Не ведись на поводу у мошенников

В последнее время значительно выросло число киберпреступлений. За текущий период 2021 года на территории района зарегистрировано 3 факта хищений денежных средств с банковских платежных карточек. В 2020 году по сравнению с 2019 годом таких преступлений совершено значительно больше. Причин этого несколько.

"Во-первых, повлияла пандемия, поскольку люди стали больше времени проводить дома, за компьютером. Во-вторых, банковская инфраструктура неумолимо прогрессирует: появились интернет-банкинги, возможность идентифицировать платежи через отпечатки пальцев и т.д. Большое количество сервисов появилось в сфере услуг, торговли, которыми активно пользуется население. Люди не до конца понимают, как это работает, в отличие от подготовленных жуликов, которых привлекает жажда легкой наживы. В-третьих, мошеннические схемы быстро расходятся по рукам, из-за чего увеличивается количество киберпреступников".

Еще одной из причин растущего числа преступлений в сфере высоких технологий считаются сами потерпевшие. Большинство белорусов к возможным угрозам относится равнодушно: мол, есть вирусы в компьютерах – и ладно.

Люди не понимают, в чем таится опасность и к какому ущербу может провести их незаинтересованность в защите информации. Когда у человека крадут деньги с банковского счета, то он первым же делом обращается в органы внутренних дел. Если у него похитили какую-то информацию из компьютера, то пойдет в милицию только тогда, когда мошенники, например, начнут вымогать средства.

Жертвами киберпреступлений может стать кто угодно, поскольку узнать мошенников порой нелегко. Если речь идет о вишинге (когда кто-то связывается по телефону, посредством мессенджера «Viber» или пишет в соцсетях с просьбой предоставить банковскую информацию), это 100% злоумышленник.

"Чтобы защитить себя, можно завести вторую банковскую карточку, на которой деньги не будут храниться – для расчета покупок в интернете. Поэтому если даже данные будут как-то скомпрометированы, то деньги украсть у злоумышленников не получится – их там просто не будет".

Чтобы украсть средства с карты, необходимы все ее параметры: номер, CVV-код (трехзначный, указанный на тыльной стороне карточки) и срок действия. Все эти данные нанесены на карточку.

Предотвратить киберпреступления вполне реально, если клиент банка или пользователь компьютера банально не будет сам передавать платежную информацию, будет применять сложные пароли, обновлять антивирусное ПО, регулярно чистить компьютер.

Начальник Берестовицкого РОВД А.М. Войтович

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

- хранить в тайне пин-код карты
- прикрывать ладонью клавиатуру при вводе пин-кода
- оформлять отдельную карту для онлайн-покупок
- деньги зачислять только в размере предполагаемой покупки
- использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
- скрыть CVV-код** на карте (трехзначный номер на обратной стороне), предварительно сохранив его
- подключить услугу "SMS-оповещение"

Не рекомендуется

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

** Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).*

*** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.*

**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*

Источник: МВД Беларуси.

ФИШИНГ: КАК ЗАЩИЩИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ, ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества

Потенциальный покупатель вашего товара предлагает перейти в мессенджер, отказываясь общаться непосредственно на торговой площадке.

Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок

Неизвестный в мессенджере присылает ссылку для перехода на интернет-сайт под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.

Незнакомец предлагает передать ему полные данные вашей банковской карты, включая CVV-код либо логин и пароль от вашего интернет-банкинга.

ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ