УВД Оршанского райисполкома информирует:

! ВНИМАНИЕ МОШЕННИКИ

В социальных сетях участились случаи выманивания реквизитов банковских карт, логинов и паролей М-банкинга, Интернет-банкинга с последующим хищение денег со счетов граждан.

ПОМНИТЕ!

- НЕ ФОТОГРАФИРУЙТЕ РЕКВИЗИТЫ СВОИХ БАНКОВСКИХ КАРТ
- НЕ ПЕРЕДАВАЙТЕ РЕКВИЗИТЫ СВОИХ БАНКОВСКИХ КАРТ В СОЦИАЛЬНЫХ СЕТЯХ
- НЕ ПЕРЕДАВАЙТЕ СВЕДЕНИЯ О СВОЕМ ИНТЕРНЕТ – БАНКИНГЕ

*В целях обеспечения сохранности Ваших денег напоминаем: реквизиты Вашей банковской карточки – **это секретная информация.** Человек, который ею владеет, имеет полный доступ к Вашим счетам.*

Управление внутренних дел Оршанского райисполкома убедительно просит ни при каких обстоятельствах **не высылать сведения о реквизитах Ваших банковских карточек, а также логинах, паролях, одноразовых кодах доступа, сеансовых ключах к Интернет-банкингу и мобильным приложениям в ответ на сообщения в социальных сетях, поступивших от родственников, друзей и знакомых.**

Под их видом могут скрываться преступники, которые мошенническим путем получили доступ к профилям в социальных сетях.

Будьте бдительны!

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.

Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь

ВНИМАНИЕ!

БЕРЕГИТЕ СВОИ ДЕНЬГИ

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!

Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...

... в котором говорится, что банковская карта заблокирована и предлагается разблокировать ее, пройдя по ссылке...

... ни в коем случае не переходите по ссылке! Незамедлительно обращайтесь в службу безопасности банка!

Если вы получили сообщение о блокировке банковской карты:

- не переходите по прикрепленной ссылке;
- никуда не пересылайте свои данные;

- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;

- обратитесь в службу безопасности банка.

Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь

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.*

Источник: МВД Беларуси.

БЫТЬ ХАКЕРОМ: не развлечение, а преступление!

Уголовная ответственность за киберпреступления наступает:

Статья 212 УК Беларуси — с 14 лет

Хищение путем использования компьютерной техники или введения в компьютерную систему ложной информации наказывается вплоть до лишения свободы на срок **до 3 лет**.

Те же действия, совершенные **повторно или группой лиц по предварительному сговору**, наказываются лишением свободы на срок **до 5 лет**.

Если **хищение крупное**, то предусмотрено наказание в виде лишения свободы на срок **до 7 лет**.

За хищение, совершенное **организованной группой или в особо крупном размере**, грозит **до 12 лет** лишения свободы.

Статья 349 УК Беларуси — с 16 лет

Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, наказывается вплоть до лишения свободы на срок **до 2 лет**.

За несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные **тяжкие последствия**, грозит наказание вплоть до лишения свободы на срок **до 7 лет**.

Управление информации и общественных связей МВД Республики Беларусь