ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

Киберпреступления – преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.)

Основные понятия, которые относятся к теме безопасного поведения в сети интернет и описывают виды киберпреступлений

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.). Источник (https://www.oac.gov.by/fighting-telecom-fraud/phishing)

Вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой. Источник (https://www.oac.gov.by/phishing/fighting-telecom-fraud/vishing)

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Преступления в информационной сфере – предусмотренные Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Сваттинг – тактика домогательства, которая реализуется посредством направления ложного вызова той или иной службе. Например, люди сообщают о минированиях, преследуя цель устроить неразбериху и панику в конкретном месте. Источник (https://pravo.by/document/?guid=3871&p0=H10800455)

Смишинг – вид мошенничества (англ. smishing – SMS + phishing), целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения. Смишинг-сообщение обычно имеет схожий внешний вид сообщения от банка, государственного учреждения, оператора электросвязи, известного магазина, а также о внезапном выигрыше в лотерею или акции и т.д. Источник (https://www.oac.gov.by/phishing/fighting-telecom-fraud/smishing)

ПРОФИЛАКТИЧЕСКИЙ МАТЕРИАЛ (https://disk.yandex.by/d/F03-laudj7830g)

Материалы по вопросам кибербезопасности и Рекомендации о том, как не стать жертвой кибермошенников

Материалы с сайта МВД Республики Беларусь (https://www.mvd.gov.by/ru/news/7021)
Киберпреступность в Беларуси (https://belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/)
Как не стать жертвой вишинга (https://belta.by/infographica/view/kak-ne-stat-zhertvoj-vishinga-24468/)
Как не стать жертвой фишинга (https://belta.by/infographica/view/kak-ne-stat-zhertvoj-fishinga-24467/)
Как не стать жертвой интернет-мошенников (https://belta.by/infographica/view/kak-ne-stat-zhertvoj-internet-moshennikov-24466/)
Как не стать жертвой киберпреступника. Защита банковской карточки (https://belta.by/infographica/view/kak-ne-stat-zhertvoj-kiberprestupnika-zaschita-bankovskoj-kartochki-16627/)
Рекомендации о том, как не стать жертвой кибермошенников и информация об уголовной ответственности за киберпреступления (https://belta.by/infographica/view/kak-ne-stat-zhertvoj-kiberprestupnika-zaschita-bankovskoj-kartochki-16627/)

В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

ст.212 «Хищение путем использования компьютерной техники»;
ст.349 «Несанкционированный доступ к компьютерной информации»;
ст.350 «Модификация компьютерной информации»;

ст.351 «Компьютерный саботаж»;
ст.352 «Неправомерное завладение компьютерной информацией»;
ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;
ст.354 «Разработка, использование либо распространение вредоносных программ»;
ст.355 «Нарушение правил эксплуатации компьютерной системы или сети».

Если Вы стали жертвой киберпреступников, обращайтесь в главное управление по противодействию киберпреступности криминальной милиции МВД Беларуси (https://www.mvd.gov.by/ru/page/upravlenie-k)

Telegram канал «Цифровая грамотность». Канал о том, как не стать жертвой мошенников в интернете (https://t.me/s/cifgram)

Приложение 1

Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Защита пожилых людей от мошенников — это постоянный процесс. Чем больше вы будете общаться и информировать их, тем меньше шансов, что они станут жертвами обмана. Мошенники постоянно совершенствуют схемы обмана, поэтому наша задача — не просто предупредить, а научить человека моментально распознавать угрозу.

Лучшая защита — это бдительность и знание простых правил: никаких кодов из СМС, никаких «безопасных счетов», только личный визит в банк и звонки правоохранителям.

Мошенники постоянно придумывают новые способы обмана, и пожилые люди часто поддаются на их уловки. Поговорите с ними о мошенничестве. Объясняйте, какие схемы сейчас популярны и расскажите реальные истории о тех, кто попался на удочку мошенников.

Основные схемы мошенничеств:

«Оператор сотовой связи» и «Белтелеком». В ходе беседы злоумышленник сообщает человеку, что у него заканчивается срок действия договора на оказание услуг. Путем оформления заявки мошенники узнают паспортные данные и склоняют к установке сторонних приложений.

«Обновление кода домофона». Мошенник звонит жертве, представляясь сотрудником управляющей компании, службы безопасности или другой официальной организации. Злоумышленники сообщают, что новый код придет в СМС и его надо сообщить для обновления в системе. Только на самом деле СМС поступает от банка для получения кредитов, где получателями денежных средств являются злоумышленники.

«Водоканал» и «Электросети»: проверка или замена счетчиков. В ходе беседы злоумышленник предлагает человеку оставить заявку на поверку или замену счетчиков. Используя легенду о необходимости заполнения заявки, злоумышленники выманивают конфиденциальные паспортные данные. Следует отметить, что злоумышленники активно используют как мессенджеры, так и домашние телефоны для осуществления указанных схем преступлений.

«Декларирование денежных средств с целью их сохранности». Мошенник убеждает потерпевшего сообщить поступивший из СМС код. Затем поступает второй звонок, где неизвестный угрожает возбуждением

уголовного дел, проведением по месту жительства обыска, в ходе которого все денежные средства будут изъяты и предлагает во избежание этого сбережения передать «курьеру» для декларирования и сохранности. Не единичны случаи, когда в роли курьеров мошенники используют лиц, ранее обманутых аферистами и убеждают в том, что они участвуют в проводимой правоохранительными органами спецоперации.

Необходимо на постоянной основе доводить до сведения населения, особенно пожилым и престарелым, что:

Сотрудники милиции и иных правоохранительных органов никогда не звонят в мессенджерах и не требуют перевода денег для «декларирования» или «освобождения от ответственности»!

Никому нельзя сообщать свои личные данные, данные банковских карт, коды из SMS по телефону, даже если звонящий говорит, что он из банка или другой организации!

Ни при каких обстоятельствах нельзя оформлять кредиты по просьбе третьих лиц и переводить денежные средства на неизвестные банковские «безопасные» счета!

Нельзя открывать электронные письма от незнакомцев и переходить на подозрительные ссылки!

С целью повышения цифровой грамотности населения (в том числе с целью профилактики преступлений в отношении пожилых и престарелых граждан) и профилактики киберпреступлений в Брестской области, функционирует телеграм-канал «КИБЕРКРЕПОСТЬ», администрируемый управлением по противодействию киберпреступности УВД.

В связи с вышеизложенным, с целью охвата всех слоев населения, профилактики киберпреступлений всем работникам рекомендуем подписаться на телеграм-канал «КИБЕРКРЕПОСТЬ», для получения актуальной и оперативной информации о совершаемых киберпреступлениях и способах противодействия таким преступлениям.

Осуществить подписку на вышеуказанный телеграм-канал можно с использованием QR-кода, а также путем введения в поисковую строку мессенджера «Telegram» «КИБЕРКРЕПОСТЬ».

УОПП УВД Брестского облисполкома

ВИШИНГ

НЕ ОТВЕЧАЙ НА ОБМАН!

ПОМНИ:

Звонок от незнакомца — это не всегда важно. Проверяйте информацию, прежде чем доверять или сообщать что-либо.

Вишинг — это вид телефонного мошенничества, при котором злоумышленники выманивают у людей конфиденциальные данные или деньги по телефону.

Они представляются сотрудниками банков, полиции, операторов связи и других организаций, чтобы втереться в доверие и получить доступ к вашим данным.

КАК РАСПОЗНАТЬ ВИШИНГ?

1. **НЕОЖИДАННЫЙ ЗВОНОК**
   Вам звонят сами, хотя вы никуда не обращались. Мошенники выбирают жертв случайно.
2. **ПРЕДСТАВЛЯЮТСЯ СОТРУДНИКАМИ РАЗЛИЧНЫХ СЛУЖБ**
   Представляются сотрудниками банка, милиции, почты и даже поликлиники, чтобы вызвать доверие и оказать давление.
3. **ПРОСЬБА СООБЩИТЬ ДАННЫЕ**
   Просят продиктовать пароли, коды из SMS, данные карт и паспортов или установить приложение.
4. **ДАВЛЕНИЕ И СПЕШКА**
   Говорят, что нужно действовать срочно, иначе будут проблемы, которые повлекут за собой потерю денег.
5. **ЦЕЛЬ — ВАШИ ДАННЫЕ И ДЕНЬГИ**
   Их цель — получить доступ к вашим личным данным и средствам, а также, возможно, похитить вашу информацию или деньги.

КАК ЗАЩИТИТЬСЯ?

- **ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ**
  Перезвоните в организацию по официальному номеру, который найдете сами. Не используйте номера из SMS или сообщений.
- **НЕ СООБЩАЙТЕ ЛИЧНЫЕ ДАННЫЕ**
  Никому и никогда не сообщайте пароли, коды из SMS и данные карт по телефону.
- **ПРЕРВИТЕ РАЗГОВОР**
  Если что-то вызывает сомнение — завершите разговор. Лучше потерять «важный звонок», чем деньги.
- **НЕ ПОДДАВАЙТЕСЬ НА ДАВЛЕНИЕ**
  Мошенники торопят вас специально, чтобы вы не успели проверить информацию и обдумать действия.
- **БУДЬТЕ БДИТЕЛЬНЫ**
  Настоящие сотрудники никогда не запрашивают конфиденциальные данные по телефону.

СТАЛИ ЖЕРТВОЙ ВИШИНГА?
Немедленно смените пароли, заблокируйте карты и обратитесь в банк. Сообщите в милицию по телефону **102**

ФИШИНГ

НЕ КЛЮЙ НА ОБМАН!

Фишинг — это вид интернет-мошенничества, при котором злоумышленники выманивают у людей конфиденциальные данные (пароли, номера карт, логины).

Они маскируются под известные компании, банки или сервисы, чтобы заставить жертву добровольно передать ценную информацию.

ПОМНИ:

Одна ошибка — и ваш аккаунт или деньги в руках мошенников.

КАК РАСПОЗНАТЬ ФИШИНГ?

1 ПОДОЗРИТЕЛЬНЫЕ ССЫЛКИ И ОТПРАВИТЕЛИ

Проверяйте адрес отправителя и ссылки. Даже небольшая ошибка в адресе может быть ловушкой.

2 ЗАПРОС ЛИЧНЫХ ДАННЫХ

Никогда и никому не сообщайте пароли, коды из SMS и данные карты. Настоящие организации этого не требуют.

3 СРОЧНОСТЬ И ДАВЛЕНИЕ

Фразы вроде «срочно», «ваш аккаунт заблокирован» — способ заставить вас потерять бдительность.

4 ОРФОГРАФИЧЕСКИЕ И СТИЛИСТИЧЕСКИЕ ОШИБКИ

Мошенники часто делают ошибки в тексте и оформлении. Будьте внимательны!

КАК ЗАЩИТИТЬСЯ?

ПРОВЕРЯЙТЕ ИСТОЧНИКИ

Заходите на сайты только через официальные адреса и приложения.

ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ

Включите двухфакторную аутентификацию везде, где это возможно.

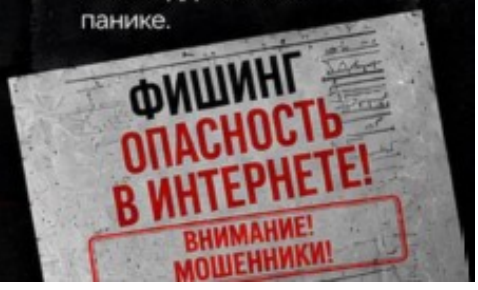
НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ

Не открывайте ссылки из писем и сообщений от неизвестных отправителей.

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ

Перепроверяйте информацию и не поддавайтесь панике.

СТАЛИ ЖЕРТВОЙ ФИШИНГА?
Немедленно смените пароли, заблокируйте карты и обратитесь в банк. Сообщите в милицию.



Соблюдение этих правил и знание того, как действуют мошенники, помогут вам сохранить деньги и спокойствие.

2026

2027

МУС

Как не попасться на удочку телефонных мошенников

или 5 способов сохранить сбережения

ПОПУЛЯРНЫЕ СХЕМЫ

ФАЛЬШИВЫЕ ОБЪЯВЛЕНИЯ

Мошенники размещают объявления на популярных интернет-площадках, в онлайн-магазинах и социальных сетях. Они предлагают товары по заведомо низкой цене, чтобы выманить у вас предоплату, после чего исчезают.

ОБМАН С ICLOUD

Мошенники предлагают бесплатные игры, высокооплачиваемую работу, затем просят войти в чужой iCloud. После этого телефон блокируют и злоумышленники вымогают деньги за разблокировку.

ЗВОНКИ ОТ «СЛУЖБ»

Мошенники представляются сотрудниками государственных органов, банковских учреждений, а также работниками служб связи и жилищно-коммунального хозяйства. Используя методы психологического давления и запугивания, они стремятся:

- выманить SMS-коды и конфиденциальные банковские данные для доступа к личным кабинетам граждан и хищения денежных средств;
- склонить к переводу личных сбережений на подконтрольные им «безопасные» счета;
- вынудить оформить кредит или передать наличные деньги курьерам.

В нашей стране не существует процедуры декларирования денежных средств через перевод их на безопасный счет или передачу третьим лицам.

5 ПРАВИЛ БЕЗОПАСНОСТИ

1. Используйте безопасные платежи. Не переводите предоплату на личные карты продавцов («по номеру телефона»). При покупках на платформах объявлений пользуйтесь встроенной «Безопасной сделкой», где деньги резервируются системой, а не уходят напрямую продавцу до получения товара.

2. Никому не сообщайте коды из SMS, пароли и личные данные. Не переходите по ссылкам из подозрительных писем и сообщений в мессенджерах.

3. Не входите в чужой iCloud и не передавайте доступ к своему устройству третьим лицам.

4. Не верьте звонкам с угрозами, кем бы ни представился собеседник. Немедленно прекратите разговор!

5. Проверяйте информацию только через официальные контакты организаций.

Если вы подозреваете обман — немедленно обращайтесь в милицию по телефону **102**

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

НЕЛЬЗЯ

Хранить пинкод вместе с картой

Сообщать CVV-код или отправлять его фото

Распространять личные данные, логин и пароль доступа к системе «Интернет-банкинг»

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

Сохрани эту информацию и поделись с другими

БЕЗОПАСНЫЙ WI-FI

Рекомендуется:

- отключить общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет;
- использовать надежный пароль для доступа к своей точке Wi-Fi;
- выключить автоматическое подключение своих устройств к точкам Wi-Fi.

ВАЖНО ПОНИМАТЬ,

что многие уязвимости в защите возникают из-за устаревшего ПО, поэтому обязательно установите все последние обновления для своего ноутбука или телефона.

Не рекомендуется:

- доверять открытым точкам Wi-Fi: именно такие сети используют злоумышленники для воровства личных данных пользователей;
- вводить свой логин и пароль доступа к учетной записи или системе банковского обслуживания при подключении к бесплатным точкам Wi-Fi.

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

ФИШИНГ: КАК ЗАЩИТИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ, ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества

Потенциальный покупатель вашего товара предлагает **перейти в мессенджер**, отказываясь общаться непосредственно на торговой площадке.

Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок

Неизвестный в мессенджере присылает **ссылку для перехода на интернет-сайт** под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.

Незнакомец предлагает **передать ему полные данные вашей банковской карты**, включая CVV-код либо логин и пароль от вашего интернет-банкинга.

ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ МВД Беларуси

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ 01

НЕОБХОДИМО:

+ Создавать персональные (уникальные) пароли к разным сервисам
+ Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
+ Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

× Использовать повторения символов
× Хранить пароли на бумажных носителях
× Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
× Сохранять пароль автоматически в браузере
× Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

+ Отключить общий доступ к своей Wi-Fi точке, даже если у вас безлимитный Интернет
+ Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
+ Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

× Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ 03

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ МВД Беларуси

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 04

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
+ Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

× Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники

× Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

+ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
+ Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

× Размещать персональную и контактную информацию о себе в открытом доступе

× Использовать указание геолокации на фото в постах

× Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса

× Употреблять ненормативную лексику при общении

× Устанавливать приложения с низким рейтингом и отрицательными отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ 06

+ Хранить в тайне пин-код карты
+ Прикрывать ладонью клавиатуру при вводе пин-кода
+ Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
+ 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

× Хранить пин-код вместе с карточкой / на карточке

× Сообщать CVV-код или отправлять его фото

× Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), логин и пароль доступа к системе «Интернет-банкинг»

× Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.


ЛЮБАЯ
ИНФОРМАЦИЯ
ДОЛЖНА БЫТЬ
ПРОВЕРЕНА
УВД БРЕСТСКОГО ОБЛИСПОЛКОМА
АЛЛО, МАМ!


ЛЮБАЯ
ИНФОРМАЦИЯ
ДОЛЖНА БЫТЬ
ПРОВЕРЕНА
УВД БРЕСТСКОГО ОБЛИСПОЛКОМА
АЛЛО, МАМ!


ЛЮБАЯ
ИНФОРМАЦИЯ
ДОЛЖНА БЫТЬ
ПРОВЕРЕНА
УВД БРЕСТСКОГО ОБЛИСПОЛКОМА
АЛЛО, МАМ!


ЛЮБАЯ
ИНФОРМАЦИЯ
ДОЛЖНА БЫТЬ
ПРОВЕРЕНА
УВД БРЕСТСКОГО ОБЛИСПОЛКОМА
АЛЛО, МАМ!