Информационно - справочные материалы

Повсеместное внедрение и использование компьютерных информационных технологий, безусловно, создает возможности для более эффективного развития экономики, политики, общества и государства в целом. Однако совершенствование и применение высоких технологий приводит не только к укреплению информационного общества, но и появлению новых угроз, одной из которых является компьютерная преступность.

По итогам 2023 года в отношении несовершеннолетних было совершено 646 киберпреступлений, из которых: вымогательство – 56; мошенничество – 440; хищение путем модификации компьютерной информации – 120; несанкционированный доступ к компьютерной информации – 23; уничтожение, блокирование или модификация компьютерной информации – 2; неправомерное завладение компьютерной информацией – 5.

Справочно.

За пять месяцев текущего года в результате совершения киберпреступлений были признаны потерпевшими 173 несовершеннолетних, в отношении которых были совершены киберпреступления, из них: вымогательство – 33; мошенничество – 99; хищение путем модификации компьютерной информации – 31; несанкционированный доступ к компьютерной информации – 11; уничтожение, блокирование или модификация компьютерной информации – 2.

Основные угрозы, которым подвергается молодежь в современном киберпространстве.

Вишинг – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее - БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

В большинстве случаев при совершении звонков потерпевшим преступники используют IP-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи. Кроме этого, зачастую злоумышленники используют мессенджеры Viber и WhatsApp, в которых существует возможность использования виртуальных номеров. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

Злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев

реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: почта, службой доставки, банками, ЕРИП и т. д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.). Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, они становятся доступны мошенникам.

Сватинг – заведомо ложный вызов милиции, аварийно-спасательных служб, путем фальшивых ложных сообщений об опасности (например, о минировании, убийствах, захвате заложников).

Сватинг в первую очередь распространен в среде, где люди, чаще всего молодые, объединяются по каким-то целям.

Справочно.

Например, в онлайн- играх. У них есть термин «вызвать милицию на дом» – когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о минировании какого-либо объекта.

В последние годы сватинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Общественная опасность таких деяний состоит в том, что заведомо недостоверные сведения дезорганизуют нормальную работу объектов транспорта, предприятий, государственных органов и учреждений, организаций независимо от формы собственности. В свою очередь, это причиняет существенный экономический вред как субъектам хозяйствования, так и гражданам. При

этом информация о возможном взрыве, поджоге либо иных действиях, предполагающих тяжкие последствия, способна посеять панику среди населения и внести неудобства в повседневную жизнь.

Стоит отметить, что ответственность за это преступление наступает с 14 лет. Наказание – штраф, арест, ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет. Если ребенку, сообщившему о ложном минировании, не исполнилось 14 лет, наступает административная ответственность родителей, а ребенка ставят на учет в инспекцию по делам несовершеннолетних.

Справочно.

Ярким примером сватинга является международная преступная группа «KRONOS», деятельность которой пресечена в 2022 году. Группой руководил белорус 2007 года рождения, в ее состав также входили 9 россиян. Участники преступной группы направили около 300 ложных сообщений в адрес объектов, расположенных на территории Российской Федерации, а также 4 – в Республике Беларусь.

DoS – это атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен. В настоящее время DoS и DDoS-атаки популярны тем, что позволяют довести до отказа практически любую систему.

Обычно атака организуется при помощи троянских программ. Предварительно трояны заражают недостаточно защищенные компьютеры обычных пользователей и могут довольно долгое время никак себя не проявлять на зараженном компьютере, ожидая команды от своего хозяина. Компьютер может подвергнуться такой атаке при посещении различных зараженных сайтов, при получении электронной почты или при установке нелицензионного программного обеспечения. Когда злоумышленник собирается начать атаку, он дает команду, и все ранее зараженные компьютеры начинают одновременно слать запросы на сайт-жертву.

Справочно.

Наиболее массовая DoS-атака в Беларуси была произведена экстремистскими каналами в 2021 году. Злоумышленники, намеренно утаивая информацию об уголовной ответственности за участие в DoS- атаке, привлекли к участию в ней более 10 тысяч граждан (преимущественно из числа молодежи). Практически все участники этого противоправного действия были установлены, а наиболее активные из них были привлечены к уголовной ответственности.

Груминг – это вхождение взрослого человека в доверие к ребенку с целью сексуального самоудовлетворения. Злоумышленник дистанционно нащупывает связь с ребенком через социальные сети, мессенджеры, онлайн-игры, электронную почту. Затем может вынудить ребенка прислать

фотографии интимного характера, вовлечь в изготовление порнографических материалов, склонить к интимной встрече в реальности.

От груминга отличают секстинг — это пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных интернет-сетей.

Кибербуллинг - травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

Эта форма психологического насилия может принимать разные обличия: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве; физическая агрессия и так далее.

Причины кибербуллинга: чувство превосходства, зависть, чувство собственной неполноценности, самореализация.

Угроза нового времени – так называемые группы смерти. И хотя обычно создателями таких групп являются сами подростки (цель - «хайп», жажда острых ощущений, желание доминировать и управлять другими), в подобных группах создается благоприятствующая атмосфера для культивирования суицидальных намерений.

В настоящее время особо актуальной становится проблема защиты аккаунтов в социальных сетях и противодействия различным формам и видам ***мошенничества***. Наиболее типичные способы обмана в соцсетях сегодня таковы:

Предоплата

Злоумышленники размещают объявления о продаже каких-либо товаров по бросовым ценам, но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

Шантаж и вымогательство

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в интернете.

Онлайн-игры

Индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты БПК для покупки игровых преимуществ, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги.

Существенную часть своей жизни современные дети и подростки проводят в интернете, а значит без базовых знаний в области кибербезопасности им, как и взрослым, не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

Мы прекрасно осознаем, что эффективное противодействие киберпреступности может осуществляться только в рамках комплексного стратегического подхода, предполагающего не только точечные меры, а и целенаправленные и спланированные совместные действия государственных органов, объединений, гражданского общества, школы и семьи.

Рекомендации по использованию на различных устройствах (компьютерах, мобильных телефонах, планшетах, IPTV) специальных программ, обеспечивающих возможность родителям контролировать информационные ресурсы, посещаемые детьми, время их нахождения в сети Интернет

1. В целях защиты информации и ограждения детей от угроз в сети Интернет рекомендуется осуществить подписку на программные продукты антивирусной защиты мобильных устройств: Kaspersky Standard Mobile, PRO32 Mobile Security. Данное программное обеспечение позволяет выстроить настройки приватности в социальных сетях, заблокировать доступ к устройству в случае потери или кражи.

2. Для осуществления постоянного мониторинга активности ребенка в сети Интернет рекомендуется воспользоваться услугой «Родительский контроль» от РУП «Белтелеком». Данное программное обеспечение позволяет:

ежедневно получать отчеты об интернет-активности ребенка;

установить контроль времени использования устройств (блокировать устройство или показывать предупреждение ребенку);

настроить правила доступа ребенка к приложениям (получать статистику и задавать правила использования приложений; блокировать приложения, которые имеют возрастные ограничения; получать согласие родителя на использование отдельных приложений по запросу; мгновенно уведомлять родителя о попытке запуска запрещенного приложения);

настроить правила посещения веб-сайтов (включить безопасный поиск, безопасный поиск на YouTube; настроить разрешенные категории поиска веб-сайтов; заблокировать определенные веб-сайты, все сайты или добавить разрешенные веб-сайты в исключения).

3. Также с целью защиты детей от негативного влияния сети Интернет рекомендуется воспользоваться комплексной услугой «Безопасный Интернет» от РУП «Белтелеком». Данная услуга представляет собой комплект программных продуктов, который позволяет обеспечить защиту компьютеров, смартфонов и планшетов от вредоносных программ (вирусов) и мошеннических операций (фишинга).

4. Для ограничения доступа несовершеннолетних детей к видеоконтенту при просмотре интерактивного телевидения «ZALA» от РУП «Белтелеком» рекомендуется воспользоваться предусмотренным функционалом телевизионных приставок IPTV. Функция «Родительский пароль» позволяет установить настройки доступа по уровням возрастных ограничений: 0+, 3+, 6+, 12+, 16+, 18+.