



2-70 / 2602

СЛЕДСТВЕННЫЙ КОМИТЕТ
РЕСПУБЛИКИ БЕЛАРУСЬ
УПРАВЛЕНИЕ
ПА МІНСКАЙ ВОБЛАСЦІ
БАРЫСАЎСКИ
РАЁННЫ АДЗЕЛ
вул. Рабочы Хімік, 13, 222520,
г. Барысаў, Мінская вобласць
тэл./факс (0177) 70 89 11
e-mail: bor_mo@sledcom.by

СЛЕДСТВЕННЫЙ КОМИТЕТ
РЕСПУБЛИКИ БЕЛАРУСЬ
УПРАВЛЕНИЕ
ПО МИНСКОЙ ОБЛАСТИ
БОРИСОВСКИЙ
РАЙОННЫЙ ОТДЕЛ
ул. Рабочий Химик, 13, 222520,
г. Борисов, Минская область
тэл./факс (0177) 70 89 11
e-mail: bor_mo@sledcom.by

ООО «Витрум Плюс»
220014, г. Минск
пер. Софьи Ковалевской,
д. 60, 9 этаж

~~О вопросах профилактики
преступлений против собственности
и информационной безопасности~~

Борисовским РОСК 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 с использованием информационно-коммуникационных технологий (далее ИКТ).

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

В производстве Борисовского РОСК находится уголовное дело, возбужденное по ч. 1 ст. 212 УК Республики Беларусь в отношении неустановленного лица, которое 27.12.2025, находясь в неустановленном месте, имея умысел на хищение денежных средств путем модификации компьютерной информации, используя в качестве средства совершения преступления неустановленные программно-технические средства и устройства, подключенные к глобальной компьютерной сети Интернет, с использованием поддельного интернет-ресурса (фишинговой ссылки) «<https://alfaprm.online>», размещенной в социальной сети «Instagram», получило доступ к счету БПК, эмитированного ЗАО «Альфа-Банк» на имя работника Вашей организации, завладело реквизитами БПК, в продолжении своего преступного умысла, совершило хищение денежных средств со счета БПК на сумму 900 рублей, в результате чего, работнику Вашей организации, причинен материальный вред на указанную сумму.

Современные методы оплаты в сети Интернет позволяют совершать платежи без знания PIN-кода БПК, путем введения в компьютерную систему сведений о номере и сроке действия карточки, а также кода

Вход. № 53
02.03.2026.

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 Instagram злоумышленники размещают с фейковых аккаунтов посты о продаже товаров (одежда, обувь, мебель и др.) Цены в объявлениях указываются ниже рыночной стоимости. Пользователи соцсети пишут в эти «интернет-магазины» 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», «Базахолка», «AV.BY» 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 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 предложениями: «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 вызываемого 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 не 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, дожидаться, 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 выше обозначенных 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 БПК, 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 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://, 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-адресу. 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 БПК, может быть достаточно для совершения операции с использованием этих данных без ведома владельца БПК, чем и пользуются злоумышленники.

На основании изложенного, прошу:

- рассмотреть указанное информационное письмо с работниками Вашей организации с целью повышения их грамотности при общении с неустановленными лицами в сети Интернет и недопущения подобных ситуаций в дальнейшем;

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

О принятых мерах прошу уведомить Борисовский РОСК.

Приложение: справочно-информационные листовки на 3 листах.

Следователь
Борисовского районного отдела
Следственного комитета



Е.А.Березко



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.



ВНИМАНИЕ!

Сотни граждан Республики Беларусь стали жертвами телефонных мошенников в 2022 году.

Каждый пострадавший лишился от 1000 до 50 000\$.

Сценарии обмана могут быть разными, суть одна: звонок с незнакомого номера, экстренная ситуация и просьба передать курьеру крупную сумму денег.



Бабушка, я попала в аварию! Помогите!

Из-за меня пострадали люди!
Срочно нужны деньги!

Вашей внучке грозит тюрьма,
но вы можете передать деньги.

Чтобы избежать уголовной
ответственности, нужно 50 000\$.

Не доверяйте голосу в телефоне!
Не дайте себя обмануть!

ПРАВИЛЬНЫЕ ДЕЙСТВИЯ:

1. Положите трубку;
2. Перезвоните родственнику и уточните, всё ли с ним в порядке;
3. Сообщите о звонке в милицию по телефону 102.

