ИНФОРМАЦИОННОЕ ПИСЬМО о состоянии преступности, связанной с неправомерным завладением реквизитами пластиковых банковских карт и хищением средств с карт-счетов граждан.

Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека, что порождает и новые виды преступной деятельности. Во всем мире сложилась тенденция, когда методы совершения киберпреступлений постоянно совершенствуются и видоизменяются и зачастую опережают развитие систем защиты.

Посредством глобальной компьютерной сети Интернет стали возможными факты вымогательств, мошенничеств, распространение наркотиков и детской порнографии, груминг, кибербуллинг и кибертерроризм, фишинг, вишинг.

Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные и имущество граждан.

Расширение в республике сферы внедрения информационно-коммуникационных технологий (далее - ИКТ) обусловило рост числа угроз и противоправных деяний в области информационной и финансовой безопасности.

Несмотря на принимаемые меры, на протяжении нескольких последних лет наблюдается устойчивый рост количества регистрируемых киберпреступлений.

Изощренность преступников, постоянное совершенствование методов и способов преступной деятельности одновременно с низкой цифровой и финансовой грамотностью граждан, недостаточным уровнем систем защиты влекут лавинообразный рост числа регистрируемых хищений с использованием компьютерной техники (статья 212 Уголовного кодекса Республики Беларусь (далее - УК)).

Число зарегистрированных таких хищений в 2020 году (2 466) почти в 4 раза превысило уровень 2019 года (618), что составляет более 90 % от общего количества преступлений в сфере высоких технологий. Причиненный ущерб составил 1 527 371 рубль (ущерб за весь 2019 год - 346 453 рубля). За три месяца 2021 года зарегистрировано уже 616 указанных преступлений с размером ущерба 573 819 рублей.

Отмеченный общий рост числа регистрируемых преступлений, предусмотренных статьей 212 УК, обусловлен увеличением таковых, совершенных посредством глобальной сети Интернет и ИКТ.

Информация о способах совершения хищений с использованием компьютерной техники согласно сведениям Единого государственного банка данных о правонарушениях приведена в таблице:

Способ совершения хищения (ст.212 УК)	2019	2020	3 мес. 2021
Посредством завладения реквизитами доступа и (или) несанкционированного доступа к ресурсам	368	1841	457
Посредством приобретения товаров в Интернете и (или) оплаты услуг	22	61	6
Посредством найденной (украденной) БПК	90	169	35
Путем использования вредоносных программ и (или) несанкционированного доступа	18	117	25
Иной способ совершения	120	278	93
Общий итог	618	2466	616

Большая часть преступлений в сфере высоких технологий совершается в условиях неочевидности.

Следует отметить, что транзакции денежных средств с банковских счетов юридических лиц и физических на подконтрольные банковские счета преступников, как показывает практика, связаны с трансграничными переводами на зарубежные счета (практически все похищенные у граждан денежные средства переводятся на счета иностранных банков, а также электронные кошельки зарубежных платежных систем).

Преступному воздействию посредством глобальной компьютерной сети Интернет преимущественно подвергается конфиденциальная информация и персональные данные граждан.

Большинство указанных хищений совершено с использованием переданных держателями реквизитов банковских пластиковых карт (далее - БПК), в частности - трехзначного защитного кода (CVV2/CVC2 кода проверки подлинности банковской карты).

При этом меры технической защиты доступа к банковским счетам успешно преодолеваются приемами «социальной инженерии», когда введенные в заблуждение о правильности своих действий клиенты банков предоставляют злоумышленникам реквизиты доступа к своим счетам, что приводит к хищению денежных средств.

Наиболее распространенными способами совершения таких преступлений в настоящее время являются хищения денежных средств граждан, разместивших объявления на торговых интернет-площадках (фишинг), посредством несанкционированного доступа к учетным записям в социальных сетях, а также с использованием реквизитов банковских платежных карточек, полученных в ходе звонков гражданам под видом сотрудника банка, правоохранительного органа

(вишинг).

Фишинг - вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным владельца банковской карты. Это достигается путем проведения рассылок СМС-сообщений/электронных писем от имени популярных брендов, внутри различных сервисов и социальных сетей, а также от имени банка.

Одна из наиболее распространенных схем фишинга на территории Республики Беларусь связана с Интернет-ресурсом «Kufar.by». Злоумышленник под предлогом приобретения товара осуществляет переписку, как правило в мессенджере «Viber», в ходе которой отправляет сообщение, содержащее ссылку с адресом фейкового Интернет-ресурса, сходного по содержанию с сайтом одной из служб доставки товара, созданного преступником специально для завладения конфиденциальными данными банковской платежной карты потерпевшего. Пользователь Интернет-ресурса «Kufar.by», думая, что вводит сведения для получения денежных средств за свой товар, предоставляет тем самым злоумышленнику все необходимые платежные данные по карте.

Вишинг - вид интернет-мошенничества, целью которого, как и фишинга, является получение доступа к конфиденциальным данным владельца карты. Основное отличие - использование телефонной связи.

Как правило, мошенники звонят банковским клиентам под видом «службы безопасности банка» или «службы финансового мониторинга» и сообщают о том, что по карте якобы совершена подозрительная операция. Под предлогом спасения денежных средств они заставляют клиента совершить ряд действий, чтобы украсть деньги с его счета. Далее схема мошенничества развивается по нескольким сценариям:

- мошенники выманивают платежные данные карты (16-значный номер, имя владельца, срок действия и трехзначный код на обратной стороне, а также код из СМС от банка) либо обманом узнают данные для входа в личный кабинет;
- мошенники в процессе звонка пронят установить на телефон специальное приложение якобы для лучшей защиты - им оказывается программа удаленного доступа и управления (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin), с помощью которой можно зайти в личный кабинет онлайн-банка жертвы и перевести оттуда деньги на свой счет;
- во время звонка мошенники убеждают своих жертв снять деньги в банкомате и зачислить их на специальный счет для «спасения средств».

В последнее время стали появляться более сложные схемы: к звонкам от «банковских работников» добавились звонки от «правоохранительных органов», которые «подтверждают», что кто-то пытает украсть деньги клиента, поэтому их надо спасти путем перевода на «безопасный» счет.

Одним из новых способов также является звонок от «банковского работника», который в разговоре указывает, что кто-то пытается взять кредит, а он, как сотрудник отдела безопасности сделает все, чтобы кредит одобрен не был. Потерпевшему для сохранности денег предлагается заблокировать карту и изменить пароль интернет-банкинга, на что последний соглашается, подтвердив всю необходимую информацию. В последующем обнаруживается пропажа со счета денежных средств.

Еще одним способом завладения денежными средствами держателей банковских карт является информирование последних посредством сети Интернет о выигрыше крупной суммы денежных средств. В ходе переписки злоумышленники, под предлогом перечисления выигрыша на банковскую карту, предлагают пройти процедуру регистрации на сайте, где держатель банковской карты указывает фамилию, имя и отчество, а также мобильный телефон. Затем запрашиваются реквизиты банковской карты, на которую якобы будет перечисляться выигрыш.

Мошенники также могут обещать интернет-пользователю крупную сумму выигрыша или выплаты, но перед этим просят заплатить небольшую «комиссию» либо осуществить «закрепительный платеж».

Помимо этого, до настоящего времени злоумышленники совершают хищения денежных средств со счетов пользователей социальных сетей, с которыми они вступили в переписку и последние под воздействием обмана, добровольно предоставили сведения о своей банковской платежной карте либо произвели перечисление денежных средств на подконтрольный преступнику счет.

Потерпевшими от названных уголовно-наказуемых деяний являются все слои населения. В 2020 году их количество составило 2 482 человека, из которых 1 759 женщин и 723 мужчины (за 3 месяца 2021 года – 622, среди которых 408 женщин и 214 мужчин).

Возраст потерпевших от хищений с использованием компьютерной техники составил:

- менее 30 лет - 617 или 24,9% (за 3 месяца 2021 г. - 106 или 17,0%);
- от 30 до 45 лет - 970 или 39,1% (197 или 31,7%);
- от 45 до 60 лет - 569 или 22,9% (199 или 32,0%);
- свыше 60 лет - 326 или 13,1% (120 или 19,3%).

По социальному положению наибольшее количество потерпевших относятся к следующим группам:

- рабочие - 860 или 34,6% (за 3 месяца 2021 г. - 245 или 39,4%);
- временно не работают и не учатся - 512 или 20,6% (89 или 14,3%);
- пенсионеры - 326 или 13,1% (99 или 15,9%);
- работники культуры, науки, медицины и образования - 271 или 10,9% (65 или 10,4%);
- в отпуске по уходу за ребенком до 3-х лет - 254 или 10,2% (46 или 7,4%);
- служащие - 162 или 6,5% (36 или 5,8%).

По образовательному уровню наибольшее количество потерпевших в 2020 году имели средне-специальное (1 072 или 43,1%) и высшее (987 или 39,7%) образование. Сохранилась данная тенденция и в текущем году, за 3 месяца которого 251 (40,3%) потерпевших имели средне-специальное и 220 (35,4%) высшее образование.

Сообщая об изложенном, прошу вышеуказанную информацию довести до сведения работников Вашего предприятия (организации, учреждения), нацелив их на необходимость более вдумчивого подхода к использованию личных банковских пластиковых карт, повышения защищенности своих финансовых сбережений от преступных посягательств.