В последнее время интернет-мошенники всё чаще воруют деньги с банковских карточек. Это становится возможным потому, что сами пострадавшие сообщают реквизиты своих банковских карт.

В настоящее время широкое распространение имеют 2 основных способа обмана:

1. **«Вишинг» –** метод, при которомзлоумышленники, подменяя реальный номер телефона на номер телефона банка, и выдавая себя за сотрудников банка или правоохранительных органов под предлогом отмены операции выманивают у держателей карт конфиденциальную информацию - номер, срок действия, трёхзначный код на обратной стороне - или побуждают к установке программного обеспечения (удалённого доступа) для действий в интернет- или м- банкинге.
2. **«Фишинг» –** цель данного способа – завладеть реквизитами банковской платёжной карты. Злоумышленник под любым мошенническим предлогом вынуждает жертву пройти по ссылке на поддельный интернет-ресурс и ввести там номер карты, срок действия и CVV-код, чтобы похитить эти данные и «очистить» банковский счёт. Киберпреступники умело подделывают различные популярные интернет-ресурсы, которые оказывают услуги населению и имеют сервис совершения онлайн- платежей: торговые интернет-площадки, службы доставки, сайты торговых сетей и так далее.

Жителей г.п.Бешенковичи и Бешенковичского района данная проблема не обошла стороной, и в настоящее время отмечается всплеск хищений денежных средств с помощью компьютерных технологий. Так на данный момент на территории Бешенковичского района совершено 7 преступлений предусмотренных ч.1 ст. 212 УК Республики Беларусь, из которых только по 2 установлен подозреваемый.

**Например:.** *В феврале 2022 года с жительницей Бешенковичского района по средствам мессенджера «Viber» связался злоумышленник, при этом последний представился сотрудником службы безопасности банка, и сообщил, что с банковской карты последней пытались похитить денежные средства. В ходе общения злоумышленник убедил потерпевшую установить на компьютер приложение «AnyDesk» (которое позволяет ему видеть все операции производимые пользователем компьютера, а в некоторых, позволяет удалённо управлять компьютером), и в ходе дальнейшего общения при помощи данного приложения узнал реквизиты банковской платёжной карты потерпевшей, а также смс-код для одобрения операций по переводу денежных средств, что и позволило совершить хищение денежных средств потерпевшей на сумму чуть больше 1000 белорусских рублей.*

*В марте 2022 года была обманута жительница нашего района, которая на сайте «Куфар» разместила объявление о продаже одежд. Спустя некоторое время с ней связался лже-покупателъ, который предложил оформить покупку и оплату при помощи одного из почтовых сервисов, после чего прислал потерпевшей интернет-ссылку для получения оплаты за товар (при этом внешний вид сайта ничем не отличался от оригинального). Введя реквизиты своей ВПК на указанном сайте, потерпевшая не только ни получила оплату, а также лишилась своих денежных средств в сумме порядка 1300 рублей.*

**Денежные средства обычно перечисляются на такие платёжные ресурсы, как электронные кошельки, банковские карты зарубежных государств, а с них денежные средства перечисляются на любые платёжные сервисы. Отследить их путь очень сложно.**

**Как обезопасить себя от хищения денег через Интернет?**

1. Самое главное - никогда и никому под каким либо предлогом не передавайте номер своей банковской карты, а также номер защитного кода своей карты. Если вам пишет ваш знакомый или друг, которому действительно нужна помощь, то перезвоните ему и удостоверьтесь, что вам пишет действительно он. В любом случае не передавайте ваши личные данные банковских карт через социальные сети.
2. В социальной сети «В контакте» есть такая функция, как дополнительный уровень безопасности. Зайдите в настройки и воспользуйтесь ей. Тогда, если вашу страницу попытаются взломать, вам придёт уведомление на мобильный телефон;
3. Подключите функцию 3D-Secure- дополнительный пароль для защиты вашей карты при любых покупках в интернете. В банке вам объяснят, как это сделать. Если она подключена, то для совершения платежа в интернете, понадобится ввести специальный код, банк пришлёт вам его через смс. Без этого кода деньги с вашей карты не снимут.

Александр РЫБАКОВ,

начальник

Бешенковичского РОВД