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 системо 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 устройств установите индивидуалы пароль, который защитит в случае утери устройст

- Незамедлительно обрати в отделение банка и заблокируйте вашу банковскую карту

Осторожно! Мошенники!

1. Получив звонок или смс-сообщение об угрозе списания денег со счета, не спешите выдавать мошенникам персональные данные.

Проверьте информацию по телефону, указанному на обороте Вашей банковской карты.

2. Самые выгодные предложения о покупке товаров и услуг на сайтах мошенников.

Прежде чем платить, убедитесь в безопасности сайта. Проверьте адресную строку браузера, ознакомьтесь с отзывами покупателей.

3. Предлагают срочно перевести или передать крупную сумму денег для помощи попавшему в беду родственнику?

Прежде чем это сделать, проверьте информацию.

4. Получив звонок или смс- предложение от «сотрудника банка», не сообщайте персональные данные, не переводите деньги, не пишите смс-сообщения и не передавайте коды из них.

Прервите разговор.

Вовремя проявленная бдительность поможет сохранить Ваши деньги.

Сообщите об этом своим родственникам, знакомым и одиноким пожилым соседям, чем окажете помощь в сохранении их имущества.

Уважаемые жители Василеостровского района!

Прокуратура района информирует о том, что в городе зарегистрировано более тысячи преступлений, связанных с использованием платежных карт, большая часть из которых совершена посредством уведомления владельцев банковских карт о проблемах со счетом по мобильному телефону с получением в ходе разговора персональных данных, достаточных для списания денег или понуждения владельца карты самостоятельно перечислить денежные средства.

Если Вам поступил звонок от неизвестного лица, который представился сотрудником банка и сообщает об угрозе списания средств или подозрительной операции по счету и для проверки просит назвать различные реквизиты банковской карты или перевести денежные средства на другой «защищенный» счет, **Помните!** настоящему сотруднику банка названная информация **не нужна.**

Знайте! С Вами работает мошенник.

Чтобы не стать жертвой мошенников ***не сообщайте*** по телефону никому информацию о Вашей банковской карте, не переводите денежные средства на неизвестные банковские счета, электронные кошельки.

Если стали жертвой обмана обращайтесь в полицию.

Расскажите об этом пожилым родственникам и своим одиноким соседям.

Безопасные покупки в сети Интернет

Покупки через интернет быстрее и удобнее, чем традиционные походы по магазинам, особенно в условиях распространения новой коронавирусной инфекции, но и шанс столкнуться с киберпреступниками в разы выше.

Риск возникает во время покупок на сайтах и в приложениях с использованием электронного кошелька, мобильного и интернет-банкинга.

Не переходите по ссылкам и не открывайте интернет-страницы, вызывающие сомнение.

Совершая покупки в Интернете пользуйтесь только личными устройствами.

Защитите устройства, установив антивирусную программу, и регулярно обновляйте её.

- Выбирайте безопасные сайты.
- Никогда не переходите по ссылкам из электронных писем и СМС сообщений от неизвестных отправителей.
- Даже если сообщение пришло от знакомого вам человека или организации, не спешите открывать их. Возможно, у мошенников появился доступ к их аккаунтам и они хотят получить доступ и к вашим данным.
- Набирайте адрес банка вручную, а еще лучше – сохраняйте в закладках адреса интернет магазинов, банков.
- Всегда проверяйте адресную строку браузера. Иногда можно попасть на сайт «двойник», сделанный мошенниками, при переходе с одной страницы известного вам сайта на другой.
- Делайте покупки на сайтах, обеспечивающих безопасное соединение. Адрес такого ресурса начинается с https://. В адресной строке есть значок в виде закрытого замка.
- Выбирайте известные интернет-магазины и сервисы. Изучайте отзывы о них других пользователей. Лучше всего посмотреть отзывы на нескольких независимых сайтах. Добросовестный продавец всегда дает полную информацию о себе: телефон, адрес и прочие контактные данные.
- Если стали жертвой мошенников - незамедлительно сообщите об этом в полицию по телефону 02, или с мобильного - 112.

В последнее время участились случаи совершения имущественных преступлений с использованием сети интернет.

Прежде всего, перед заказом товара на интернет-сайте, убедитесь в том, что он ведет свою деятельность на протяжении длительного периода, а не зарегистрирован недавно. Указанную информацию можно проверить на сайте www.reg.ru, путем ввода названия интересующего сайта в поисковую строку. Сайт, который зарегистрирован недавно является потенциально опасным, и в случае получения злоумышленниками денежных средств покупателя приостанавливает свою работу, а абонентские номера, с которых звонили представители магазина, становятся недоступны.

Кроме того, перед заказом товара, необходимо почитать отзывы покупателей на иных источниках информации. Не делайте выводы на положительных отзывах, оставленных на сайте, на котором хотите совершить заказ.

Стоимость товаров в магазине мошенников зачастую существенно ниже, чем в других. Перед заказом товара, посмотрите его среднюю стоимость, или посмотрите ее на сайте официального поставщика. Не поддавайтесь на провокационные лозунги о выгодных условиях, таких как: «акция», «количество ограничено», «спешите купить», так как они не несут за собой никакой выгоды для покупателя и созданы лишь для привлечения внимания.

Если представитель продавца начинает торопить с оформлением заказа или его оплатой, стоит отказаться от покупки. Мошенники часто используют временной фактор, чтобы нельзя было оценить все нюансы сделки.

Особенно должно насторожить предложение перевести деньги через анонимные платежные системы, электронные деньги, банковским переводом на карту частного лица. В таком случае нет гарантии возврата или получения товара.