ПЛАН-КОНСПЕКТ

выступления в рамках проведения воспитательно-профилактической

работы с гражданами по теме:

**«Как не стать жертвой в киберпространстве»**

*СЛАЙД 1*

В настоящее время Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека.
С одной стороны, это открывает перед белорусскими гражданами и обществом ряд перспектив, с другой – влечет появление новых рисков и угроз. Так, бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений.

Вопросы цифровой трансформации преступности сегодня являются одними из наиболее злободневных. И от того, насколько эффективно удастся противостоять этому вызову, зависит не только защищенность прав и интересов граждан, но и информационная безопасность общества и государства. При этом универсальных подходов, позволяющих эффективно противодействовать высокотехнологичным преступлениям, не выработано ни одним государством мира.

*Справочно: несмотря на принимаемые меры, на протяжении последних лет в Республике Беларусь наблюдается устойчивый рост количества регистрируемых киберпреступлений: в 2015 году – 2 440 преступлений, в 2016 – 2 471, в 2017 – 3 099, в 2018 – 4 741, в 2019 – 10 539, в 2020 – 25 561.*

Среди **факторов, стимулирующих рост киберпреступлений**, можно выделить следующие.

**Опережающие темпы освоения сети Интернет в Республике Беларусь**. Так, в 2020 году доля населения нашей страны, пользующегося Интернетом, составила 85,1%; по плотности проникновения широкополосного доступа в сеть Интернет Беларусь вышла на среднеевропейские показатели, а по скорости – на передовые позиции в мире.

**Уровень компьютерной грамотности граждан недостаточно высок, отстает от скорости внедрения тех или иных компьютерных систем в повседневную жизнь**. Кроме того, многие граждане недостаточно ответственно относятся к защите и безопасности собственной информации и личных данных.

**Ускоренный переход многих сфер общественных отношений, включая товарный и денежный обороты, в интернет-пространство,** вызванный распространением коронавирусной инфекции Covid-19.

Развитие дистанционных способов совершения преступлений, при которых отсутствует прямой контакт между злоумышленниками и их жертвами, привело к тому, что киберпреступления ушли из физической реальности в онлайн-пространство.

***Что такое киберпреступность?***

***Что относится к компьютерным преступлениям?***

В настоящее время при характеристике компьютерных преступлений используется целый ряд понятий: «информационное преступление», «киберпреступление», «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий», «виртуальное преступление».

Согласно действующему законодательству Республики Беларусь,
**в содержание понятия «компьютерная преступность» включают:**

1) преступления против информационной безопасности *(модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);*

2) хищение имущества путем модификации компьютерной информации;

3) изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего;

4) иные преступления, так или иначе связанные с использованием компьютерной техники *(доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет; разглашение врачебной тайны; незаконное собирание либо распространение информации о частной жизни; клевета; оскорбление; распространение ложной информации о товарах и услугах; заведомо ложное сообщение об опасности; шпионаж; умышленное либо по неосторожности разглашение государственной тайны; умышленное разглашение служебной тайны и др.).*

Таким образом, **к компьютерным преступлениям относятся** правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

*СЛАЙД 2*

***Состояние преступности в сфере высоких технологий***

На протяжении последних лет число преступлений в сфере высоких технологий неуклонно продолжает расти. В 2020 году в Брестской области зарегистрировано 3 124 преступления (2019 - 1095, +185,3%).

В текущем году данная тенденция продолжилась. Всего в области по итогам 8 месяцев т.г. зарегистрировано 1312 высокотехнологичных преступлений (АППГ – 1032, +27,1 %).

***В чем состоит цель киберпреступников***

Как правило, киберпреступники выдают себя за людей из действующих на законных основаниях организаций и учреждений, **чтобы обманом вынудить граждан раскрыть личную информацию и предоставить преступникам деньги, товары и/или услуги**.

Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные, имущество и денежные средства граждан.

**Виды киберпреступлений в отношении граждан**

Наиболее распространенным видом проявления киберпреступности является **хищение денежных средств с карт-счетов граждан**. Причем в большинстве случаев эти преступления становятся возможны в результате беспечных действий самих потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих способов:

***Фишинг*** *- неофициальный термин происходит от английского «fishing» («рыбная ловля»). В качестве своеобразной «удочки» преступники используют специально созданный интернет-сайт с формой ввода на нем реквизитов доступа к банковскому счету, а в качестве «наживки» – некий сообщенный потерпевшему предлог для перехода на этот сайт и заполнения платежных реквизитов.*

*СЛАЙД 3*

Например, преступник отслеживает на интернет-сайте kufar.by свежие объявления о продаже чего-либо. Просмотрев абонентский номер автора объявления, находит его в одном из мессенджеров *(Viber, Telegram, WhatsApp)* и вступает в переписку, якобы желая купить выставленный на продажу предмет. Затем пересылает в мессенджере ссылку на поддельную страницу предоплаты, где продавцу нужно ввести реквизиты своей карты для того, чтобы получить деньги от покупателя. При переходе по гиперссылке невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных сервисов *(Куфар, ЕРИП, CDEK, Белпочта, сайты различных банков и др.).* Адрес поддельной веб-страницы также может напоминать реальный *(kufar-dostavka.by, erip-online.com, belarusbank24.xyz, cdek-zakaz.info и др.).* Если жертва «попадется на удочку» и заполнит форму, соответствующие реквизиты доступа к банковскому счету окажутся у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета или электронные кошельки, зарегистрированные на подставных лиц.

*Справочно: наиболее часто для совершения такого вида киберпреступлений в Беларуси в 2020 году использовалась интернет-площадка «Kufar».*

Гиперссылки на фишинговые сайты могут пересылаться не только в ходе переписки в мессенджерах, но и при общении в социальных сетях, а также размещаться на других сайтах, якобы что-то продающих или покупающих.

*СЛАЙД 4*

**В последнее время участились случаи создания фишинговых сайтов, ориентированных под запросы пользователей в поисковых системах**. Граждане попадают на них прямо из Google и Яндекса после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет банкинг» и т.д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска, но не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения, потерпевший заполняет открывшуюся форму авторизации, данные которой отправляются не банку, а преступнику.

Таковых в прошедшем году совершено 455 (44,1% всех высокотехнологичных преступлений). По состоянию на 01.09.2021 года в области уже совершено 542 преступления данной категории (41,3% всех преступлений по линии СВТ, зарегистрированных в 2021 году).

*Пример преступления, совершенных с использованием методики «фишинга»:*

***22 июня т.г.*** *возбужденно уголовное дело по заявлению жительницы
г. Пинска, 1982 г.р., в котором она просит установить и привлечь к уголовной ответственности неизвестное лицо, которое 15 июня т.г. примерно в 11.00 часов в ходе переписки в мессенджере «Viber» под предлогом покупки товара склонило ее к передаче реквизитов банковской карточки ОАО «СБ Беларусбанк», зарегистрированной на ее имя, после чего в результате несанкционированного доступа к компьютерной информации похитило денежные средства в сумме 1 949 рублей, причинив материальный ущерб.*

*В ходе проверки было установлено, что 15.06.2021 примерно в 11.00 часов гражданка на торговой интернет-площадке «Куфар» разместила объявление о продаже туфлей. После размещения объявления ей на мобильный телефон в мессенджере «Viber» пришло сообщение от неизвестного пользователя с целью покупки данного товара.*

*В последующем неизвестное лицо прислало потерпевшей ссылку «https://evropochta.pay-get.by», пояснив, что последней необходимо ввести реквизиты своей банковской платежной карты, для последующего перевода на данную карту денежных средств за товар.*

*Далее гражданка перешла по вышеуказанной ссылке и ввела реквизиты своей банковской карточки, а также коды, которые пришли ей на телефон, после чего были списаны денежные средства в сумме 1 949 рублей.*

**Наиболее оптимальным способом обезопасить себя будет открытие дополнительной банковской карты, которая будет предназначена лишь для совершения оплат в сети Интернет, и на которой не будут храниться денежные средства.**

*СЛАЙД 5*

**Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует**:

- вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);

- ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);

- очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;

- уточнить у собеседника номер телефона, если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);

- избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить доменное имя (адрес ресурса). Сделать это можно отыскав в интернете официальный сайт и сверив написание доменного имени. Отличие в одну букву или символ свидетельствует о том, что перед Вами ссылка на поддельный ресурс.

С 2020 года по настоящее время на территории Брестской области наблюдается всплеск активности преступлений, совершенных путем завладения реквизитами банковских карт в ходе телефонных разговоров под видом сотрудника банка - «вишинг».

***Вишинг*** *(англ. vishing, от voice phishing) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т.д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом/платежной картой.*

В 2020 году с использованием методики «вишинга» злоумышленниками был совершено 530 (51,4% всех высокотехнологичных преступлений). По состоянию на 01.09.2021 года уже совершено 707 преступлений данной категории (53,9% от всех зарегистрированных по линии СВТ в 2021 году).

Злоумышленники, представляясь представителями банковских учреждений, осуществляют звонки на мобильные телефоны граждан и под видом представителя банковского учреждения Республики Беларусь пытаются завладеть реквизитами их банковских платежных карт и иными конфиденциальными данными. В процессе общения указанные лица сообщают, что необходимо срочно осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. В 2020 году для осуществления подобных звонков преступники зачастую использовали современные возможности сети Интернет, в частности возможность «подмены номера».

*СЛАЙД 6*

**Суть «вишинга» заключается в том**, что у потерпевшего на экране мобильного телефона отображается совершенно любой абонентский номер телефона, заданный злоумышленником, обычно это номер какого-либо банковского учреждения и сам звонок по своим внешним признакам не является подозрительным. В настоящее время для общения с гражданами преступники преимущественно используют различные интернет-мессенджеры, в частности «Viber», где в качестве имени пользователя (никнейма) они указывают официальный номер банка либо его название, в качестве «аватарки» используют логотип или эмблему банковского учреждения.

Следует отметить, что зачастую злоумышленники владеют какой-либо минимальной информацией о гражданах (имя, отчество, дата рождения, последние цифры банковской карты и др.), это способствует повышению доверия к звонящему и производит на него определенное впечатление. В дальнейшем злоумышленник просит сообщить информацию о банковской карте (ее номер, срок действия, CVV-код, содержание СМС-сообщения, которое в ходе разговора поступает на мобильный телефон). Получив интересующую информацию, он совершает хищение денежных средств. Существуют различные способы хищения денежных средств – путем перевода на иную банковскую карты, находящуюся в пользовании злоумышленника, электронные кошельки различных платежных систем, открытие онлайн-кредита и др.

*В качестве примера изобретательности преступников можно привести следующие:*

***22 января т.г.*** *в УВД Брестского облисполкома поступило обращение жительницы г. Бреста по факту поступившего телефонного звонка от неустановленного лица с просьбой предоставления реквизитов банковской платежной карты. В ходе первоначальной проверки установлено, что 21.01.2021 в 12:09 часов на абонентский номер заявительницы в интернет мессенджере «Viber» поступил телефонный звонок от неизвестного ей ранее лица в никнейме которого был указан абонентский номер 375173375750 Звонивший мужчина представился сотрудником ОАО «БПС-Сбербанк» и настойчиво потребовал пригласить к телефону сына заявительницы 1982 г.р. Заявительница передала телефон своему сыну, которому неизвестный сообщил, что с находящейся у него банковской платежной карты происходит списание денежных средств и попросил предоставить персональные данные, чтобы заморозить транзакцию, на что последний ответил отказом, упомянув что не пользуется услугами ОАО «БПС-Сбербанк», а использует банковскую карту ОАО «Приорбанк» и положил трубку. Через несколько минут с указанного выше абонентского номера поступил повторный звонок. Звонивший мужчина представился сотрудником ОАО «Приорбанк», повторно сообщил, что с находящейся у него банковской платежной карты происходит списание денежных средств и вновь попросил предоставить персональные данные и реквизиты находящейся в пользовании последнего банковской карты, на что вновь получил отказ. После указанного разговора на абонентский номер заявительницы в интернет мессенджере «Viber» поступил звонок с абонентского номера 37067876341 (указанный никнейм пользователя: «102»). Звонивший мужчина представился сотрудником ОВД Ленинского района г.Бреста майором милиции Соколовым Никитой Владимировичем и сообщил, что вышеуказанные звонки были осуществлены действительно от сотрудников банковских учреждений и попросил предоставить персональные данные ее сына, на что также получил отказ. Сразу же после окончания разговора с указанного выше номера поступил повторный звонок. Звонившая женщина представилась заведующей отделом финансов Московского района Никитиной Светланой и повторила просьбу о предоставлении ранее запрашиваемой информации, на что также получила отказ.*

***04 июня т.г.*** *возбужденно уголовное дело по заявлению жителя г. Пинска, в котором он просит установить и привлечь к уголовной ответственности неизвестное лицо, которое 24 мая т.г. примерно в 13.44 часов в ходе телефонного разговора в мессенджере «Viber» от имени сотрудника службы безопасности ОАО «Приорбанк», склонило потерпевшего к оформлению кредита и переводе всех денежных средств на принадлежащую ему банковскую карту, с которой затем похитило их, причинив материальный ущерб на сумму 9 700 рублей.*

*В ходе проверки было установлено, что 24.05.2021 примерно в 13.44 часов потерпевшему в мессенджере «Viber» поступил входящий звонок с номера 37124956577, в ходе разговора неизвестный мужчина представился сотрудником службы безопасности ОАО «Приорбанк» и сообщил, что с банковской карты последнего пытаются похитить денежные средства. В ходе дальнейшего телефонного разговора по указаниям неустановленного лица пинчанин установил на свой мобильный телефон приложение «AnyDesk», посредством чего данное лицо получило удаленный доступ к мобильному телефону, в т.ч. к приложению банкинга и карт-счету, и совершило попытку хищения денежных средств в сумме около 200 рублей с банковской платёжной карты, после чего звонок прервался. Далее на мобильный телефон потерпевшего в мессенджере «Viber» поступил ещё один звонок, в ходе которого неустановленное лицо представилось сотрудником милиции и под предлогом разоблачения работников банка, которые якобы совершают хищения денежных средств с банковских счетов граждан, убедило пинчанина оформить кредит в ЗАО «Альфа-Банк». Последний в отделении данного банка оформил на свое имя кредит на сумму 9 700 рублей НБ РБ и перевел данные денежные средства на банковский счет ЗАО «Банк БелВЭБ», оформленный неустановленным лицом на имя заявителя с использованием его персональных данных. С указанного банковского счета денежные средства последнего были похищены.*

С целью предотвращения совершения преступлений указанной категории на территории области, сотрудниками ОВД во взаимодействии с иными правоохранительными органами, учреждениями образования, СМИ, трудовыми коллективами и иными заинтересованными проводится определенная профилактическая работа. К сожалению, следует констатировать факт, что имеются граждане, которые знали о подобного рода мошенничествах, вместе с тем попали на уловку так называемых «лжесотрудников» банков.

**Запомните! Сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен**.

*СЛАЙД 7*

Если Вам поступил такой звонок, **следует помнить**:

- **ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Запомните, банк никогда не станет звонить своим клиентам посредством интернет-мессенджеров!** Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме. В случае если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и Банк это заметит, то его сотрудники сперва инициативно заблокируют Вашу банковскую платежную карту, после чего сообщат Вам причину принятого решения (ничего не уточняя) и пригласят в свое учреждения с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;

- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы. Скорее всего, собеседник сообщит, что Вам вообще не звонил. Современные технологии позволяют подменить номер на экране Вашего телефона на совершенно любой, в том числе заменить его для примера названием учреждения банка;

- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения. Даже в этом случае не сообщайте никакой информации собеседнику;

- сами перезвоните в свой банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся. Скорее всего, специалист сообщит Вам, что никаких несанкционированных операций зафиксировано не было, а сотрудник Банка Вам не звонил.

Если же Вы сообщили кому-либо информацию о своей банковской платежной карте, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта.

Помните, что если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства (онлайн-кредит).

*В качестве примера преступлений, совершенных с использованием методики «вишинга» можно привести следующие:*

***31 мая т.г.*** *возбуждено уголовное дело по заявлению жительницы г. Кобрина, 1978 г.р., по факту хищения с принадлежащей ей банковской платёжной карты ОАО «Банк БелВЭБ» денежных средств.*

*Установлено, что с 2006 года в ОАО «Банк БелВЭБ» у нее открыт счет, к которому эмитирована банковская платежная карта. 27.05.2021 в 12 часов 29 минут гражданке посредством мессенджера «Viber» позвонил неизвестный мужчина, который представился сотрудником техслужбы ОАО «Банк БелВЭБ», а также сообщил ей, что в банк посредством Интернет-банкинга поступил запрос на оформление потребительского кредита на её имя, а также сказал, что участились случаи мошенничеств подобным способом, поэтому они перепроверяют информацию. Женщина сообщила данному лицу, что не оформляла никаких кредитов. Мужчина говорил убедительно, назвал ее имя, отчество и последние 4 цифры ее банковской карты. Потерпевшая спросила у мужчины, почему он звонит в «Viber», на что он ответил, что банк может связываться с клиентом любым способом. Потом она попыталась закончить разговор и сказала, что обратится в отделение банка. Мужчина пояснил, что кредит оформляется в настоящее время и, если его не прервать сейчас, то денежные средства будут похищены. Гражданка поверила данному мужчине.*

*В последующем он переключил ее якобы на службу безопасности банка и с ней стал разговаривать другой мужчина. Данный мужчина назвал дату ее рождения, часть идентификационного номера до первой буквы, дату выдачи паспорта, дату ее последней транзакции и последнюю операцию в Интернет-банкинге. Далее в ходе общения с мужчиной она назвала ему остаток своего идентификационного номера. Данному мужчине реквизиты своей банковской карты она не сообщала. В ходе общения на телефон стали поступать коды, которые она ему сообщила. Коды ей приходили из ОАО «Банк БелВЭБ». После этого потерпевшая поняла, что делает что-то не так и прервала разговор. Мужчина продолжал ей перезванивать в мессенджер, но она позвонила в информационный центр банка, сообщила о случившемся и заблокировала карту. Далее пошла в отделение ОАО «Банк БелВЭБ» в г.Кобрине, где ей сообщили, что на её имя открыт онлайн-кредит на сумму 9800 рублей НБ РБ, а также, что все денежные средства, в том числе которые находились на банковском счете до получения кредита, похищены.*

***15 июня т.г.*** *возбужденно уголовное дело по заявлению жительницы г.Бреста Н., 1981 г.р., о том, что с находящейся в её пользовании банковской платёжной карты ЗАО «МТБанк» неустановленным лицом путем несанкционированного доступа похищены денежные средства на сумму 8 260 рублей НБ Республики Беларусь.*

*В ходе проведения проверки установлено, что 10 июня т.г. ей посредством мессенджера «Viber» поступил аудиозвонок, в ходе которого неизвестный мужчина, представился оперуполномоченным по борьбе с экономическими преступлениями Фроловым Павлом и предупредил, что их разговор записывается и он должен быть конфиденциальным. В ходе разговора последний сообщил, что 10 июня т.г. неустановленными лицами на ее имя в ЗАО «МТБанк» был оформлен кредит на сумму 9000 рублей, а также то, что с целью установления данных лиц, необходимо направиться в отделение данного банка расположенное по адресу: г. Брест, ул. Советская, д.54, и оформить на своё имя кредитный договор на максимально возможную сумму. Гражданка направилась в указанное отделение банка, где оформила на своё имя кредит на сумму 8 260 рублей. Денежные средства по данному кредитному договору были зачислены на карту, выданную последней к кредитному счёту. Реквизиты данной карты последняя предоставила ранее звонившему мужчине в ходе осуществления очередного аудиозвонка. В ходе разговора мужчина уточнил у потерпевшей, у какого сотрудника она заключала кредитный договор и как он выглядел. После этого звонивший попросил направиться в ОАО «РРБанк» и ОАО «Идея Банк» и также взять кредиты на максимально возможные суммы и максимально большие сроки, однако в указанных банках в кредитовании было отказано.*

*Ближе к вечеру гражданка осознала, что с ней общались мошенники, после чего она позвонила в ЗАО «МТБанк», сотрудники которого ей сообщили об отсутствии денежных средств на её кредитном счёте и заблокировали её карту. Впоследствии с заявлением о данном факте гражданка обратилась в Московское РУВД г. Бреста.*

***Иные способы совершения преступлений***

***Свободный доступ к банковской карте*.**

Не всегда для хищения с банковских счетов используются хитрые схемы. В ряде случаев причинами этого становятся утеря банковских карт, оставление их в легкодоступном месте, их передача иным лицам для осуществления разовых платежей. При этом увеличивает риск остаться без заработанных денежных средств хранение PIN-кода рядом с картой *(например, записанным на бумажке в кошельке или на самой банковской карте).*

Разновидностью подобного легкомыслия является хранение фотоизображений банковских карт или платежных реквизитов в памяти мобильного телефона, в почтовом аккаунте или дистанционном облачном хранилище. При несанкционированном доступе к такому хранилищу преступник получает и беспрепятственный доступ к банковскому счету его владельца.

***Покупка с предоплатой*.**

Наиболее примитивной, но от этого не менее работающей формой интернет-мошенничества является размещение преступниками на виртуальных досках объявлений, тематических сайтах, в социальных сетях, группах интернет-мессенджеров объявлений о продаже каких-либо товаров по «бросовым» ценам. Но для получения товара (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту или электронный кошелек. Правда, после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

***Шантаж*.**

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. Например, получив несанкционированный доступ к Интернет-ресурсам *(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 сети Интернет.

***Иные мошенничества*.**

Также можно выделить еще несколько типов мошенничества, которые в недавнем прошлом зачастую успешно использовались на территории Республики Беларусь:

* Просьбы пополнить счет определенного номера мобильного телефона или платежной карты в виде: «Мама, пополни счет на 20 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!».
* Звонок с номера друга или родственника, в котором собеседник утверждает, что он сотрудник правоохранительных органов, просит вознаграждение, обещая предотвратить возбуждение уголовного дела в отношении близкого человека.
* Когда мошенник звонит и сразу отменяет вызов. Перезвонив на отобразившийся номер, абонент слышит автоответчик или гудки, в это время со счета его мобильного телефона списываются деньги, так как вызов совершается с применением переадресации на платный номер.
* Когда приходит SMS-сообщение о некоем выигрыше, после чего абоненту предлагают отправить платное сообщение в ответ или отправить небольшую сумму на банковскую карту для получения «лжевыигрыша».
* Когда приходит SMS-сообщение с гиперссылкой, пройдя по которой пользователь запускает процесс скачивания вируса.
* Когда поступает звонок от «представителя сотового оператора», во время которого злоумышленники предлагают перерегистрировать SIM-карту. При этом пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного телефона списываются деньги.
* Когда приходит SMS-сообщение или поступает звонок, в ходе которого сообщается, что абонент не оплатил штраф. После этого человеку предлагается произвести его оплату, перечислив деньги на «специальный» расчетный счет или пополнив банковский счет.
* Когда приходит SMS-сообщение с информацией о том, что платежная карта заблокирована, и указывается номер, по которому можно получить справку или помощь. После звонка у абонента запрашивают PIN-код, CVV-код (трехзначный код на обратной стороне карты), номер карты и другие данные, необходимые для снятия денег с банковского счета.

***Как не стать жертвой киберпреступления***

1. **Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт**, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

**ВНИМАНИЕ:** *помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp)*.

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, **обязательно проверяя доменное имя ресурса в адресной строке браузера**.

3. **Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам**; это же относится к фотографиям и иным видам информации конфиденциального характера.

4. Следует **воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги**, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

5. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт **по просьбе пользователей сети Интернет**.

6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам **необходимо использовать сложные пароли, исключающие возможность их подбора**. Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).

7. При составлении платежных документов **важно проверять платежные реквизиты получателя денежных средств**.

8. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек **не следует отвечать на подобные сообщения, а необходимо связаться с данными пользователями напрямую посредством иных средств связи**.

9. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать обэтом факте лиц, с которыми общались посредством данных социальных сетей.

10. **Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров**; не переходить по ссылкам в сообщениях о призах и выигрышах.

11. Необходимо **использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу** не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

12. Следует **ознакомить с перечисленными правилами безопасности своих родственников и знакомых**, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.