ПРОКУРАТУРА ВАСИЛЕОСТРОВСКОГО РАЙОНА РАЗЪЯСНЯЕТ

Как избежать хищения денежных средств с банковской карты?

Виды хищения

Банковский «скимминг» - незаконное снятие денежных средств с банковских карт граждан с использованием накладок на терминалы банкоматов, средств видеофиксации, а также различных электронных устройств сканерного типа

Хищение безналичных денежных средств путем удаленного взлома программного обеспечения граждан, позволяющего переводить денежные средства (система «Банк-Клиент», Онлайн-банк)

Хищение денежных средств после получения преступником доступа к паролям, телефонным номерам и (или) реквизитам расчетных счетов граждан, в том числе путем введения в заблуждение (обмана)

Хищение денежных средств путем получения доступа к мобильным устройствам с установленным онлайн-банком или банковской карте с системой бесконтактных платежей

Что нужно сделать, чтобы не стать жертвами злоумышленников?

- Снимайте денежные средства только в официальных отделениях банков;

- Будьте внимательны при использовании банкоматов;

- Убедитесь, что посторонние не наблюдают за вашими действиями по вводу пароля и совершению операций по карте;

- При использовании мобильного устройства не устанавливайте вредоносное программное обеспечение;

- Если Вам прислали MMS или ссылку с неизвестного номера, не открывайте вложенные файлы, не переходите по ссылкам, удаляйте подозрительные сообщения;
- Используйте антивирусы только от официальных поставщиков

- Не торопитесь следовать инструкциям и отвечать на запрос лица представившегося сотрудником банка
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- Проверяйте информацию, позвонив в контрактный центр банка, или обратитесь в отделение банка

- При использовании мобильного устройства установите индивидуальный пароль, который защитит Вас в случае утери устройства;

- Незамедлительно обратитесь в отделение банка и заблокируйте вашу банковскую карту