Управление по образованию Борисовского
районного исполнительного комитета
222520, г.Борисов,
ул. Орджоникидзе, 9

ПРЕДСТАВЛЕНИЕ
о принятии мер по устранению причин и условий, способствовавших совершению преступлений

В Борисовском районном отделе Следственного комитета Республики Беларусь (далее Борисовское РОСК) с целью выяснения причин и условий совершения хищений денежных средств граждан с использованием интернет-ресурсов, социальных сетей и принятия мер по их недопущению, проведен анализ криминогенной обстановки на территории Борисовского района Минской области.

Так, установлено, что на территории г.Борисова и Борисовского района выявлены преступления данной категории, совершенные в 2022 году, по которым потерпевшими являются работники и учащиеся средних учебных учреждений нашего региона, в том числе по уголовным делам №22126021863 и №22126022017, находящимися в моем производстве.

В ходе расследования уголовного дела №22126021863 установлено следующее:

уголовное дело №22126021863 возбуждено Борисовским РОСК 02.12.2022 по признакам преступления, предусмотренного ч. 1 ст. 212 УК Республики Беларусь, по факту того, что неустановленное лицо, находясь в неустановленном месте, используя в качестве средства совершения преступления неустановленные программно-технические средства и устройства, подключенные к глобальной компьютерной сети «Интернет», путем модификации компьютерной информации, выразившейся во внесении в компьютерную систему процессингового центра банка заведомо для себя ложную информацию о правомерном держателе БПК преподавателя одного из учреждений образования г.Борисова, в ходе телефонного разговора, представившись сотрудником банка и милиции, получило доступ к счету БПК, откуда совершило хищение денежных средств.

Указанные в допросе потерпевшей обстоятельства дают повод полагать, что она не информирована о подобных преступлениях, о безопасном своем поведении при встрече с мошенниками и безопасном поведении в сети Интернет.

В ходе расследования уголовного дела №22126022017 установлено следующее:

уголовное дело №22126022017 возбуждено Борисовским РОСК 30.12.2022 по признакам преступления, предусмотренного ч. 1 ст. 212 УК Республики Беларусь, по факту того, что неустановленное лицо, находясь в неустановленном месте, используя в качестве средства совершения преступления неустановленные программно-технические средства и устройства, подключенные к глобальной компьютерной сети «Интернет», путем модификации компьютерной информации, выразившейся во внесении в

компьютерную систему процессингового центра банка заведомо для себя ложную информацию о правомерном держателе БПК работника одного из учреждений образования г.Борисова, в ходе телефонного разговора, представившись сотрудником правоохранительных органов, получило доступ к счету БПК, откуда совершило хищение денежных средств.

Указанные в допросе потерпевшей обстоятельства дают повод полагать, что она не информирована о подобных преступлениях, о безопасном своем поведении при встрече с мошенниками и безопасном поведении в сети Интернет.

При этом в Ваш адрес и адрес учебных учреждений г.Борисова ранее уже направлялись информационные письма о доведении информации о безопасном поведении в сети Интернет и иных преступлениях в сфере киберпреступности.

Таким образом, установлено, что причиной совершения противоправных действий, явилось беспечное отношение потерпевших к сохранности личного имущества, в том числе денежных средств.

Анализ изучения материалов уголовного дела показал, что условиями, способствовавшими совершению данных преступлений, явились: незнание жертв о данном виде хищения, непроведение профилактических мероприятий Управлением по образованию Борисовского районного исполнительного комитета, направленными на принятие мер по обеспечению сохранности личного имущества, у том числе указанным выше способом.

В целях исключения совершения аналогичных преступлений прошу довести данную информацию до Ваших работников и учащихся, исключив переводы денежных средств под обманом моешенников, а также предоставление сведений о реквизитах банковских платежных карточек, а именно: номере карт-счета, срока действия, кодов доступа, сведений из смс-сообщений банков, в социальных сетях («ВКонтакте», «Одноклассники»), в мессенджерах, в том числе «Вайбер», в непроверенных ссылках.

Кроме того, установлено, что по ряду уголовных дел, находящихся в производстве Борисовского РОСК, злоумышленники различными способами вводят заблуждение граждан: под видом работника службы безопасности банка, представителей иных государственных организаций, сотрудником правоохранительных органов, покупателя/продавца торговый площадок глобальной сети Интернет («Куфар» «Онлайнер» и др.) под предлогом сдачи квартиры, покупки либо продажи товаров, в том числе бывших в употреблении. В ходе общения потерпевшие лично сообщают полный номер банковской карточки, срок действия, CVC/CVV код, паспортные данные, кодовое слово (цифровой код) из СМС-сообщений, переходят по фишинговым ссылкам неустановленных лиц, по ссылкам, указанным в сообщениях о призах, выигрышах, оплачивают покупки на предоставленные злоумышленниками счета.

Мошенники, представляющиеся сотрудниками банка, при этом могут не спрашивать реквизиты карточек, сами называть держателю БПК номер карточки и последние операции по ней, могут направлять фотографии

удостоверений сотрудников банка и правоохранительных органов, сообщать жертве сведения о проведении спецоперации, о которой никому нельзя рассказывать, в том числе родственникам и банковским работникам, мошенники могут просить перевести деньги с депозитов и счетов якобы для сохранения на иные счета либо «зеркальные карточки» жертвы, а также на страховые счета, которые в действительности страховыми не являются. Однако сотрудники банка в действительности никогда не осуществляют звонки посредством мессенджера «Вайбер», не проводят спецоперации и разбирательства с осуществлением звонков на телефоны клиентов банка. Необходимо проинформировать Ваших работников о том, что они не должны передавать какую-либо информацию (реквизиты карточек, коды, сведения из смс-сообщений) таким «сотрудникам». С сотрудниками банка может быть только оговорен вопрос о необходимости каких-либо мероприятий непосредственно в отделении банка, в связи чем необходимо узнать у такого сотрудника, в какое отделение банка необходимо прибыть данному гражданину.

Помимо вышеуказанного способа совершения хищения в широких распространениях имеет способ завладения денежными средствами с карт-счетов граждан, выразившийся в хищении денежных средств с карт-счетов банковских платежных карт путем взлома страниц пользователей различных социальных сетей, мессенджеров, аккаунтов игровых приложений и т.п., после чего от имени пользователей рассылаются сообщения их знакомым с безобидным содержанием, а именно: с просьбой о якобы переводе денежных средств с банковской платежной карточки злоумышленника на банковскую карточку пользователя. При этом злоумышленник просит предоставить номер банковской платежной карточки пользователя, срок действия, защитный код и иную информацию. После получения указанных данных злоумышленник совершает хищение денежных средств с карт-счетов пользователей социальных сетей. Также могут рассылаться сообщения о проведении розыгрышей.

Результатом противоправных действий злоумышленников является завладение денежными средствами перечисленными потерпевшими, а также снятие всех денежных средств, находящихся на счетах банковских платежных карточках, а в некоторых случаях открытие на имя потерпевших кредитных обязательств со всеми вытекающими последствиями (неустойка, проценты по кредиту). В последнее время участились случаи оформления мошенниками онлайн-кредитов на жителей г.Борисова и Борисовского района путем обмана их посредством телефонных звонков. При этом стоит указать, что без участия граждан (если они не будут вообще общаться с такими «сотрудниками банка» по телефону, совершать по их указаниям какие-либо действия, устанавливать мобильные приложения) такой кредит на них взять мошенники не смогут. Всю информацию нужно уточнять по официальному номеру банка.

Сотрудники банка или правоохранительных органов в телефонном разговоре никогда не будут предлагать взять кредит для установления

мошенников, либо в иных случаях подозрения на мошеннические операции по Вашему счету.

Также можно стать жертвой преступления, введя реквизиты банковской платежной карточки и паролей при оплате каких-либо платежей в интернет-банкинге, если перейти по неправильным ссылкам на сайт банка. Так при пользовании данными интернет-услугами необходимо пользоваться установленными специальными приложениями интернет-банкинга (м-банкинга) соответствующего банка. Так как при вводе в поисковик (интернет-браузер) в глобальной сети Интернет запроса о сайте банка либо непосредственно интернет-банкинга можно перейти по фишинговым (ложным) ссылкам на сайты, с помощью которых мошенники получают доступ к карт-счету жертвы. При этом отличать поддельный сайт от официального будет только доменное имя.

Также имеются факты завладения денежными средствами граждан при прохождении последними опросников либо розыгрышей банков в глобальной сети Интернет (в мессенджерах и соцсетях), якобы от имени банка, где в предоставленной форме в последующем необходимо ввести логин и пароль от интернет- банкинга либо реквизиты банковской карточки.

В настоящее время также участились случаи звонков по телефону либо в мессенджерах от имени сотрудников правоохранительных органов с просьбой передать некоторую сумму денег во избежание уголовной ответственности родственников жертв, которые якобы попали в ДТП, после чего похищаются денежные средства жителей г.Борисова и Борисовского района.

При должной осведомлённости и бдительности граждан вышеуказанные преступления могли быть предотвращены. Жители города Борисова и Борисовского района, в том числе работники учреждений образования г.Борисова и Борисовского района, надлежащим образом не информированы о том, что недопустимо перечислять денежные средства на непроверенные счета, передавать третьим лицам реквизиты своих банковских платежных карточек, на которые начисляется заработная плата, стипендия и иные платежи, переходить по непроверенным интернет-ссылкам, а также о последствиях таковых манипуляций.

В целях исключения совершения аналогичных преступлений в отношении подчиненных Вам работников, требую довести данную информацию на занятиях по правовому информированию, разъяснив, следующее:

- не следует перечислять денежные средства на непроверенные счета,
- не следует сообщать в телефонных разговорах (даже сотруднику банка), социальных сетях, торговых площадках сети Интернет номер банковской платежной карточки, иные реквизиты, паспортные данные, CVC/CVV код, коды из смс-сообщений, в том числе для отмены каких-либо операций, необходимо перезвонить в свой банк по официальному номеру, не сообщая никаких данных по неизвестным номерам;

- не следует переходить по непроверенным ссылкам в сообщениях о призах, выигрышах, компенсациях за взлом аккаунта и т.д.

-не следует переходить по непроверенным ссылкам сайтов банка (интернет-банкинга) в браузере компьютера либо иного устройства, а проводить все оплаты только в официальном мобильном приложении М-банкинга,

-не следует передавать незнакомым лицам денежные средства для решения вопросов сотрудниками правоохранительных органов о не привлечении лиц к ответственности, по звонкам о якобы произошедших ДТП с родственниками,

- не следует по указанию в телефонном разговоре каких либо лиц (в том числе сотрудников банка) переустанавливать интернет-банкинг либо устанавливать иные мобильные приложения, так как это может привести к удаленному доступу к их устройству.

В случае, если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, проверять данную информацию путем телефонных звонков специалисту банка по официальным телефонам банка.

Принять иные меры, которые по Вашему мнению исключат возможность совершения подобных преступлений.

Вместе с тем установлено, что в качестве свидетелей по уголовным делам допрашивались учащиеся средних и средне-специальных учреждений г.Борисова, так как в настоящее время данная категория граждан (учащиеся Республики Беларусь) чаще всего являются лицами, которые под обманом либо по просьбе мошенников оформляют на свое имя банковские счета, карточки, электронные кошельки, которые в последующем используются мошенниками для совершения преступлений. Учитывая указанное, прошу довести до учащихся и работников учреждений образования на совещаниях и дополнительных классных собраниях (провести в каждом классе и учебной группе) информацию о том, что в 2021 году введена уголовная ответственность по ст. 222 УК Республики Беларусь (можно ознакомиться в открытых источниках в сети Интернет) за незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам.

То есть необходимо довести, что ни в коем случае нельзя передавать иным лицам (даже знакомым) свои паспортные данные, реквизиты банковских карточек (счетов, электронных кошельков), а также реквизиты доступа к данным счетам (логин и пароль к интернет-банкингу). При этом мошенниками могут указываться различные предлоги получения данных сведений, а именно: подработка на интернет магазин, акция банка по оформлению карт с вознаграждением оформление аккаунтов в сети Интернет, работа с криптовалютой и

преступной деятельности использовалась его карточка (достаточно самой только передачи данных либо карточки).

По этому во избежание возможности привлечения к уголовной ответственности учащихся Ваших учебных заведений прошу провести такие дополнительные занятия по правовому обучению и просвещению.

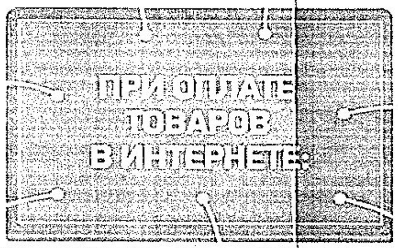
На основании изложенного, в целях устранения причин и условий, способствовавших совершению данного преступления, руководствуясь ст.199 УПК Республики Беларусь и ст. 21 Закона Республики Беларусь от 04.01.2014 №122-З «Об основах деятельности по профилактике правонарушений», -

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 активен, антивирусные базы и программа - обновляться, следует регулярно проводить антивирусное сканирование.*

Источник: Следственный комитет Республики Беларусь.

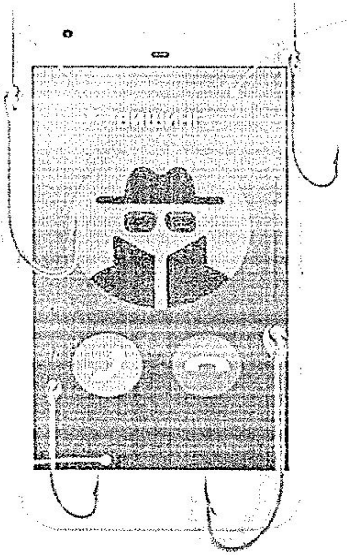
© Инфографика

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.

© Инфографика

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, полученными из

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