Платежная система

Развернуть Скрывать

Пресс-релизы Пресс-центр

30.10.2019

Рекомендации по повышению безопасности при использовании платежной карточки

Рекомендации по безопасному использованию платежной карточки в физической среде

	Управление PIN и другими кодами / паролями	Хранение PIN-кода в секрете, кода CVV2 / CVC2 / CID или любого другого пароля, связанного с использованием платежной карточки — Не сообщайте PIN-код никому, даже членам семьи (никто не имеет права запрашивать PIN-код, код CVV2 / CVC2 / CID или любой другой пароль). — Запомните PIN-код, не записывая его на платежной карточке или на любом другом носителе. — Даже если записали PIN-код, убедитесь, что эта информация хранится в безопасности, отдельно от платежной карты. — Храните конверт с уязвимыми идентификационными данными, полученными из банка в момент получения карточки (PIN, CVV2 / CVC2 / CID) отдельно от карточки, чтобы исключить их одновременное хранение в случае несанкционированного использования. — Вводите PIN-код осторожным способом при совершении платежей в POS-терминалах или при снятии наличных в банкоматах банка, чтобы избежать их мошеннического воспроизведения и использования третьими лицами. — Периодически меняйте PIN-код[1]. — Не используйте комбинацию цифр / общий пароль для доступа ко всем платежным инструментам. — Немедленно свяжитесь с банком и измените PIN-код в случае подозрения относительно несанкционированного владения им другими лицами.
	Применение количественных пределов на ежедневные операции, осуществленные платежной карточкой	— Для предупреждения мошенничества, активизируйте опцию применения количественных пределов для операций, осуществленных посредством платежной карточки. Пределом является максимальным значением операций или максимальное количество операций, которых можно осуществлять ежедневно/еженедельно/за определенный период с платежного счета, к которому прикреплена платежная карточка.
	Применение мер предосторожности при использовании платежной карточки	— Консультируйте регулярно сайт вашего банка для знания мер безопасности при использовании платежной карточки и контактные данные банка в случае необходимости. — В случае утери, кражи или других подозрительных ситуаций незамедлительно информируйте банк и требуйте блокировку карточки. Услуги по поддержке банковских карточек доступны 24/7/365. — Проверьте сумму, указанную на экране POS-терминала/банкомата, до начала сделки.
		— Активируйте услугу SMS- уведомление[2], с помощью которой вы сразу будете уведомлены об операциях, осуществленных с платежной карточкой.

	Активация услуг уведомления об осуществленных сделках	— В случае неудавшейся сделки с помощью платежной карточки, незамедлительно проверьте остаток счета, к которому привязана платежная карточка, просмотрев содержимое полученных уведомлений, или с помощью интернет-банкинга, мобильного банкинга или других средств, предоставленных банком-эмитентом для этого.
	Безопасное хранение/ использование платежной карточки и подтверждающих документов	— Храните карточку в условиях, исключающих ее повреждение, утерю или кражу, или компрометирование введенных на ней данных. — Подпишите карточку на обратной стороне в указанном месте незамедлительно при ее получении. — Не передавайте карточку другим лицам. — Требуйте осуществление операций у торговца/банковской кассы только в своем присутствии, не позволяйте ее фотографирование или ксерокс лицами, не имеющих разрешение на осуществление данных действий, во избежание кражи данных, внесенных на карточку, которые могут быть использованы при осуществлении операций в онлайн-среде. — Избегайте хранить/передавать конфиденциальную информацию посредством телефона, электронной почты и/или другими способами связи через незащищенные каналы. — Требуйте подтверждающие документы или просматривайте полученное уведомление после каждой операции, осуществленной на специальном устройстве (банкомат, POS-терминал) и тщательно проверьте выделенную на нем информацию (число, номер карточки, фамилия/имя, сумма операции, валюта операции). — Храните все подтверждающие документы, связанные с операциями, для их сверки с операциями, указанными в выписке счета.

1. Данная услуга предоставляется банками как в банкоматах, так и посредством автоматизированных систем дистанционного обслуживания (internet-banking, mobile-banking и др.).

2. Данная услуга позволяет получать уведомления на мобильное устройство без подключения к интернету.

Рекомендации для безопасного использования платежной карточки в онлайн-среде

	Проверка безопасности онлайн-торговцев	— Проверьте в рамках электронных торговых платформ наличие символов 3D-Secure (Mastercad SecureCode, VERIFIED by VISA, American Express SafeKey). Они обычно отражены в нижней стороне веб-страницы торговца. — Убедитесь, что сайт торговца защищён наличием логотипа SSL[3] или его адрес начинается с „https://", что обозначает шифрование передаваемой информации; — Никогда не предоставляйте PIN-код, при осуществлении онлайн-операций он не нужен, поэтому ни один онлайн-торговец не вправе требовать его внесение в специальное поле на электронной торговой платформе. — Избегайте использование опции «хранение данных», допускающей возможность осуществления будущих операций без необходимости ввода данных платежной карточки.
		— Избегайте использование публичных сетей Wi-Fi для осуществления онлайн-операций, так как они могут использоваться для захвата передаваемых данных. — Защитите свой компьютер, активируя обновления безопасности, представляемые поставщиками программного обеспечения (как правило, бесплатно) и установите антивирусную программу или программу

	Использование безопасной среды для осуществления платежей	antimalware[4], которая поможет обнаружить мошеннические программы, предназначенные для сбора введенных личных данных, обнаружить сайты, созданные мошенниками для получения конфиденциальных данных и т. д. — Избегайте доступа к подозрительным ссылкам в электронных письмах, социальных сетях, программах мгновенной передачи сообщений, особенно в тех случаях, когда требуется внесение личных данных или информации с карточки. — В случае онлайн-сделок рекомендуем использование виртуальной карточки , на счет которой можете перечислить лишь необходимую для операции сумму. — Храните все подтверждающие документы по осуществленным операциям до окончательного расчета сумм со счета карточки.
	Использование кода CVV2/CVC2/CID и одноразовых паролей	— Не сообщайте никому код CVV2/CVC2/CID или любой другой одноразовый пароль, полученный от вашего банка для авторизации платежа или подключения к системе интернет-банкинга/мобильного банкинга.

---

3. Стандарт безопасности для связи между браузером и сервером.

4. Программа защиты, специально разработанная для противодействия программному обеспечению, предназначенному для проникновения или повреждения информационной системы (компьютера) без согласия владельца.

5. Карточка, позволяющая осуществлять только онлайн-операции, будучи привязанной к отдельному платежному счету. Отсутствие магнитной ленты и чипа не допускают осуществление платежей в физической среде.

Метки
Рекомендации [1]
безопасное использование платежная карточка [2]
платежные карточки [3]

Ссылки по теме:

[1] http://bnm.md/ru/search?hashtags[0]=Рекомендации [2] http://bnm.md/ru/search?hashtags[0]=безопасное использование платежная карточка [3] http://bnm.md/ru/search?hashtags[0]=платежные карточки