ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

КРИМИНАЛЬНОЙ МИЛИЦИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

для сотрудников органов внутренних дел

по теме противодействия киберпреступности



Минск, 2021**Содержание**:

|  |
| --- |
|  |
| Тема № 1. Вишинг . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 3 |
| Тема № 2. Фишинг . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 5 |
| Тема № 3. Сваттинг . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  | 7 |
| Тема № 4. Социальные сети и мессенджеры . . . . . . . . . . . . .  | 8 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Тема № 1. Вишинг**

**«Хищение имущества путем модификации компьютерной информации (ст. 212 УК РБ)»**

В Беларуси по-прежнему острой остается проблема совершения хищений денежных средств со счетов белорусов мошенниками, под видом «лжебанкиров» звонящих на телефоны белорусов и выведывающих конфиденциальную информацию.

С начала этого года на территории Республики Беларусь было совершено свыше 10 тысяч киберпреступлений, что на 53% больше по сравнению с аналогичным периодом прошлого года.

Почти на 70% (с 5.243 до 9.119) увеличилось количество ***хищений имущества путем модификации компьютерной информации***. При этом существенный рост (почти на 450%) произошел за счет увеличения количества этих хищений в особо крупных и крупных размерах.

Сегодня наиболее часто встречаются три основные типа дистанционного хищения средств со счетов граждан.

1. Самая распространенная схема – «звонок из банка». Так, под видом работника банка звонящий сообщает, что якобы кто-то пытается перевести со счета жертвы деньги, и для блокировки операции просит сообщить номер банковской платежной карты и CVV-код. Расчет при этом идет на стрессовую ситуацию, в которой оказывается жертва, а также секундную утерю ею концентрации. Если жертва сообщает реквизиты – преступник моментально обнуляет счет, переведя деньги себе на счет.

2. Вторая схема – «получение кредита». На телефон жертвы поступает звонок через мессенджер (как правило, Вайбер) от злоумышленника. Тот представляется либо сотрудником работником, либо высокопоставленным сотрудником правоохранительных органов (информацию о милиционерах и номера служебных телефонов найти не составляет труда). Он сообщает, что якобы со счета жертвы кто-то пытается вывести все деньги и предлагает совместно поймать преступника за руку: для этого от жертвы требуется открыть кредитную линию в банке и сообщить «лжесотруднику» реквизиты счёта. Если жертва следует алгоритму, то со счёта преступник похищает все деньги, оставляя пострадавшего с обязательством погашения выплаченных денег.

3. Суть третьей схемы заключается в получении дистанционного доступа к мобильному устройству жертвы. Как и в предыдущих схемах, злоумышленник под видом работника банка сообщает об угрозе, нависшей над банковским счетом жертвы. Якобы для защиты счета просят абонента установить на своем телефоне программу удаленного доступа (AnyDesk, TeamViewer и др.) и предоставить им код доступа. Если жертва соглашается, то преступники получают полный контроль над устройством: как правило, они заходят в приложение интернет-банкинга на телефоне владельца, и переводят деньги с его счёта на свой собственный.

*Специалисты ГУПК КМ МВД предупреждают!*

1. Никогда и ни при каких обстоятельствах не сообщайте по телефону незнакомым лицам персональные данные, коды из СМС и так далее. Работники банков или правоохранительных органов владеют необходимой информацией, вашего опроса им не требуется.
2. Ни в коем случае не предоставляйте доступ к устройству посторонним лицам. Не устанавливайте по их просьбам программы и не сообщайте коды доступа.
3. Заблокировать ваш карт-счет работники банка могут и без вашего участия, поэтому все подобные звонки – очевидное мошенничество.
4. Если у вас возникли сомнения в отношении происходящего, незамедлительно обратитесь в банк и сообщите о звонке.
5. Обезопасьте свой основной банковский счет! Для совершения онлайн-платежей откройте в том же банке другой счет, который сможете пополнять при необходимости. И если даже этот счет будет скомпрометирован, ваш основной останется в безопасности.
6. Нередки случаи, когда под предлогом позвонить родственнику неизвестные просят воспользоваться вашим телефоном и, получив его, моментально открывают микроредит и переводят деньги себе на счёт. В итоге мошенник получает ваши деньги, а вы – кредитные обязательства по выплате.

**Тема № 2. Фишинг**

*Фишинг* (от англ. fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) и последующего хищения денежных средств.

Наиболее частым примером фишинговой атаки может служить сообщение, отправленное жертве по электронной почте и подделанное под официальное письмо – от банка или платёжной системы – требующее проверки определённой информации или совершения действий. Такие письма обычно содержат ссылку на фальшивую веб-страницу, в точности похожую на официальную и содержащую форму, требующую ввести конфиденциальную информацию.

Наиболее массовым способом совершения такого вида киберпреступлений в Беларуси явилось использование злоумышленниками интернет-площадки «Kufar», как источника поиска жертв преступлений, осуществляющих продажу (покупку) товаров. Организованные группы, взаимодействуя через закрытые чаты мессенджера Telegram осуществляют «отработку» потенциальных потерпевших, получая реквизиты банковских платежных карт путем обмана или направления ссылки на фишинговый интернет-ресурс. Похищенные средства переводятся в виде криптовалюты, чаще всего на электронные кошельки, оформленные на подставных лиц.

Еще одним способом фишинговых преступлений является подмена оригинальных сайтов. Зачастую в доменных именах второго уровня данных ресурсов указаны наименования, созвучные с названиями банковских учреждений и сервисов *(belarusbank-erip.online, ibank-belapb24.com, epey.by, e-rip.cc, erip.cc, dostavka-kufar.by и иные).* Пройдя по такому адресу и введя данные конфиденциальные сведения, человек отправит их непосредственно мошеннику.

***Меры безопасности:***

Если не терять бдительности, то защититься от фишинга вполне реально. В первую очередь, следует быть внимательнее с URL (адресом) ссылки, полученной по почте, или загрузившейся страницы банка. Адрес похож на настоящий во всем, кроме главного: домена второго уровня. Например, вместо адреса https://online.belarusbank.by могут быть использованы: https://online.belarusbank.**erip**.by, https://online. belarus.**bank**.by. Поэтому, прежде чем вводить свои логин и пароль на странице, стоит удостовериться в том, что вы находитесь на подлинном ресурсе. Для этого внимательно прочтите адресную строку ресурса в браузере, поищите гиперссылки на самой странице и попробуйте по ним перейти.

Не следует слепо доверять ссылкам, полученным посредством SMS-сообщения или в электронном письме. Как бы правдоподобно ни выглядели призывы их авторов нажать ссылку, делать этого не следует.

При использовании онлайн-площадки «Kufar» общайтесь с потенциальным покупателем только непосредственно на данном сайте и не соглашайтесь продолжить общение в иных мессенджерах - технически сайт защищает вас от получения ссылок на фишинговые ресурсы. Не спешите выполнять просьбы потенциальных покупателей о переводе денег через платежные интернет-системы по присылаемым ссылкам, так как не исключено, что под видом платежной системы она ведет на фишинговый ресурс. Следует самостоятельно ввести адрес системы и уже непосредственно на оригинальном сайте вводить данные банковской платежной карты.

**Тема № 3. Сваттинг**

**«Заведомо ложное сообщение об опасности» (ст.340 УК)**

В последнее время участились сообщения о лжеминировании различных объектов социальной сферы, предприятий, развлекательных и торговых центров. Из числа общего количества число тех, которые сопряжены с использованием компьютерной техники, составило 113 фактов с начала этого года.

В основном мы ведем речь о так называемом сваттинге. Это новое явление для Беларуси, но уже весьма активное. Подростки, объединенные одним интересом (как правило, участники сетевых игр), от имени своего соперника по игре сообщают в органы правопорядка о таких вот «лжеминированиях» и тем самым «подставляют» его. Основной мотив – развлечение и получение хайпа, причинить максимум неприятностей недругу. Часто подростки таким способом мстят обществу за свои проблемы, которые они из реальной жизни переносят в виртуальный мир…

Но при этом они не отдают себе отчет в том, что за эту «шалость» предусмотрена суровая уголовная ответственность – вплоть до лишения свободы на срок до 7 лет! А если «лжетеррорист» несовершеннолетний (что весьма часто и происходит), то ответ за его «шалости» придется держать родителям. Их ждет масса неприятностей, включая внушительный штраф (оплата услуг выезда экстренных служб и возмещение издержек) и постановка ребенка на профучет. Да и подросток сам себе существенно осложняет будущую жизнь в обществе: такая выходка однозначно станет для него «черной меткой» и лишит возможности поступить на обучение в понравившийся ВУЗ, выбрать будущую профессию, трудоустроиться, получить ряд социальных и общественных специализаций – это как минимум.

*Специалисты ГУПК КМ МВД предупреждают!*

1. Учащиеся: помните, что вычислить автора такого сообщения не составляет труда. Вас и ваших родителей ждет серьезная ответственность!
2. Родители: интересуйтесь, в какие онлайн-игры играет ваш ребенок, какие отношения в игровом мире поддерживает, как игра влияет на его поведение в реальном мире.

**Тема № 4. Социальные сети и мессенджеры**

Сегодня сложно найти человека, который не имел бы аккаунта в социальных сетях и не пользовался бы мессенджерами. Присутствие в виртуальном мире тоже требует определенных навыков и мер безопасности.

*Угроза №1. Кибербуллинг*

Проявление насилия в цифровом пространстве называется «кибербуллинг». Это общее определение и подразумевает под собой как травлю в виртуальном пространстве, так и причинение вреда человеку в реальном мире путем давления, шантажа, угроз, клеветы.

Природа данного явления многогранна. Источник травли, как правило, отмечается повышенной агрессивностью и в реальном мире, поэтому не стоит обесценивать его эмоции. Этому явлению способствует и кажущаяся анонимность: отсутствие визуального контакта «развязывает» язык, придает киберхулигану смелость.

Как показывают исследования, более половины интернет-пользователей становились жертвами кибербуллинга. Однако если взрослый человек более устойчив морально к таким атакам, то для подростка встреча с источником травли может иметь весьма плачевные последствия.

Как же оградить себя от киберхулиганов? Во-первых, всегда можно прекратить общение с людьми, которые причиняют боль в интернете. Во всех социальных сетях есть функция блокировки нежелательных пользователей. Просто заблокируйте агрессора, тем самым закрыв ему доступ к дальнейшим негативным действиям.

Во-вторых, следует обратиться в компетентные органы. В милицию – если источник травли переходит юридические нормы; к психологам – если мишенью выбран подросток, и так далее. Это касается как общения в виртуальном пространстве, так и копирование-цитирование запрещенной законодательством информации (к примеру, репосты сообщений интернет-сообществ, признанных экстремистскими).

В-третьих, всегда отдавайте отчет, в каких сообществах вы состоите, какую переписку и с кем ведете, насколько полно вы раскрыли собеседнику данные о себе. Чем большим объемом информации о вас владеет преследователь, тем большим влиянием на ситуацию он обладает.

*Угроза №2.*

Мошенничество в социальных сетях – очень частое и многовидовое явление. Ежегодно появляются различные мошеннические схемы, которые приходят на смену устаревшим. В большинстве случаев данной противоправной деятельностью занимаются иностранные граждане.

Самые популярные схемы:

1. Благотворительные фонды и сбор денег на лечение. В таких случаях мошенники создают группу и распространяют информацию о том, что якобы нужны средства для лечения тяжелобольного. Чтобы не попасться на удочку мошенников, стоит запросить документы и дополнительные сведения.
2. Осуществление несанкционированного доступа к аккаунту пользователя социальной сети. Доступ может быть получен различными способами: методом подбора пароля, с использованием поддельных фишинговых сайтов, вредоносного программного обеспечения, методов социальной инженерии. Получив несанкционированный доступ к аккаунту пользователя, злоумышленник заходит в учетную запись жертвы и осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера. Далее злоумышленник ждет отклика от ничего не подозревающих собеседников, а получив его, проявляет свои способности в риторике и убеждении для получения денежных средств или конфиденциальной информации жертвы.
3. Мошенничество под предлогом продажи одежды. Можно встретить различные интернет-магазины, которые предлагают приобрести одежду по заманчивой цене. Но не стоит сразу заказывать, особенно, если требуется предоплата. Полезной окажется любая собранная информация в сети Интернет в отношении данного интернет-магазина, включающая в себя отзывы покупателей, наименование юридического лица, страну его регистрации.
4. Розыгрыши и лотереи. В социальной сети часто разыгрываются различные призы, и для их получения достаточно вступить в группу и сделать репост. Если группа настоящая, тогда пользователи действительно смогут получить призы. Однако бывает, что сообщество фальшивое, либо о выигрыше в личные сообщения напишет посторонний человек. Не стоит сообщать свои личные данные, а тем более платить за доставку. Как минимум, необходимо удостовериться, что розыгрыш действительно был проведен, и вы оказались победителем. Еще лучше узнать у предыдущих призеров, получили ли они свои подарки.
5. Группы «Отдам даром». Даже на бесплатных вещах, которые якобы может получить любой желающий, мошенники наживаются. Допустим, они предлагают отдать новый телефон, который якобы им оказался не нужен. Но от пользователя потребуется оплатить доставку или страховку. Чтобы убедиться, что это действительно ваш знакомый, необходимо ему позвонить или во время переписки задать вопрос, на который мошенник гарантировано не будет знать верный ответ. После этого уже можно точно знать, кто именно просит деньги.