Согласно списку рассылки

О вопросах профилактики
преступлений против собственности
и информационной безопасности

Уважаемый руководитель!

Управлением Следственного комитета Республики Беларусь по Минской области (далее — УСК) на системной основе осуществляются мероприятия по выработке действенных мер по противодействию совершения преступлений против собственности и информационной безопасности (киберпреступности).

На киберпреступность влияет ежегодный рост числа абонентов сотовой электросвязи, держателей банковских платежных карточек (далее - БПК), а также пользователей сети Интернет.

В настоящее время отмечается рост хищений, совершаемых путем модификации компьютерной информации (ст. 212 Уголовного кодекса).

Несмотря на принимаемые Следственным комитетом Республики Беларусь, а также иными государственными органами, банковскими учреждениями, меры профилактического характера, продолжают фиксироваться случаи хищения денежных средств с банковских счетов, доступ к которым обеспечивается при использовании БПК, после передачи либо завладении информацией о реквизитах БПК злоумышленниками.

Современные методы оплаты в сети Интернет позволяют совершать платежи без знания пин-кода БПК, путем введения в компьютерную систему сведений о номере и сроке действия карточки, а также кода безопасности — CVC/CVV (трехзначный защитный код проверки подлинности карты, находящийся на оборотной стороне). Данные обстоятельства позволяют злоумышленникам, завладевшим указанными реквизитами БПК, совершать платежи в сети Интернет без ведома владельца, обладая всей необходимой для этого информацией.

Вместе с тем, Интернет-банкинг постепенно завоевывает статус основной платформы для заказа банковских услуг, осуществления денежных переводов и управления открытыми расчетными счетами.

Для доступа к системе виртуального банкинга клиент должен установить мобильное приложение или зарегистрироваться на официальном сайте финансового учреждения. Авторизация производится с привязкой к номеру телефона. Часто пользователи Интернет-банкинга указывают пароль, который совпадает с логином пользователя в учетной записи, то есть номером телефона клиента, что позволяет методом подбора осуществлять вход в личные кабинеты пользователей.

Примеры наиболее распространенных в настоящее время противоправных действий в сфере информационных технологий:

1. В социальной сети Instagram злоумышленники размещают с фейковых аккаунтов посты о продаже товаров (одежда, обувь, мебель и др.) Цены в объявлениях указываются ниже рыночной стоимости товаров. Пользователи социальной сети пишут в адрес этих «интернет-магазинов» и договариваются о покупке. В ходе общения «продавец» делает на товар скидку, показывая чеки от других покупателей, обещает бесплатную доставку, но при соблюдении обязательного условия: 100% предоплата. Когда покупатели соглашались и переводили деньги, «продавец» исчезал.

2. Аферисты оформляют в мессенджерах профиль с логотипом мобильного оператора и от его имени звонят абонентам. Пользователю сообщают о необходимости продления договора по оказанию услуг связи, замены sim-карты, перерегистрации, предлагают поучаствовать в выгодной акции. Затем собеседнику сбрасывают ссылку на якобы официальное приложение компании и убеждают установить на телефон вредоносный файл. После этого мошенники получают удаленный доступ к данным пользователя (SMS, личной переписке, информации о банковских картах, паролях и т.д.), тем самым получая возможность устанавливать сторонние приложения, позволяющие оформлять банковские услуги.

3. На торговых площадках «Куфар», «Барахолка», «AV.BY» и других злоумышленник находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хотел бы приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности лично за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на БПК пользователя, после того как пользователь соглашается, высылает в его адрес ссылку с фишинговой страницей сайта банковского или иного

учреждения (страница может быть визуально схожа со страницей Интернет- банкинга и отличаться только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится на недействующей странице Интернет-банкинга определённого банка. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свои реквизиты БПК, логин и пароль от Интернет-банкинга либо паспортные данные, а также коды из SMS-оповещений. Введя указанную информацию пользователю, как правило, сообщается об ошибке либо невозможности совершить платеж. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка или ином ресурсе, получая тем самым доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может осуществить операцию, и просит повторить указанные действия с какой-либо другой карточки (родственников или знакомых).

4. Злоумышленник после несанкционированного доступа к страницам пользователей в социальных сетях рассылает от его имени пользователям, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи в переводе денежных средств под различными предлогами, например: «Привет, не мог ли ты одолжить мне денег, отдам через пару дней», «Привет, положи, пожалуйста, 10 рублей на телефон, я отдам», «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)». Далее входит в доверие к неравнодушным пользователям и, якобы для перевода им денежных средств, просит сообщить реквизиты БПК и коды из SMS-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего данную рассылку, и не догадываясь о преступности намерений, сообщает ему указанные сведения, ввиду чего злоумышленник получает доступ к денежным средствам пользователя и совершает их хищение.

5. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, при этом злоумышленник пользуется сервисом по подмене номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним, либо использует для осуществления звонка мессенджер «Viber», где у вызывающего абонента имеется ярлык с логотипом банковского учреждения. Далее он представляется сотрудником банка и сообщает о

подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков. Когда пользователь сообщает, что никаких операций он не производил, злоумышленник заявляет, что указанные операции необходимо заблокировать, а для этого необходимо внести определенную сумму денег. В итоге добросовестные граждане снимают со счетов свои сбережения либо оформляют кредиты и в дальнейшем переводят все денежные средства на подконтрольные мошенниками счета.

6. Потерпевший в сети Интернет находит рекламу о получении дополнительного заработка в виде торговли (трейдинга) (криптовалютой, акциями и т.д.) на виртуальной бирже, после чего вводит свои анкетные данные (номер мобильного телефона, Ф.И.О.) и через некоторое время ему в различных мессенджерах (WhatsApp, Telegram, Viber и др.) поступает звонок от якобы представителя данной биржи, который рассказывает о преимуществах торговли, а также быстром и высоком заработке посредством трейдинга, после чего отправляет ссылку для регистрации учетной записи. Пройдя регистрацию потерпевший видит отображение своей учетной записи и баланса электронного кошелька. После этого, мошенник предлагает пополнить баланс кошелька учетной записи, как правило, в сумме 100 долларов США, после чего отправляет потерпевшему реквизиты банковского счета, на который следует перечислить денежные средства. После перевода денежных средств на балансе учетной записи потерпевшего отображается сумма перевода. Далее, после выполнения всех указаний и инструкций «представителя» биржи (нередко именуемых себя «консультантами»), его баланс на бирже растет в геометрической прогрессии, однако, когда потерпевший решает осуществить вывод денежных средств «представитель» биржи указывает, что вывод денежных средств невозможен ввиду нарушения требований налогового законодательства государства, на территории которого зарегистрирована биржа (либо иное основание) и указывает, что для решения данной проблемы нужно вновь пополнить баланс учетной записи, но уже на сумму, значительно выше первоначальной. Изначально консультанты позволяют вывести небольшие суммы денег, что создает впечатление надежности и доходности вложений, а также стимулирует к увеличению вложенной суммы. Однако, при последующих попытках вывести средства, сайт либо закрывается, либо отклоняет запрос, а «консультант» перестает выходить на связь.

7. Злоумышленники звонят пожилым людям, в основном на городской номер телефона, представляются родственниками, которые попали в ДТП и якобы нуждаются в срочной материальной помощи для возмещения ущерба и избежания факта привлечения к уголовной ответственности. Как правило, звонят в будние дни днем, когда молодые члены семьи на работе или учебе. Для убедительности используют заплаканный голос. После объяснения причины «родственник» передает трубку «следователю» и тот завершает начатое соучастником: рассказывает, что деньги нужно завернуть в простыни либо пакет, дождаться, пока приедет человек, и отдать. Для реалистичности ситуации просят передать средства гигиены для родственника. Если курьер за деньгами не приезжает, потерпевших убеждают, что нужно самостоятельно идти в банк и переводить деньги на электронные счета. Аферисты остаются на связи со своими жертвами вплоть до передачи денег. Они перезванивают с городского телефона на мобильный и продолжают разговор, чтобы потерпевший не смог позвонить настоящим родственникам.

Запрашиваемая преступником *указанная в вышеобозначенных ситуациях информация* ***либо известна сотрудникам банка, либо не требуется им ни при каких обстоятельствах. Сотрудники банка никогда, в том числе и в ходе телефонного разговора, не будут узнавать у клиента подобную информацию.***

Для того чтобы обезопасить себя и свои денежные средства от подобных способов хищения, необходимо:

- не разглашать логины, номера телефонов, пароли, пин-коды, реквизиты БИПК, расчетных счетов, секретные CVC/CVV-коды, данные касательно последних платежей и срока действия пластиковых карточек третьим лицам;

- в ходе использования карты подключить и использовать технологию «3D Secure». На настоящий момент это самая современная технология обеспечения безопасности платежей по карточкам в сети Интернет. Позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества по карте. При использовании этой технологии держатель банковской карточки подтверждает каждую операцию по своей карточке специальным сеансовым паролем, который он получит в виде SMS-сообщения на свой мобильный телефон;

- исключить передачу посторонним лицам полученных SMS-сообщений сеансовых паролей для подтверждения операций, а также своих банковских карточек, каким быто ни было способом;

- вводить секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с **https://, а не http://;**

- производить регулярный мониторинг выполненных операций, используя раздел с историей платежей;

- не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации; SMS-информирования о расходных операциях);

- подобрать сложный пароль, используя либо набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта, менять пароль каждые 2-4 недели, если пользуетесь чужим компьютером для входа в систему Интернет-банкинга;

- не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт используется компьютер общего доступа;

- в ходе использования Интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

- вход в личный кабинет на сайте интернет-банкинга привязать к MAC или IP-адрес. Это действие обеспечит максимальный уровень безопасности.

В случае обнаружения утерянной кем-либо БПК не стоит размещать ее фотографию в сети Интернет с целью поиска владельца. Информации, имеющейся на изображении БGK, может быть достаточно для совершения операции с использованием этих данных без ведома владельца банковской платёжной карточки, чем и пользуются злоумышленники.

В целях устранения причин и условий, способствовавших совершению преступления, руководствуясь статьей 4 Закона Республики Беларусь от 13.07.2012 № 403-З «О Следственном комитете Республики Беларусь», прошу:

рассмотреть указанное информационное письмо с сотрудниками возглавляемого Вами предприятия (организации);

в соответствии с требованиями Закона Республики Беларусь от 04.01.2014 №122-З «Об основах деятельности по профилактике

правонарушений» на системной основе проводить информирование сотрудников о проявлении осторожности и бдительности, соблюдении установленных правил безопасности пользования персональными БПК, предупредить о недопустимости игнорирования и пренебрежения действенных требований, направленных на сохранение благосостояния граждан;

с учетом темпа развития информационных систем, внедрения новых цифровых технологий принимать дополнительные меры по безопасности использования банковских продуктов, осмотрительного поведения в сети Интернет;

разместить на информационных стендах прилагаемые к письму справочно-информационные листовки.

О принятых мерах прошу уведомить территориальный отдел Следственного комитета.

Приложение: информационные листовки на 4 л.

С уважением,

Начальник Копыльского районного отдела
Следственного комитета
Республики Беларусь
подполковник юстиции О.А.Бабареко

Не станьте жертвой мошенников

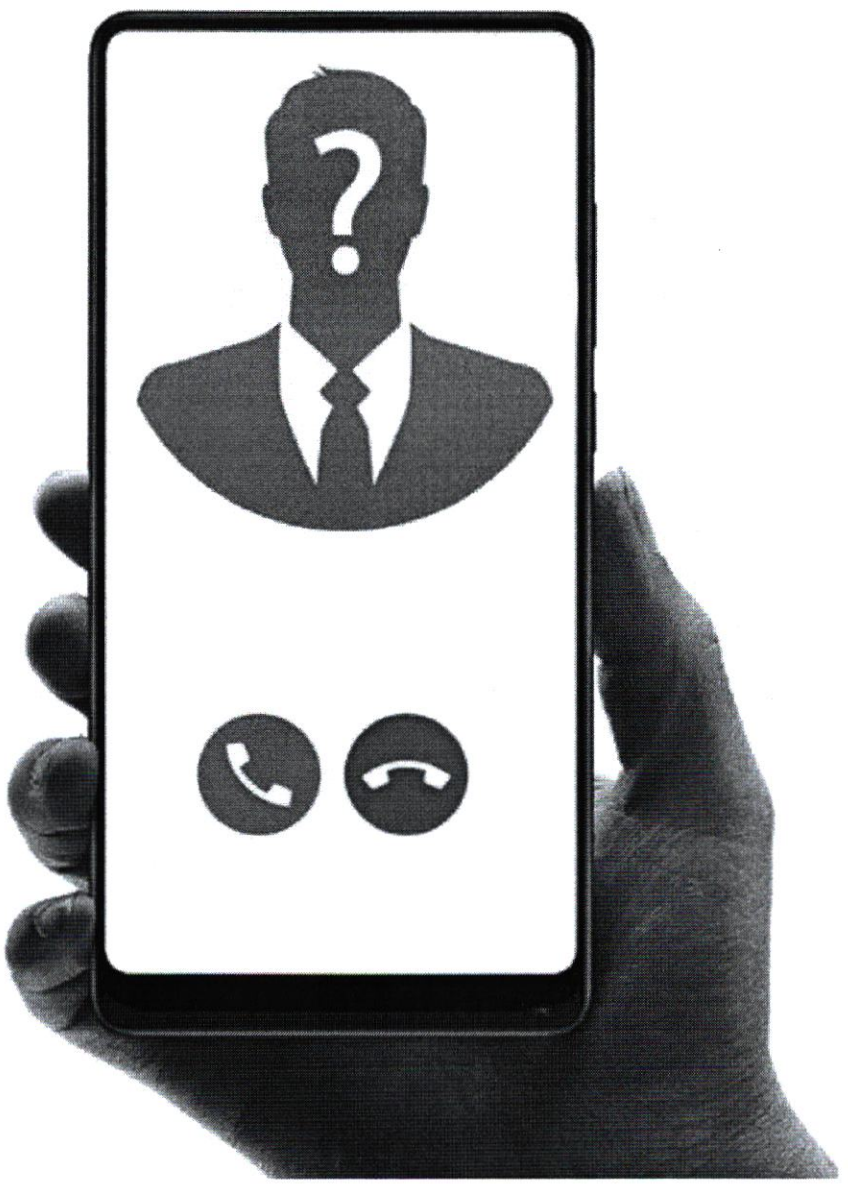
С незнакомого номера Вам звонит родственник и сообщает, что попал в жуткое ДТП и ему грозит тюрьма или он находится в больнице. Потом трубку берет якобы следователь и говорит, что срочно нужны деньги, чтобы откупиться или оплатить дорогостоящее лечение.
Не доверяйте голосу по телефону!

Ваши действия:

1. Положите трубку;

2. Перезвоните родственнику и уточните, все ли с ним в порядке;

3. Сообщите о звонке в милицию.



Не дайте себя обмануть!

КАК НЕ СТАТЬ ЖЕРТВОЙ ФИШИНГА

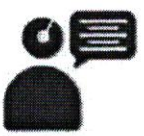
Фишинг (англ. phishing от fishing "рыбная ловля, выуживание") - вид интернет-мошенничества для получения доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков или внутри социальных сетей.

внимательно проверять ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта

зачастую фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих

перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где s означает secure) - безопасное

вместо того чтобы кликать по ссылке, следует ввести адрес вручную в новом окне браузера



даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника

обнаружив фишинговую операцию, необходимо сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети (если такие ссылки рассылает кто-то из пользователей) и т.д.

не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше воспользоваться мобильным интернетом или потерпеть, чем потерять все деньги на карте

Источник: Следственный комитет Республики Беларусь.

КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;

никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.

КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ

используйте для платежей отдельную карту

после завершения сеанса оплаты рекомендуется выйти из браузера

переводите на указанную карту точную сумму денежных средств, которая необходима вам для оплаты

при работе на устройстве, с которого производится оплата, ни в коем случае не переходите по сомнительным ссылкам

производите оплату только с устройств (ноутбуков, планшетов, компьютеров, мобильных телефонов), защищенных антивирусным программным обеспечением*

не используйте для расчетов устройство, к которому имеют доступ более одного человека

в настройках используемого браузера нужно запретить сохранение логинов, паролей и другой конфиденциальной информации

**Антивирус должен быть включен, антивирусные базы и программа - обновляться, следует регулярно проводить антивирусное сканирование.*

Источник: Следственный комитет Республики Беларусь.