Запомни правила безопасности, чтобы злоумышленники не могли получить доступ к твоей карте.

1. Никому не показывай свой CVV/CVC-код (цифры на обратной стороне карты). С его помощью мошенники могут оплачивать покупки в интернете. Само собой, пин-код тоже храни как зеницу ока.

2. Снимая деньги в банкомате, прикрывай кнопки рукой, когда набираешь пин-код: на панелях могут быть камеры.

3. Если в кафе ты платишь картой, не отдавай ее официанту. Он может списать данные и пользоваться твоей картой в интернете.

4. Подключи мобильный и интернет-банк. Так ты всегда будешь в курсе всех операций по карте.

5. Перед сменой номера телефона не забудь отключить мобильный банк, иначе у нового владельца останется доступ к твоим картам!

Прокуратура города Владимира информирует

о некоторых способах дистанционных мошенничеств

Воображаемый друг

Мошенники могут взломать страничку твоего друга в социальной сети и вступить с тобой в переписку.
Иногда они не сразу просят денег, а пытаются вовлечь в диалог.

Что должно насторожить: «друг» отвечает на твои сообщения, но коротко и неинформативно. Указывает реквизиты карты для перевода.

Что делать: связаться с человеком по другим каналам (смс, телефон, соцсети) и уточнить, действительно ли ему нужны деньги. Задать вопрос, ответ на который знает только твой друг.

Привет из «банка»

По телефону мошенник может представиться сотрудником банка и сообщить о блокировке карты, подозрительной активности на счете или еще каких-нибудь «проблемах».

Что должно насторожить: ты не совершал никаких операций в последнее время. «Сотрудник банка» взволнованно объясняет опасность, старается вызвать быструю реакцию. И главное — спрашивает пароль!

Что делать: никогда не сообщай никому (даже сотруднику банка!) пароли и цифры, напечатанные на обратной стороне карты. Позвони в банк по номеру телефона, указанному на карте, и проверь информацию.

Настойчивый покупатель

Если на твое объявление откликается потенциальный покупатель и сразу просит сообщить реквизиты карты — будь осторожен!

Что должно насторожить: покупатель не хочет сначала посмотреть товар, говорит, что у него мало времени, что он переведет деньги, а потом заедет. Просит полные реквизиты карты, CVV-код.

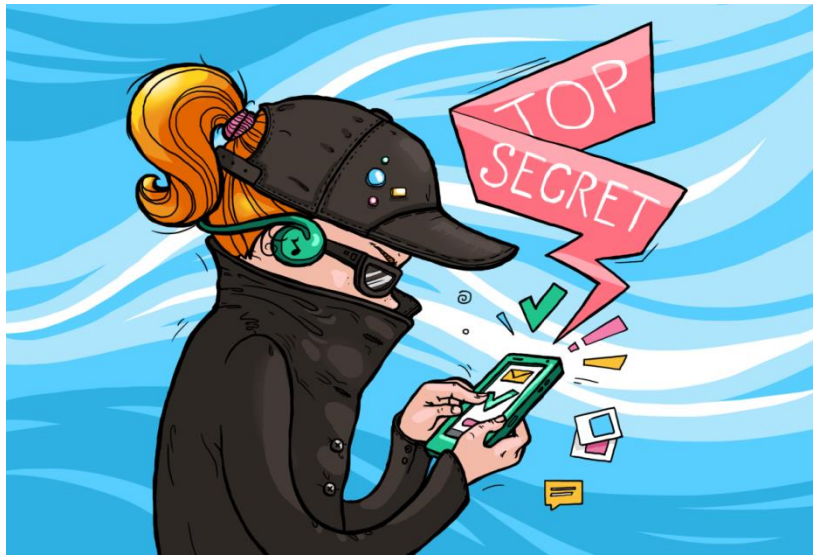
Что делать: запомнить, что для перевода денег с карты на карту нужен только номер карты! Все остальные данные нельзя передавать неизвестным.

Счастливый обладатель

Неожиданное сообщение о том, что ты выиграл приз, тоже должно вызвать подозрения.

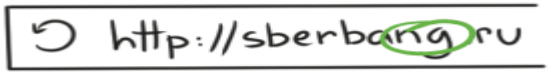
Что должно насторожить: ты не участвовал ни в каких акциях, тебя просят внести предоплату или сообщить реквизиты.

Что делать: если приятные новости требуют от тебя первоначальных вложений, будь уверен: это мошенники. Настоящий работодатель тоже никогда не попросит платить вперед.



Сетевые ловушки

Каждый день в интернете появляется миллион новых сайтов! 15 % из них созданы мошенниками. Ниже — несколько правил, которые помогут тебе обойти эти ловушки.

1. Проверяй название сайта. 

2. Не доверяй порталу с ошибками. Мошенники редко вычитывают собственные тексты, поэтому, если ты видишь на сайте много орфографических ошибок, это повод насторожиться.

3. Не переходи по внешним ссылкам. Увидел рекламу прикольного рюкзака в паблике? Не спеши переходить по ссылке, лучше сделай запрос в поисковике: сайт и название компании.

4. Обрати внимание на домен. Если видишь ресурс со странным доменом (не .ru, .com, .org, а какой-нибудь .tt) или браузер предупреждает тебя, что сайт небезопасен, подумай дважды, стоит ли доверять такому порталу.

5. Плати только через защищенное соединение. Если при оплате ты не видишь пометку Secure Connection — это повод заподозрить неладное.

7. Подумай, прежде чем платить заранее. Покупая товары на сайтах бесплатных объявлений, не переводи деньги с карты на карту заранее. Закажи доставку с оплатой на месте.