ОСТОРОЖНО: МОШЕННИКИ!

Как обезопасить себя от мошенничества с банковскими картами?

Не переходите по ссылкам и не устанавливайте приложения или обновления, пришедшие по СМС и электронной почте.

Никому не сообщайте номер банковской карты, который указан на ее лицевой и оборотной стороне, свои персональные и паспортные данные, срок действия карты и пин-код.

Что делать, если...

...Вам пришло СМС «Ваша банковская карта заблокирована», «Я случайно положил Вам 100 руб. на телефон. Верните мне на номер 8-9XX-XXX-XX-XX»?
Не отвечайте и не перезванивайте на номера, указанные в СМС. Проверить, заблокирована ли карта, можно в ближайшем отделении банка или по телефонам, указанным на ее оборотной стороне.

...Вам позвонили и сообщили, что с Вашей карты происходят подозрительные операции по переводу денежных средств и просят данные карты, персональные и паспортные данные?
Не верьте, это мошенники. Если сомневаетесь, положите трубку и для уточнения информации позвоните в банк по номерам телефонов, указанным на Вашей карте.

...На сайтах бесплатных объявлений («Авито.ру» и т.д.) у Вас просят перевести предоплату, персональные и паспортные данные?
Не соглашайтесь - это мошенники.

...Вы потеряли/у Вас украли телефон с подключенной услугой «Мобильный банк»?
Срочно обратитесь к оператору сотовой связи для блокировки SIM-карты и в отделение банка для прекращения действия услуги.

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.

ОСТОРОЖНО МОШЕННИКИ

Ожидание

Реальность

Прокуратура Приморского района Санкт-Петербурга разъясняет:

Не передавайте сведения своих банковских карт незнакомцам по телефону!

Помните! Сведения о номерах Ваших карт и пин-кодах нужны только мошенникам!

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО: МОШЕННИКИ!

Мошенники представляются службой безопасности банков, сообщают о краже денег с банковских счетов

САМОСТОЯТЕЛЬНО ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ В БАНКЕ

НЕ СООБЩАЙТЕ ПАРОЛИ И НОМЕРА СВОИХ БАНКОВСКИХ КАРТ

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ НА НЕИЗВЕСТНЫЕ СЧЕТА И НОМЕРА ТЕЛЕФОНОВ