

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



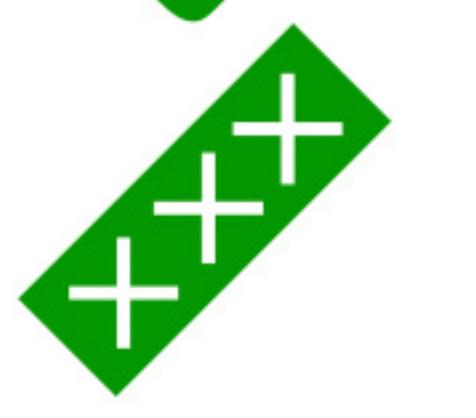
оформлять
отдельную
карту для
онлайн-покупок



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



123 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"



SMS 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.



Источник: МВД Беларуси.

© Инфографика БЕЛТА