СЛЕДЧЫ КАМІТЭТ
РЭСПУБЛІКІ БЕЛАРУСЬ
Партызанскі (г. Мінска) раённы аддзел
вул.Велазавадская, 3
220033 г. Мінск
тэл. (017) 3899272, факс (017) 3899256

СЛЕДСТВЕННЫЙ КОМИТЕТ
РЕСПУБЛИКИ БЕЛАРУСЬ
Партизанский (г. Минска) районный отдел
ул.Велозаводская, 3
220033. г. Минск
тэл. (017) 3899272, факс (017) 3899256

«__» апреля 2021 №5/15-____
На №_______ от _______________

Национальная академия наук Беларуси
пр-т Независимости, 66
220072, г. Минск,

О вопросах профилактики преступлений против собственности и информационной безопасности

В Республике Беларусь все чаще становятся актуальными проблемы преступности в сфере высоких технологий. Активизация киберпреступлений происходит на фоне ежегодного роста числа абонентов сотовой электросвязи, держателей банковских платежных карт (далее – БПК), а также пользователей сети Интернет.

В настоящее время наряду с тенденцией роста противоправных деяний в сфере высоких технологий существенно увеличилось количество принимаемых решений о возбуждении уголовного дела о хищениях с использованием компьютерной техники (ст. 212 УК).

Участились случаи хищения денежных средств с банковских счетов, доступ к которым обеспечивается при использовании БПК, после передачи либо завладения информацией о реквизитах БПК злоумышленниками.

Современные методы оплаты в сети Интернет позволяют совершать платежи без знания пин-кода карты, путем введения в компьютерную систему сведений о номере карты, сроке ее действия, владельце, а также коде безопасности – CVC (как правило, трехзначный код, находящийся на оборотной стороне карты). 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.

Так, в производстве Партизанского (г. Минска) районного отдела Следственного комитета находится уголовное дело, возбужденное 24.03.2021 по признакам преступления, предусмотренного частью 2 статьи 212 УК, по факту совершения 22.02.2021 хищения денежных средств, сопряженного с несанкционированным доступом к компьютерной информации с использованием данных банковской платежной карты ОАО «АСБ Беларусбанк», эмитированной на имя сотрудницы Вашей организации, чем последней причинен имущественный вред.

Согласно материалам уголовного дела, потерпевшей (является старшим научным сотрудником), поступил звонок в мессенджере «Вайбер», в ходе которого неизвестное лицо, представившись сотрудником службы безопасности банка, убедило Вашу сотрудницу в том, что кто-то несанкционированно пытается снять денежные средства с ее карт-счета, и для предотвращения данной операции необходимо сообщить номер карты, срок действия и CVC-код, что потерпевшая и сделала. В последствии с БПК потерпевшей путем несанкционированного доступа произведен перевод денежных средств.

Следует отметить, что в последнее время участились случаи противоправных действий в сфере информационных технологий, а именно хищений с БПК и счетов физических и юридических лиц, примеры подобных фактов приведены далее.

1. Злоумышленник после несанкционированного доступа к страницам пользователей в социальных сетях рассылает пользователям, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи в переводе денежных средств под различными предлогами: «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 смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, и не догадываясь о преступности намерений, сообщает ему указанные сведения, ввиду чего злоумышленник получает доступ к денежным средствам пользователя и совершает их хищение.

Проведя несанкционированную операцию по переводу денежных средств, злоумышленник часто сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

2. На торговых площадках «Куфар», «Барахолка» и других правонарушитель 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 за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на БПК пользователя и, после того как пользователь соглашается, высылает в его адрес ссылку с фишинговой страницей сайта какого-либо банковского 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 не на действующей странице интернет-банкинга определенного банка. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свой логин и пароль от интернет-банкинга либо паспортные данные, а также коды из смс-сообщений. Введя указанную информацию пользователю, как правило, сообщается об ошибке либо отсутствии платежа. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка, 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 картой (родственников или знакомых).

3. На торговых площадках «Куфар», «Барахолка» и других злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену, как правило, ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности встретиться для передачи указанного в объявлении имущества и предлагает воспользоваться услугами «Доставка Куфар», «Белпочта (ЕМС)», «курьерская служба (СДЭК)» и т. д. При согласии покупателя злоумышленник высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где предлагается ввести реквизиты банковской карты для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также коды из смс-сообщений. После ввода указанной информации пользователю обычно сообщается об

ошибке либо сайт перестает загружаться (зависает). В это время всю введенную информацию видит злоумышленник и вводит ее на действительном сайте банка, получая доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

4. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником банка (может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты либо информацию о недавно совершенных оплатах). Злоумышленник 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 сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя сообщить отдельные реквизиты БПК либо паспортные данные, и сообщает, что в адрес пользователя высылает смс-сообщения с кодами, которые необходимо назвать после звукового сигнала. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка и получает доступ к денежным средствам пользователя и совершает их хищение.

Вся **запрашиваемая преступником** указанная в выше обозначенных ситуациях информация **известна сотрудникам банка, которые не устанавливают ее в ходе телефонного разговора**.

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

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW- коды, данные касательно последних платежей и срока действия пластиковых карт 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 карты подтверждает каждую операцию по своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли для подтверждения операций, а также своих банковских карт, каким бы то 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://;

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

не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации);

подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Менять пароль каждые 2 – 4 недели, если пользуетесь чужими компьютерами 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-адресу. Это действие обеспечит максимальный уровень безопасности.

В случае обнаружения утерянной кем-либо БПК не стоит выкладывать ее фотографию в сети Интернет с целью поиска владельца. Информации, имеющейся на изображении БПК, достаточно для совершения операций с использованием этих данных без ведома владельца банковской карты, 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 информационное письмо с сотрудниками Национальной академии наук Беларуси с участием следователя Партизанского (г. Минска) РОСК Чубрик В.В. с целью недопущения совершения преступлений в отношении сотрудников Вашей 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.

О принятых мерах прошу уведомить Партизанский (г. Минска) районный отдел Следственного комитета в месячный срок.

Также прошу разместить приложение к настоящему письму на информационных стендах Национальной академии наук Беларуси.

Приложение: информация на 4-х л.

С уважением,

Следователь В.В.Чубрик

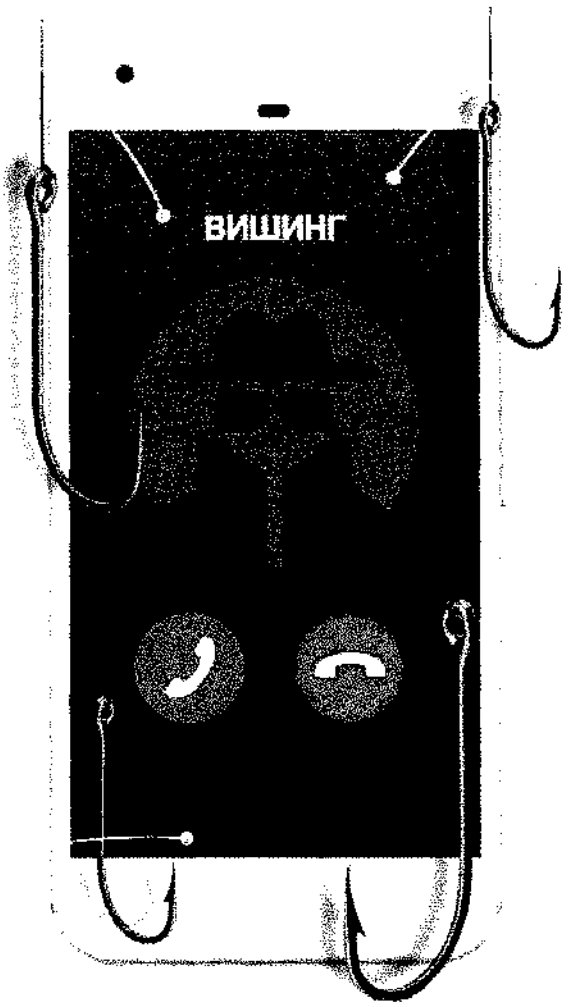
Исп./Чубрик В.В.
р.т.3899272

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 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 ИНТЕРНЕТ-МОШЕННИКОВ

ПРИ ОПЛАТЕ ТОВАРОВ В ИНТЕРНЕТЕ:

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.

GROUP-IB

ПРАВИЛА ВЫЖИВАНИЯ В ЦИФРОВОМ МИРЕ

Киберпространство — это особая цифровая среда, где полезное и интересное соседствует с опасностью и риском. Чтобы пользоваться интернетом безопасно, важно соблюдать базовые правила.

Безопасность устройств

- Регулярно обновляй операционную систему и приложения на смартфоне, планшете и персональном компьютере.
- Устанавливай приложения только из официальных источников (App Store, Google Play и Windows Market).
- Для каждого аккаунта используй индивидуальный пароль, который рекомендуется менять раз в три месяца. Роутера это тоже касается.
- Обязательно делай резервные копии важной информации.
- Всегда блокируй свои устройства (ПК, смартфон, планшет), когда не работаешь с ними.

Фишинг

- Помни, что злоумышленники постоянно придумывают новые правдоподобные сценарии, чтобы обмануть тебя — заставить открыть файл, перейти по ссылке или ввести персональные данные на мошеннической странице.
- Всегда внимательно проверяй адресата, от имени которого тебе пришло сообщение в электронной почте. Если возникли сомнения, лучше позвонить или другим способом связаться с человеком, от которого пришло письмо, чтобы убедиться, что это не мошенник.
- Не открывай подозрительные ссылки, файлы от незнакомцев в почте и в социальных сетях.
- Если тебе звонят из банка и просят выполнить какое-то подозрительное действие или раскрыть данные, сразу положи трубку и перезвони в банк по номеру телефона, указанному на сайте или на оборотной стороне банковской карты.

Безопасность в соцсетях

- Никогда не размещай в соцсетях данные паспорта, банковской карты или других документов, содержащих твои персональные данные.
- Не добавляй в друзья неизвестных тебе людей и закрой свой профиль от незнакомцев.
- Не хвастайся дорогими покупками в интернете и не раскрывай незнакомцам подробности о своей семье и семейном бюджете.
- Не выкладывай в соцсети фотографии родителей, родственников, близких и знакомых без их согласия.

Кибербуллинг и травля в интернете

- Если кто-то оскорбляет и провоцирует тебя в сети, сохраняй спокойствие и не ведись на провокацию.
- Сразу прекрати общение с этим человеком, заблокируй его и сообщи родителям или взрослому, которому доверяешь.

Управление «К»
МВД Республики Беларусь