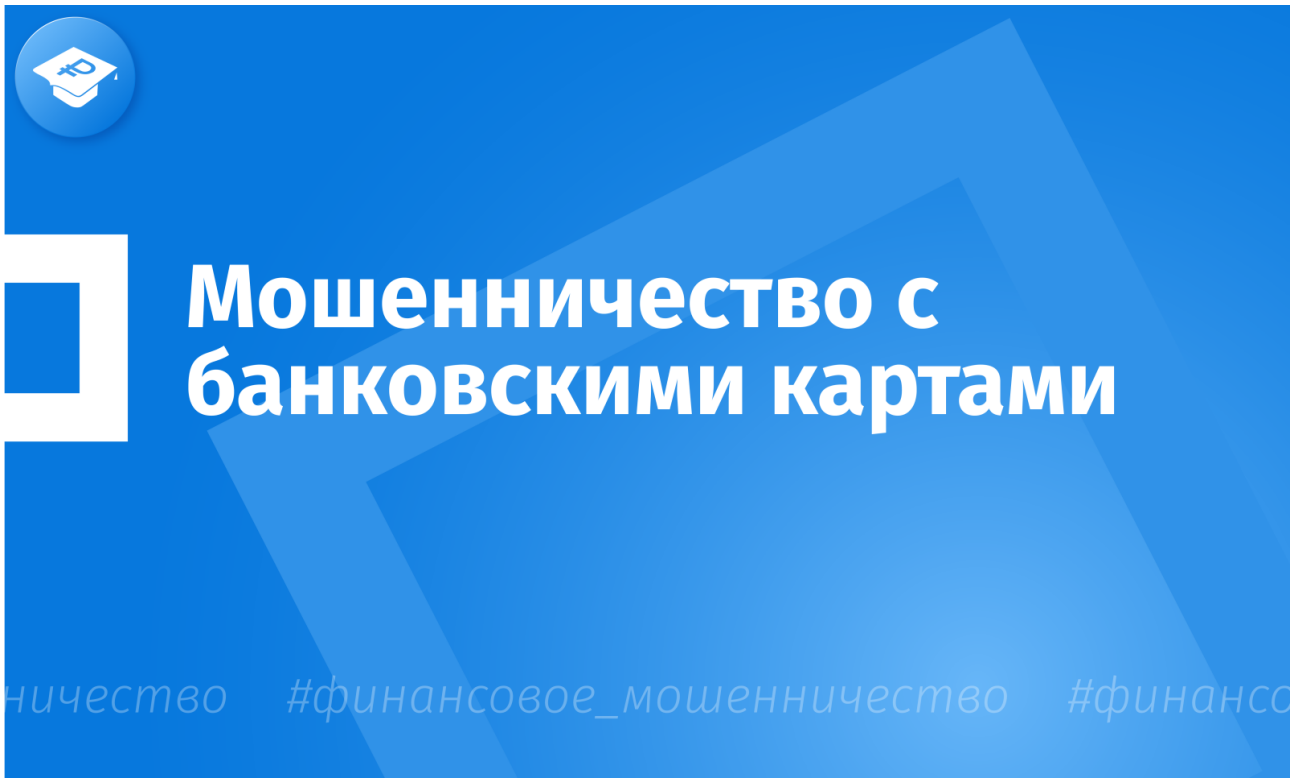
4 АВГУСТА, ЧЕТВЕРГ

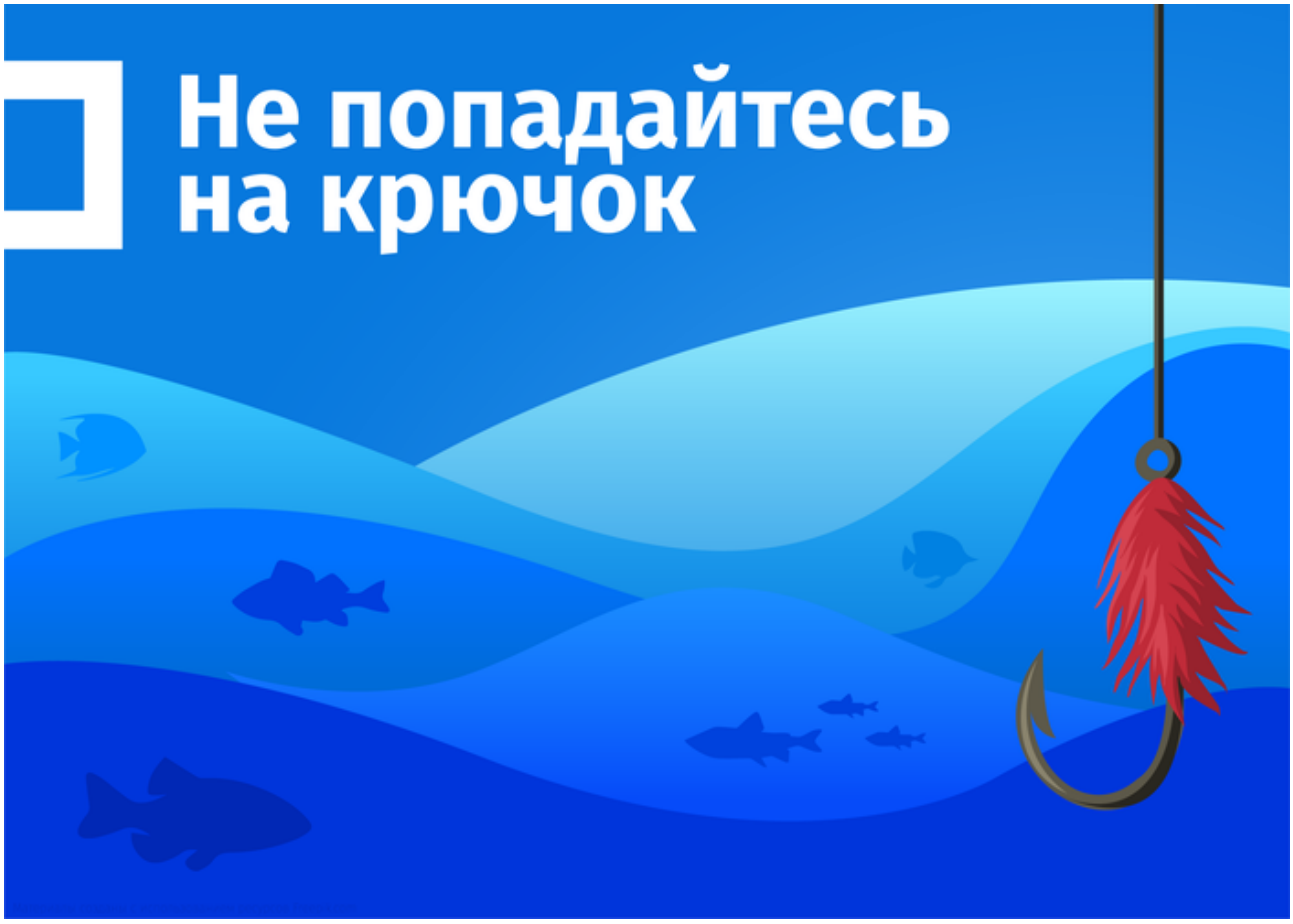
Открытый бюджет города Москвы

Распространенные виды мошеннических схем с банковскими картами в сети Интернет



Мошенничество с банковскими картами в сети Интернет – достаточно распространенный способ хищения денежных средств.

Чаще всего злоумышленники используют такой вид мошенничества, как фишинг (от англ. «phishing», «fishing» - рыбная ловля, выуживание). Это интернет-мошенничество, используемое для кражи конфиденциальных данных.



Мошенники часто:

- рассылают сообщения с вредоносными ссылками, ведущими на копии сайтов известных организаций, банков, интернет-магазинов, социальной сети и т.д. – перейдя по такой ссылке вы попадаете на ресурс, где вас разными приемами пытаются заставить ввести свои учетные данные, реквизиты банковских карт и прочую личную информацию;
- используют вредоносные QR-коды, которые ведут на фишинговые сайты. Они размещаются на поддельных документах (например, квитанциях об оплате ЖКУ), рекламной брошюре у врача или на информационном стикере, висящем в банке, (QR-код, ведущий на безопасный сайт заклеивается другим, который ведет соответственно на фишинговый сайт).

Особенно внимательными надо быть на площадках торговли подержанными товарами!

Выступая в качестве покупателя или продавца, злоумышленник просит продиктовать все данные карты (включая код безопасности CVC/CVV) для перевода денежных средств или направляет ссылку на фишинговый сайт для совершения оплаты, после чего исчезает.

Как обезопасить себя от мошенников в сети Интернет?

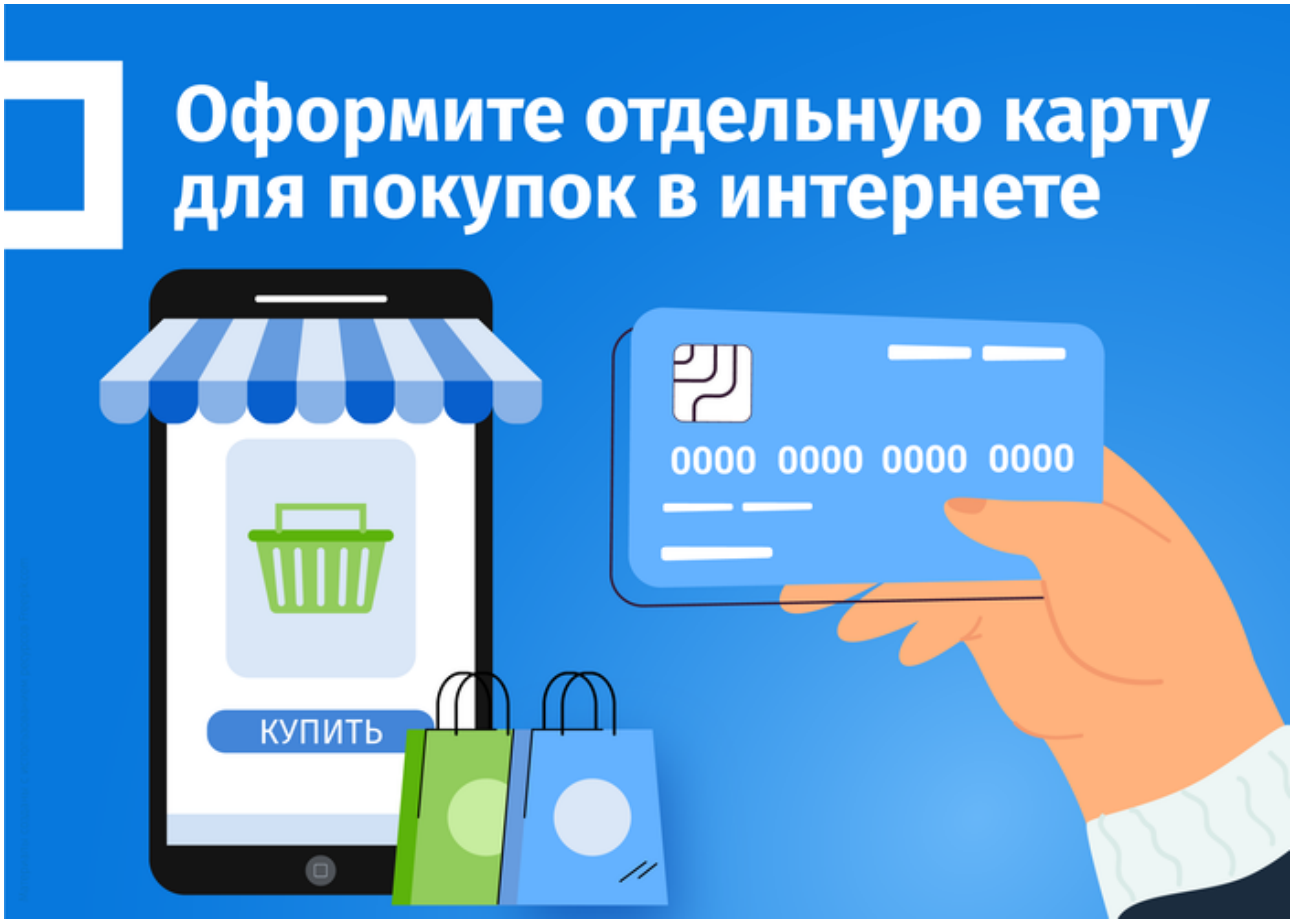
- Внимательно изучайте Интернет-страницу сайта, в том числе адресную строку. Убедитесь, что адрес начинается с букв https:// и рядом стоит значок в виде закрытого замка. Такие Интернет-страницы обеспечивают безопасное соединение, что в большинстве случаев предотвращает утечку персональных данных.

Обратите внимание, что сайты крупных банков в российских поисковых системах

отмечены специальным значком (галочка в синем кружке), который подтверждает, что сайт внесен в список адресов сайтов кредитных организаций. На таких сайтах безопасно проводить операции с денежными средствами!

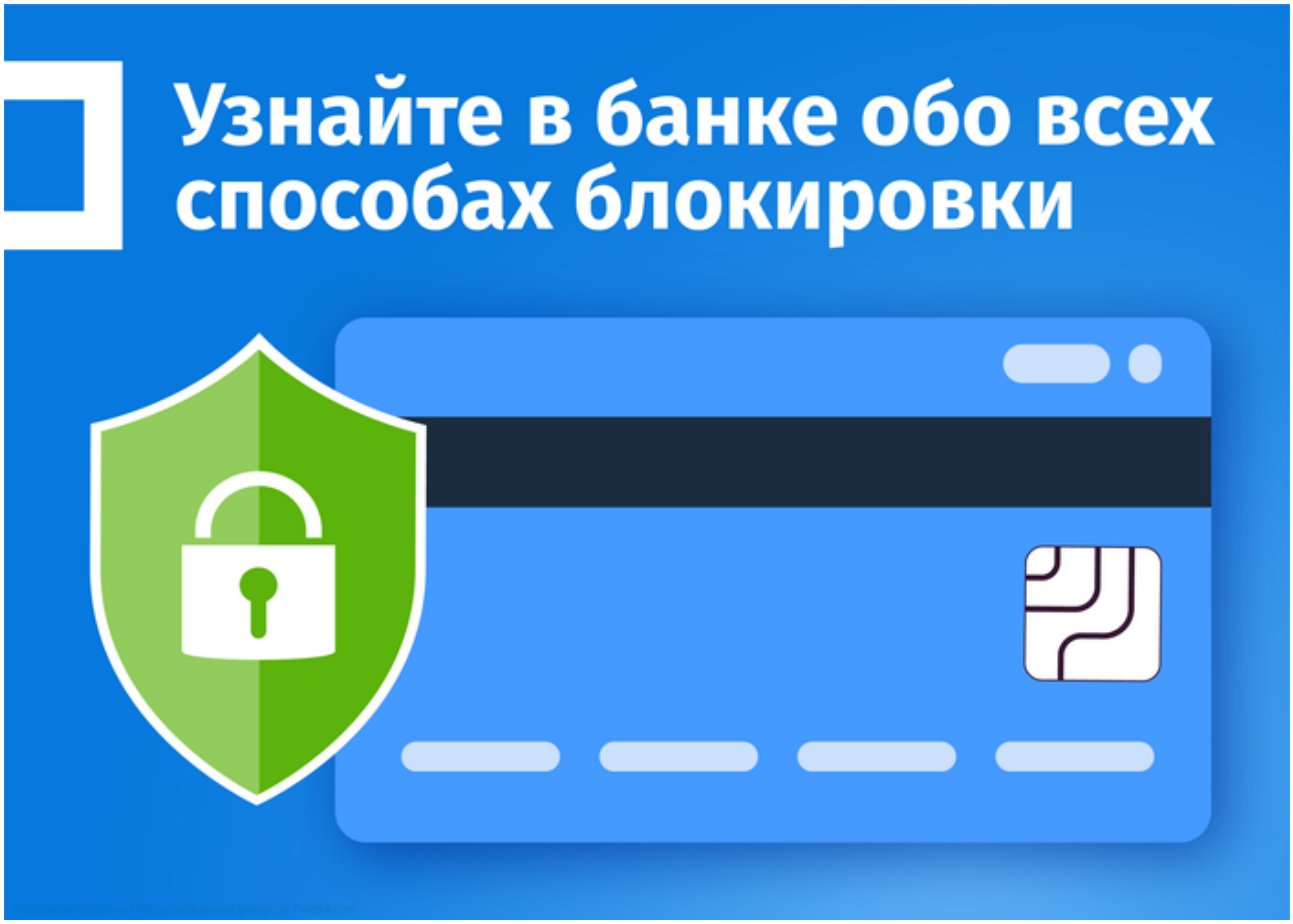
- Не открывайте подозрительные ссылки, даже если они получены от близких и друзей.
- Относитесь с особой осторожностью к рекламным предложениям с большими скидками, розыгрышами и дорогостоящими призами.
- Оформляйте отдельную карту или счет для онлайн-покупок и пополняйте их непосредственно перед совершением оплаты. Такая осторожность поможет сохранить основную часть денежных средств в случае недобросовестных действий.

Кроме того, на карту можно установить лимит или ограничение на покупки в онлайн магазинах. Эту операцию можно совершить в мобильном приложении банка или личном кабинете на сайте банка.



- Не сообщайте секретные коды из смс-сообщений и уведомлений банка. Чаще всего такие коды приходят при попытке оплатить покупку или услуги в Интернете. Иногда подобные сообщения могут прийти, когда покупку вы не совершали. Это означает, что мошенники уже получили частичный доступ к информации о вашей карте.
- Устанавливайте и регулярно обновляйте антивирусные программы. Современные программы для компьютеров и смартфонов проверяют на безопасность не только скачанные файлы, но и Интернет-сайты. Хорошая антивирусная программа подскажет, при работе с какими сайтами следует быть осторожным.
- Внимательно проверяйте реквизиты получателя денежных средств. При оплате с

помощью QR-кода обращайте внимание на реквизиты организации, размер денежной суммы и другие данные на странице, открывшейся после сканирования кода.
- Будьте внимательны с предоплатой. Если сомневаетесь в добросовестности продавца, предложите ему оплатить товар при получении или выслать его наложенным платежом за ваш счет. Проверяйте состав и качество посылки до совершения оплаты.
- Используйте сервисы для проверки сайтов. Проверяйте безопасность сайтов по адресу: https://yandex.ru/safety/, а финансовую организацию – на сайте Центрального Банка Российской Федерации: https://cbr.ru/.



Что делать, если мошенникам удалось получить доступ к карте и списать денежные средства?

- Заблокируйте карту. Сделать это можно, позвонив в банк по телефону «горячей» линии, в личном кабинете на сайте кредитной организации, в мобильном приложении или посетив отделение банка. Некоторые банки предоставляют функцию смс-команд, позволяющих управлять картой или счетом при помощи сообщений. Заранее узнайте в банке все способы блокировки карты. Это позволит оперативно ограничить доступ злоумышленникам к вашим денежным средствам.
- Обратитесь в банк с заявлением о несогласии с операцией. Важно подать его не позднее дня, следующего за днем поступления информации о совершении подозрительной операции по счету. Банк проверит, сообщались ли ПИН-код, код безопасности или срок действия карты посторонним. Банк не компенсирует потери, если Вы нарушили правила безопасности.
- Обратитесь в отделение полиции. Хищение денежных средств – это уголовно

наказуемое деяние. Действия правоохранительных органов помогут быстрее найти злоумышленника.

По материалам портала Правительства Москвы "Открытый бюджет города Москвы": https://budget.mos.ru/