Помните!

Во-первых: Не записывайте пин-код на карте или в легкодоступных местах.

Во-вторых: Не передавайте никому реквизиты своей карты. Если конкретнее – номер карты, срок действия, имя и фамилия.

В-третьих: Если расплачиваетесь карточкой в магазине/ресторане/гостинице, не допускайте, чтобы карточка пропадала из виду.

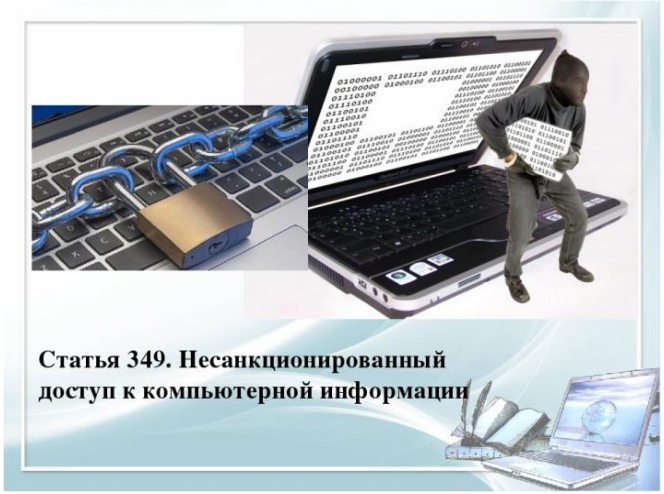
В-четвертых: Никто не должен знать баланс вашей карты. Проверка баланса где-либо - это самая рискованная электронная операция по карте.

В-пятых: Заведите себе отдельную карту для банкоматов и кладите на неё только нужную сумму.

В-шестых: Будьте предельно осторожны с кредитными (на которых есть кредитный лимит) картами.

В-седьмых: Держите в своём мобильном телефоне номер сервисного центра банка, где выдали вам карточку.

Вывод: карту украли – сразу звоним в банк и блокируем.



Государственное учреждение образования «Мядельский учебно-педагогический комплекс ясли-сад – средняя школа»

Памятка по защите от мошеннических действий

Защита информации от несанкционированного доступа

Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Основные функции, которые должны осуществляться программными средствами, это:

1) идентификация субъектов и объектов;

2) разграничение (иногда и полная изоляция) доступа к вычислительным ресурсам и информации;

3) контроль и регистрация действий с информацией и программами.

Наиболее распространенным методом идентификации является парольная идентификация. Однако практика показывает, что парольная защита данных является слабым звеном, так как пароль можно подслушать или подсмотреть, перехватить или просто разгадать.

Осторожно! Мошенничество с банковскими картами

- **«Ваша карта заблокирована», «Соверши платеж».** Подобные СМС-сообщения приходят с неизвестных номеров. При звонке на указанный номер Вас просят указан номер вашей банковской карты, CVC2/CVVC2 или Пин-код карты.
- **Карта попала в чужие руки.** Любой продавец, официант может сфотографировать, переписать данные вашей карты, поэтому необходимо не выпускать из виду вашу карту.
- **Оплата дважды.** При рассете за покупку сообщает об отмене и просит повторно произвести оплату. Спустя какое-то время вы обнаруживаете, что деньги за покупку были списаны дважды.
- **Близнецы – «симки».** Этот спосо используется, когда мошенники уже завладели данными карты и им необходимо при помощи кода из СМС-сообщения подтвердить транзакцию перевода на нужный счет.

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

- хранить в тайне пин-код карты
- прикрывать ладонью клавиатуру при вводе пин-кода
- оформлять отдельную карту для онлайн-покупок
- деньги зачислять только в размере предполагаемой покупки
- использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
- скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его
- подключить услугу "SMS-оповещение"

Не рекомендуется

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

** Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).*

*** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.*

**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*