания, иных предметов порнографического характера, совершенные лицом, достигшим восемнадцатилетнего возраста, наказываются **только** лишением свободы на срок от двух до четырех лет (ч.2 ст.343 УК Республики Беларусь).

Все уголовные дела, приведенные в шести историях выше возбуждены по ч.2 ст.343 УК Республики Беларусь, так как во всех случаях распространение информации осуществлялось с использованием глобальной компьютерной сети Интернет или иной сети электросвязи общего пользования либо выделенной сети электросвязи, соответственно наказание за такое преступление может быть очень суровым.

Относится или нет материал или предмет к порнографическим - решит экспертная комиссия.

А что же такое **хранение** порнографических материалов или предметов? Ты хранишь их, когда они фактически находятся у тебя во владении, и потом ты хочешь их распространить.

А **распространяешь** ты их тогда, когда совершаешь действия, направленные на то, чтобы ознакомить с такой информацией неопределенный круг лиц. Распространение может выражаться в рекламировании, передаче на любых основаниях, в том числе путем показа или демонстрации кому-либо.

Все фигуранты наших историй распространяли порнографические материалы, когда передавали их друг другу, другим лицам, в том числе, друзьям и знакомым. Даже показав другу в телефоне или компьютере такой фильм или фотографию, ты рискуешь своей свободой.

Демонстрировать можно по-разному. Это и показ в виде фотографии, слайда, кино-, телекадра на экране либо с помощью другого технического устройства или любым иным способом.

Ответственность за совершение такого преступления наступает с шестнадцати лет, а за распространение, рекламирование, трансляцию или демонстрацию заведомо несовершеннолетнему порнографических материалов - с восемнадцати лет.

Но если ты не достиг 16 лет (или 18 лет при демонстрации несовершеннолетнему) – это не значит, что никакой ответственности ты не понесешь.

Если факт выявлен, то будет проводиться проверка и приниматься решение об отказе в возбуждении уголовного дела. Если же, например, уголовное дело было возбуждено, так как сразу лицо, совершившее преступление, не было установлено, а потом оно стало известно и выяснилось, что не достигло возраста привлечения к уголовной ответственности - принимается решение о прекращении производства по уголовному делу из-за недостижения возраста, с которого наступает уголовная ответственность.

Копия одного из таких постановлений направляется органом дознания или предварительного следствия в комиссию по делам несовершеннолетних для проведения с тобой необходимой профилактической работы. Впоследствии ты подлежишь постановке на учет в инспекцию по делам несовершеннолетних, и с тобой будет проводиться индивидуальная профилактическая работа. Более того, в отношении тебя даже может быть решен вопрос о направлении в специальное учебно-воспитательное учреждение (ст.14 Закона Республики Беларусь «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»).

И помни, что глобальная сеть Интернет является объектом пристального внимания сотрудников управлений по нарконтролю и противодействию торговле людьми, они проводят постоянные мониторинги сетей и выявляют распространителей порнографии. Также информация о наличии в свободном доступе порнографических материалов или предметов порнографического характера, их передаче или получении может поступать от обычных граждан и даже от твоих друзей и знакомых (о чем ты можешь даже не догадываться).