**Рекомендации по безопасности в цифровом пространстве**

Рассмотрим основные уловки кибермошенников, а также рекомендации по противодействию последним:

1. **Клонирование SIM-карты.**

Информация с SIM-карты оператора сотовой подвижной электросвязи, которая попала в руки злоумышленника, может быть скопирована (клонирована) в память компьютера, а потом перенесена на «чистую» SIM-карту. После чего она может быть вывезена за границу и активирована в режиме роуминга. Однако счета за оказанные услуги связи будут выставлены владельцу, на которого она зарегистрирована.

Для защиты от подобного вида мошенничества никогда не следует передавать свою SIM-карту третьим лицам, особенно незнакомым. При сдаче телефона или другого устройства связи в ремонт необходимо извлечь SIM-карту.

В случае утери (кражи) телефона (SIM-карты) необходимо незамедлительно обратиться к своему оператору сотовой связи для оказания услуг по ее блокировке. Особенно следует придерживаться данных рекомендаций в случае утери телефона за границей во избежание начисления задолженности на большую сумму (при использовании телефона злоумышленниками), которую придется внести по возвращении в Республику Беларусь. Стоит учитывать и тот факт, что счета за пользование мобильной связью в режиме роуминга выставляются оператором пользователям не сразу, а по прошествии достаточного количества времени.

1. **Просьба о помощи.**

Достаточно распространенный вид мошенничества. Абоненту приходит SMS с просьбой о помощи. Вариантов таких сообщений достаточно много, но суть у них одна. Например: «Мама (папа, сестра, брат и т.д.), пишу с чужого номера. На моем телефоне закончились деньги. Срочно положи столько-то рублей на номер…» Могут приходить сообщения о «попадании в аварию», «неприятности с контролерами в общественном транспорте» и т.д.

Для защиты от такого вида мошенничества всегда необходимо уточнить у родных, друзей, знакомых полученную информацию.

При желании перезвонить на номер, с которого пришло подобное SMS, стоит обратить на него внимание. Так как это может быть короткий номер или номер иностранного оператора.

1. **Ошибочный платеж («Верните деньги!»).**

Существует несколько схем такого мошенничества, рассмотрим их подробнее.

SMS может приходить как от оператора сотовой связи (злоумышленник на самом деле пополнил баланс мобильного телефона пользователя), так и с произвольного номера, повторяя «оригинальное» сообщение оператора. Причем в первом случае деньги, как правило, зачисляются на счет абонента, а во втором – нет.

Далее на мобильный номер абонента может поступить звонок с просьбой о возврате денежных средств на определенный номер злоумышленника за ошибочно произведенный платеж. Абонент, подтвердив свое согласие о возврате денежных средств, переводит указанную «ошибочную» сумму на мобильный номер злоумышленника. В первом случае злоумышленник обращается с заявлением к сотовому оператору и повторно переводит со счета абонента-жертвы сумму «ошибочного» платежа. Второй вариант развития событий предполагает, что деньги на счет абонента фактически не поступают, а абонент делится со злоумышленником своими деньгами.

В целях защиты от такого вида мошенничества необходимо помнить, что у всех операторов существует отработанная процедура возврата ошибочно уплаченных средств для пополнения баланса чужого абонентского номера.

В случае возникновения подобной ситуации не стоит переводить денежные средства на незнакомый абонентский номер, а рекомендуется посоветовать звонящему обратиться к оператору сотовой связи в целях урегулирования данного вопроса.

1. **Входящие звонки с неизвестных иностранных номеров.**

Данный вид мошенничества также основывается на невнимательности абонента.

Например, глубокой ночью абоненту поступает входящий звонок из-за границы, который буквально сразу сбрасывается, а абонент не успевает на него ответить. Абонент, находясь в сонном состоянии, перезванивает на неотвеченный неизвестный иностранный номер, а после установления соединения либо ничего не слышит, либо у него включается автоответчик. При этом со счета абонента списываются денежные средства.

Для защиты от данного вида мошенничества абоненту необходимо проверять номер мобильного оператора, на который он собирается сделать звонок, и без необходимости не перезванивать на незнакомые иностранные номера.

1. **Странные номера входящих вызовов и SMS.**

Этот вид мошенничества предполагает деятельность злоумышленников, связанную с незаконной терминацией (оригинацией) голосового трафика в обход надлежащих коммутационных узлов операторов электросвязи, уполномоченных на пропуск международного и (или) межсетевого трафика, и (или) использованием услуги IP-телефонии в нарушение установленного законодательством порядка.

Подобная деятельность влечет негативные экономические последствия как для операторов электросвязи, уполномоченных на пропуск международного и (или) межсетевого трафика, а также на оказание услуг телефонии по IP-протоколу в пределах действия сетей электросвязи Республики Беларусь, так и для абонента, с лицевого счета которого в случае осуществления звонка на подобные номера будут списаны средства как за исходящий вызов.

В целях осуществления противодействия такому виду мошенничества абонент может обратиться к своему оператору сотовой связи и сообщить о подобном факте. Оператор электросвязи, совершив необходимые действия, сможет пресечь на стороне своей сети незаконную деятельность третьих лиц.

1. **Звонки со стороны «службы поддержки» сотового оператора.**

Злоумышленники представляются сотрудниками технической поддержки оператора и под различными предлогами (несвоевременная оплата счета, технические проблемы, случайная блокировка абонентского номера технической службой, сбой в работе оборудования, перевод оборудования оператора для работы с другими голосовыми кодеками и т.д.) предлагают абоненту либо перевести деньги на указанный ими номер, либо оплатить штраф, либо перезвонить на короткий номер для решения возникшей проблемы или на номер телефона, на котором будет включен автоответчик с «рекомендацией», какие действия предпринять абоненту в дальнейшем.

Чтобы исключить данной вид мошенничества, необходимо помнить, что операторы сотовой связи всегда приглашают абонента в фирменный центр продаж своих услуг в целях решения всех возникших проблемных вопросов.

1. **Выигрыш приза.**

На телефон абонента поступает звонок (также возможно получение SMS). При этом звонящий представляется сотрудником известной радиостанции, банка, телеканала или туристической фирмы и поздравляет абонента с выигрышем ценного приза, туристической поездки и т.д.

Для получения приза абоненту предлагается в течение ближайших минут перезвонить на короткий номер указанной компании, где абонента в очередной раз поздравят с выигрышем ценного приза и предложат оплатить, например, налог на выигрыш, перечислив денежные средства на электронный кошелек или предоставив в течение часа сотруднику компании данные карты экспресс-оплаты за услуги связи на определенную сумму.

После этого обманутый абонент приезжает за призом в офис известной компании и узнает, что никакого розыгрыша не проводилось.

Чтобы не стать жертвой такого мошенничества, не стоит спешить перезванивать на короткие номера и отправлять денежные суммы на электронные кошельки различных платежных систем. Самый верный способ – обратиться в офис названной компании, телеканала, радиостанции, банка или туристической фирмы и на месте уточнить у сотрудников все вопросы, связанные с возможным выигрышем. Не стоит забывать, что, как правило, компании всегда освещают в средствах массовой информации ход и результаты проведения различного рода розыгрышей и акций.

1. **Звонки со стороны «банковских структур и организаций».**

Всегда стоит помнить, что настоящий технический специалист или сотрудник банка никогда, ни в каких случаях не будет запрашивать у клиента конфиденциальную информацию, касающуюся реквизитов банковской карты, а также персональные данные из паспорта и т.д.

В случае возникновения подозрения, что с вами разговаривает злоумышленник, необходимо прекратить разговор, а для уточнения вопросов, возникших с вашей банковской картой или банковским счетом, самостоятельно перезвонить по номеру горячей линии банка, указанного на его официальном интернет-сайте.

Также не следует перезванивать на тот номер телефона, с которого вам звонили злоумышленники. Так как он с высокой степенью вероятности будет изначально подменен или вы сами можете дозвониться до злоумышленников, которые затем продолжат разыгрывать свой «спектакль».

Стоит в том числе иметь в виду, что в настоящее время существуют технологии, позволяющие злоумышленникам заблокировать телефонную линию жертвы и перенаправлять все последующие ее звонки на мошенников.

В данном случае, если у вас имеются достаточные подозрения, то для связи с банком воспользуйтесь, к примеру, стационарным телефоном.

Запомните, ни в коем случае не сообщайте злоумышленникам реквизиты вашей банковской карты и не осуществляйте перевод средств на другие счета, которые предложены звонящим злоумышленником.»

1. **К вам пришла SMS с просьбой перейти по указанной ссылке для разблокирования вашей электронной почты, аккаунта в соцсети и т.д.**

SMS-рассылка в настоящее время стала очень популярным инструментом для продвижения своих товаров, работ и услуг, а также информирования клиентов о новых акциях и т.д.

К SMS, которые содержат ссылку, следует относиться с настороженностью. Учитывая, что объем SMS ограничен, многие компании используют сервисы по сокращению ссылок и понять, на какой интернет-ресурс ведет конкретная ссылка, не представляется возможным.

Этим и пользуются злоумышленники, перенаправляя при помощи таких SMS, содержащих сокращенные ссылки, на свои ресурсы, где обычно на визуально схожей с оригинальной страницей интернет-ресурса злоумышленники предлагают, к примеру, ввести свой логин и пароль или иные данные, которые затем получают злоумышленники для доступа к вашему личному кабинету, странице соцсети и т.д.

Кроме того, переход по ссылке может означать автоматический акцепт предлагаемой услуги.

Перед переходом по ссылке, присланной в SMS, всегда следует еще раз перепроверить информацию, позвонив на горячую линию сервиса или зайдя на их интернет-ресурс.

***Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные или совершить какие-либо действия по указанию мошенника. Ведь Ваша безопасность, в первую очередь, в Ваших руках!***

ПАМЯТКА

**«Как не стать жертвой при осуществлении финансовых**

**операций в сети Интернет»**

Что сегодня может быть проще, чем купить в интернете понравившийся товар? Совершить такую покупку может даже ребенок или пользователь, не вполне уверенно владеющий навыками работы с персональным компьютером. Этот процесс обусловлен тем, что большинство людей сегодня все чаще испытывает дефицит свободного времени и тратить его на походы по магазинам, особенно в поисках обычных товаров, стало для многих недоступной роскошью. Кроме этого, купить или продать товар в сети Интернет стало очень просто благодаря огромному числу торговых площадок, которые делают этот процесс максимально быстрым и удобным, предоставляя возможность оплаты с использованием банковских платежных карт и доставки товара в любой уголок мира.

**Наиболее распространены способы совершения преступлений**

1. **«Предоплата» (обман продавца)**

Суть данного способа заключается в том, что злоумышленник выступает в роли покупателя. На одной из интернет-площадок с объявлениями он находит продавца и копирует его контактные данные. После чего ищет его в мессенджерах (социальных сетях), представляясь покупателем. В ходе переписки, злоумышленник сообщает, что товар ему понравился и он хочет его приобрести в связи с чем уже якобы совершил предоплату (зачастую высылается скриншот электронного карт-чека о перечислении средств). Для того, чтобы получить данные средства продавцу высылают ссылку на поддельную страницу (она выглядит как один из разделов официального сайта интернет-площадки или банковского учреждения), где продавцу нужно ввести номер своей карты, имя держателя, срок действия, CVV-код указанный на оборотной стороне карты (информацию, содержащуюся в СМС-сообщении, поступившем из банка, для подтверждения получения предоплаты). После получения конфиденциальных сведений, злоумышленник совершает хищение средств.

1. **«Доставка» (обман покупателя)**

Злоумышленник размещает объявление на интернет-площадке о продаже товара по крайне выгодной цене. После того, как потенциальный покупатель начинает вести переписку во внутреннем чате площадки, злоумышленник под различными предлогами убеждает его продолжить общение в мессенджере или социальной сети. Во время общения мошенник уговаривает покупателя внести предоплату или оформить доставку, и чтобы развеять сомнения покупателя, сообщает о якобы новой услуге удержания (холдирования) средств, которая появилась на торговой площадке, т.е., если доставка не произойдет, то торговая площадка автоматически вернет средства на карту. При этом покупателю высылается ссылка на поддельную страницу, которая имитирует официальную страницу торговой площадки или интернет-банкинга, где нужно ввести данные карты (далее осуществляются действия по схеме обмана продавца).

1. **Использование социальных сетей**

Осуществив несанкционированный доступ к персональным аккаунтам пользователя сети Интернет, злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты, при этом, хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу» очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон).

1. **Звонок от «представителя» банка с просьбой срочно предоставить необходимую информацию**

Преступники от имени сотрудников банка сообщают, что необходимо 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. Для маскировки преступники используют функцию «подмены номера», как следствие у потерпевшего на экране мобильного телефона может отображаться совершенно любой абонентский номер телефона, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным. Получив необходимую информацию о реквизитах карты, преступники осуществляют хищение.

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

-        вести общение с покупателями (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);

-        использовать отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;

-        избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки.

-        если Вы все же перешли по подобной ссылке и видите уведомление о том, что в системе имеется денежный перевод и для его получения необходимо ввести данные банковской платежной карты, ни при каких обстоятельствах не вводите запрашиваемые сведения, так как это прямой путь к утрате собственных средств.

-        если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо в срочном порядке произвести блокировку карты, позвонив в банк либо самостоятельно в интернет-банкинге.

-    если Вам поступил звонок из «банка» ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. 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.

-    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.

-    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.

**Как не попасться на уловки мошенников**

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя ваши эмоции.

С клиентом банка посредством телефонного звонка или в социальных сетях связывается мошенник под видом представителя банка или с аккаунта друга, родственника. В ходе звонка или переписки собеседник описывает свою сложную жизненную ситуацию и просит ему материально помочь или «запугивает» ложной информацией о сомнительных операциях с банковской карточкой (наличии заявки на кредит, блокировке счета, мошеннических атаках и др.), представляясь работником банка, и предлагает для сохранения оставшихся денежных средств перевести их на новый счет. Собеседник говорит очень убедительно и, как правило, торопит развивающиеся события.

Сценарии могут быть разными, а итог один: клиент самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли. Поэтому такие случаи не относятся к принципу «нулевой ответственности» банка, так как конфиденциальные данные злоумышленнику сообщили вы сами.

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в банк по номеру, указанному на Вашей банковской карте, официальном сайте либо прийти в офис лично.

Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!

Вот несколько простых советов, соблюдение которых, позволит не стать жертвой злоумышленников:

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (задайте другу вопрос, ответ на который знаете только вы оба);
2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по номерам, указанным на вашей банковской карте либо официальном сайте финансового учреждения;
3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от Банка – это повод уточнить ее достоверность и перезвонить в Банк по официальным номерам;
4. Работники банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему Интернет-банкинга. В такой ситуации немедленно прервите разговор и свяжитесь с Банком по официальным номерам.
5. Никому не сообщайте данные своей карточки и всегда держите её в поле зрения при совершении платежей;
6. Обязательно подключите 3D-secure и смс-оповещение;
7. Используйте только официальный сайт для входа в систему Интернет-банкинга или официальное мобильное приложение соответствующего банковского учреждения;
8. Регулярно обновляйте пароли, используемые для входа в систему Интернет-банкинга, а также для подтверждения платежей;
9. В случае выявления действий по карточке, которые не совершались ее держателем, необходимо оперативно обратится в Банк по официальным номерам или заблокировать карточку самостоятельно в Интернет/М-банкинге (при наличии такой возможности).

**Что бы обезопасить себя и повысить уровень цифровой грамотности, рассмотрим самые распространенные на текущий момент схемы мошенничества:**

1. **«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber, WhatsApp и Telegram. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка. У мошенников есть возможность звонить с номеров, похожих (реже – полностью совпадающих) на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (зачастую сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVС-код). Это нужно якобы «для сохранности ваших денег».

**Как мошенник пытается вас убедить:**

* «*Мы звоним с официального номера, проверьте на сайте».*
* *«В целях конфиденциальности я включаю робота, который защитит ваши данные»*.
* Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
* Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
* Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

***Важно! Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!***

Еще один из способов получить доступ к Вашим денежным средствам, используя методы социальной инженерии, побудить клиентов банковских учреждений установить сторонние мобильные приложения для удаленного доступа в мобильное устройство потенциальной жертвы. Для примера, одним из таких приложений является “AnyDesk - удаленное управление” из сервисов Google Play/App Store.

Звонки осуществляются, как правило, на мобильные телефоны из указанных выше мессенджеров. При этом мошенники представляются сотрудниками банка, сообщают о якобы зафиксированных попытках совершения подозрительных операций на внушительные суммы, предлагают подтвердить их легитимность. В ходе разговора, с целью скорейшего вхождения в доверие, опрашивают клиента, задавая вопросы общего характера: «Передавалась ли БПК третьим лицам», «Доставляются ли СМС-оповещения» и т.п. Сообщают о блокировке сомнительных операций и счета клиента. Для повышения степени защищенности Интернет-банкинга и восстановления доступа к счету клиенту настоятельно рекомендуют установить приложение «AnyDesk - удаленное управление» из сервисов Google Play/App Store. В случае согласия пострадавшего, конечно же, оказывают помощь и консультацию в установке. Установленное приложение позволяет злоумышленникам получить удалённый доступ к вашему устройству.

1. **«Потенциальный покупатель»**

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети Интернет. По каким-то причинам «покупатель» не может сегодня привезти или перечислить деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

**Важно! Не переходите по подозрительным ссылкам.** Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в Интернете путем обычного поиска.

**Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.**

1. **«Сообщения в социальных сетях»**

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

1. **«Розыгрыши/раздачи/опросы от Банка или иных организаций»**

Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» либо для зачисления денежных средств в честь юбилейной даты со дня образования того или иного финансового учреждения. Цель опроса — изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение. Однако, по окончанию опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения или ввести персональные данные Вашей карты для зачисления на нее денежных средств.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

**Важно! Посетите официальную страницу организации, а не ресурс, ссылку на который прислал мошенник или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.**

1. **«Фишинг и новшества в различных платежах»**

Дополнительно хотим рассказать о новой мошеннической схеме, которая в текущее время широко распространена на территории Российской Федерации и, к сожалению, может быть актуальна для граждан Республики Беларусь.

Злоумышленниками по электронной почте рассылаются фальшивые уведомления об оплате долгов за жилищно-коммунальные услуги, которые возникли за время самоизоляции. В письмах сообщается о задолженности и просьбой оплатить поддельные квитанции онлайн, либо предоставить сведения об уже совершенной оплате. В случае, если клиент начинал производить оплату и вводить реквизиты карточки на сайте, куда его привели ссылки из письма, мошенники получали доступ к его счету. В случае игнорирования клиентом подобных сообщений, ему звонили от лица управляющей компании и убеждали в наличии «долга по квартплате». При этом мошенники пытались выяснить способы оплаты и реквизиты карточки, по которой проводился платёж, и предлагали совершить «тестовую транзакцию для проверки», а также сообщить им код из SMS.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные. Ведь Ваша безопасность в первую очередь в Ваших руках!

В настоящее время на территории Брестской области продолжает наблюдаться активность злоумышленников, которые осуществляют звонки на мобильные телефоны граждан и под видом представителя банковского учреждения Республики Беларусь пытаются завладеть реквизитами их банковских платежных карт, а также иными конфиденциальными данными. 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. Следует отметить, что преступники используют современные возможности сети Интернет (например, возможность «подмены номера»), а также используют для звонков интернет-мессенджеры, в частности «Viber», где в качестве имени пользователя (никнейм) указывают официальный номер банка либо его название, как следствие у потерпевшего на экране мобильного телефона может отображаться совершенно любой абонентский номер телефона или никнейм, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, а также наименования реальных финансовых организаций, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным.

Следует обращать внимание на то, что **сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен**.

Если Вам поступил такой звонок, то:

-    **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.

**Мошенники в киберпространстве и как им противостоять!**

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя Ваши эмоции.

Например, злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта друга, родственника или знакомого в социальных сетях. В ходе звонка или переписки мошенник:

1. Описывает свою сложную жизненную ситуацию и просит помочь ему материально;
2. Представляется работником банка, «запугивает» ложной информацией о сомнительных операциях с банковской платежной карточкой (наличии заявки на кредит, блокировке счета или мошеннических атаках), и предлагает для сохранения оставшихся денежных средств перевести их на новый счет;
3. Представляется потенциальным покупателем товара, объявление о продаже которого было размещено держателем карточки в сети интернет (наиболее популярны платформы по продаже б/у вещей).

**Сценарии могут быть разными, а итог один: держатель карточки самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли.**

**Помните! Такие случаи не относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные злоумышленнику сообщил он сам.**

**Обращаем Ваше внимание, что телефонный номер мошенника может быть похож на телефонный номер Банка и отличаться одной или несколькими цифрами.**

**Иногда, действительно, требуется получение комментариев от держателя карточки по факту совершения операции, которая является сомнительной для Банка. В таком случае Банк направляет на телефонный номер клиента SMS-сообщение с просьбой перезвонить в Центр клиентской поддержки Банка.**

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в Банк по номеру, указанному на Вашей банковской карте.

**Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!**

Вот несколько простых советов, соблюдение которых, позволит не стать жертвой злоумышленников:

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (задайте другу вопрос, ответ на который знаете только вы оба);
2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по указанному на банковской карте или официальном сайте номерам;
3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от Банка — это повод уточнить ее достоверность и перезвонить в Банк;
4. Работники Банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему дистанционного банковского обслуживания (Интернет-банкинг, М-банкинг и другие). В такой ситуации немедленно прервите разговор и свяжитесь с Банком;
5. Никому и никогда не сообщайте данные своей карточки и всегда держите ее в поле зрения при совершении платежей;
6. Обязательно подключите 3D-secure и смс-оповещение;
7. Используйте только официальный сайт Банка для входа в систему Интернет-банкинга или официальное мобильное приложение;
8. Регулярно обновляйте пароли, используемые для входа в систему дистанционного банковского обслуживания, а также для подтверждения платежей;
9. В случае выявления действий по карточке, которые вами не совершались, необходимо оперативно обратится в Банк или самостоятельно заблокировать карточку в системе дистанционного банковского обслуживания.

**Рассмотрим самые распространенные схемы мошенничества сейчас:**

1. **«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

**У вас просят конфиденциальные данные**

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVС-код). Это нужно якобы «для сохранности ваших денег».

**Как мошенник пытается вас убедить**

* «*Мы звоним с официального номера, проверьте на сайте».*
* *«В целях конфиденциальности я включаю робота, который защитит ваши данные»*(вы слышите в трубке лёгкий шелест).
* Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
* Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
* Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

**Важно!** Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

1. **«Потенциальный покупатель»**

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

**Ссылка**

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

**QR-код**

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

**Важно!** Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

**Запомните!** Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

1. **«Сообщения в социальных сетях»**

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

**Важно!**При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

1. **«Розыгрыши/раздачи/опросы от Банка или иных организаций»**

Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи я годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение.

Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения либо с целью получения последнего – ввести данные Вашей банковской карты.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

**Важно!** Посетите официальную страницу организации или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

**ПЛАН-КОНСПЕКТ**

**к проведению комплекса профилактических мероприятий**

**«Декада кибербезопасности «КиберДети»**

**ВВЕДЕНИЕ**

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.

Экспоненциально увеличивающийся поток информации и преобладание цифровой информации в образовательной среде современной школы актуализируют проблему профилактики цифровой безопасности современных школьников. Особое место в данном вопросе принадлежит профилактике цифровой зависимости школьников, поскольку  дети проводят в интернете довольно много времени.

Как известно, интернет не только содержит множество полезной информации и предоставляет выбор развлечений, но и таит массу угроз, которые могут повлиять и на материальное состояние семьи, и на психологическое здоровье детей.

На текущий момент возраст интернет-пользователя снизился настолько, что порой пятилетние малыши обращаются с компьютером и мобильными устройствами более ловко, чем взрослые. Помимо всех известных положительных моментов, интернет несет в себе опасность, которая может затронуть даже пользователей младшего дошкольного возраста.

Рассмотрим основные угрозы, которым подвергается молодежь в современном киберпространстве.

1. **ВИШИНГ**

**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.

1. **ФИШИНГ**

**Фи́шинг** – 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: Kufar, Белпочта, 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.

Стоит отметить, что применяемая злоумышленниками схема хищений характерна не только для Беларуси. Столь же системно эти преступления совершаются в отношении пользователей схожих ресурсов, ориентированных на иные государства СНГ: России (avito.ru), Украины (olx.ua), Казахстана (olx.kz) и др.

1. **СВАТИНГ**

**Сватинг** – заведомо ложный вызов полиции, 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. 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.

1. **ДДОС-атаки**

**DoS**  – это атака на вычислительную систему с целью довести её 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.

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.

1. **ГРУМИНГ**

**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.

Порой под влиянием ситуации или эмоций, может показаться, что переслать такие фото – хорошая идея. Чаще всего парни и девушки делают это флиртуя, поддавшись настойчивым уговорам, пытаясь развлечь своих друзей, чтобы получить их признание (чаще пересылают чужие фото, чтобы похвастаться), или же просто отомстить. Эта идея, прямо скажем, не очень хорошая: злоумышленник может воспользоваться такой доверчивостью во вред.

1. **КИБЕРБУЛЛИНГ**

**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 террора 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 превосходства над соперником, чувство собственной неполноценности, самореализация.

 Особо следует отметить способ воздействия запрещенным контентом. Ребенку могут показывать порнографические материалы, нанося ущерб психике, так как изображенное со временем перестанет восприниматься ребенком как аморальное поведение.

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.

1. **МОШЕННИЧЕСТВО В СОЦСЕТЯХ**

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.

1. **СОВЕТЫ ПО БЕЗОПАСНОСТИ**

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.

***Советоваться с родителями***

Если ребенок хочет зарегистрироваться на каком-либо сайте, создать профиль в социальной сети и выложить свои фотографии, лучше перед этим посоветоваться с родителями. Взрослый человек сможет лучше проанализировать ситуацию и понять, опасен ли сайт, а также помочь выбрать снимки, которые можно выложить на всеобщее обозрение.

***Установить дистанционный контроль***

Функция**«родительского контроля»** – это и как специализированное ПО, так и услуги провайдера, которые включает в себя стандартный набор функций. А именно:

* ограничение времени нахождения ребенка в сети;
* ограничение времени пользования компьютером;
* возможность создания графика с допустимыми часами работы в течение дня;
* блокировка сайтов с запрещенным контентом;
* ограничение на запуск приложений (например, игр и иных приложений) и установку новых программ;

***Беречь личные данные***

Даже если ребенок думает, что хорошо знает человека, с которым общается онлайн, не нужно рассказывать подробности о себе и о родителях. Номер телефона, адрес, номер школы и класса, место работы родителей и их график, время, когда в квартире нет взрослых, а также данные из документов, номера банковских карт – такую информацию ни в коем случае нельзя передавать другим людям.

***Не делиться информацией о знакомых***

Правило, приведенное выше, распространяется и на других людей. Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают. Нельзя показывать их фотографии – ни выкладывать их в своих профилях в социальных сетях, ни тем более в частной переписке.

Если хочется выложить групповое фото с праздника или тренировки, сначала стоит обсудить это с теми, кто изображен на снимке. И лучше, если они сообщат родителям, что такое фото публикуется в интернете.

***Фильтровать информацию***

Мошенники активно используют интернет в своих интересах. Они могут обманывать людей и манипулировать ими, давя на жалость или страх. Поэтому надо научиться скептически относиться к любой информации, размещенной в интернете, и не доверять слепо всему, что там пишут.