Не ведись на поводу у мошенников

В последнее время значительно выросло число киберпреступлений. За текущий период 2025 года на территории района зарегистрировано 18 фактов хищений денежных средств с банковских платежных карточек. В 2024 году по сравнению с 2025 годом таких преступлений совершено значительно меньше. Причин этого несколько.

Во первых, 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. Во вторых, 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 наших граждан 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 совершается хищение денег 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.

Ромашкевич С.С., вриод начальника Берестовицкого РОВД