Прокуратура Приморского района Санкт-Петербурга информирует:

Внимание мошенники!

Как действуют мошенники?

Запрашивают по телефону или в электронном письме:
-персональные сведения (серия, номер паспорта, адрес регистрации, имя и фамилия владельца карты);
-реквизиты и срок действия карты;
-пароли или коды их СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин, ПИН-код и CVV-код банковских карт.

Предлагают:
-установить программы удаленного доступа (или сторонние предложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);
-перейти по ссылке из СМС-сообщения;
-включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;
-под их руководством перевести для сохранности денежные средства на «защищенный счет»;
-зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Что делать Вам:

- не сообщать реквизиты банковских карт;
- не выполнять операции по переводу денежных средств;
- прекратить общение с мошенниками и перезвонить на официальный номер банка;
- избегать подключение к общедоступным сетям WI-FI;
- избегать использование ПИН-кода или CVV-кода при заказе товаров и услуг через сеть Интернет, а также по телефону (факсу);
- применяя сервисы СМС-банка, сверяйте реквизиты операции в СМС-сообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя;
- при возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.