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.*

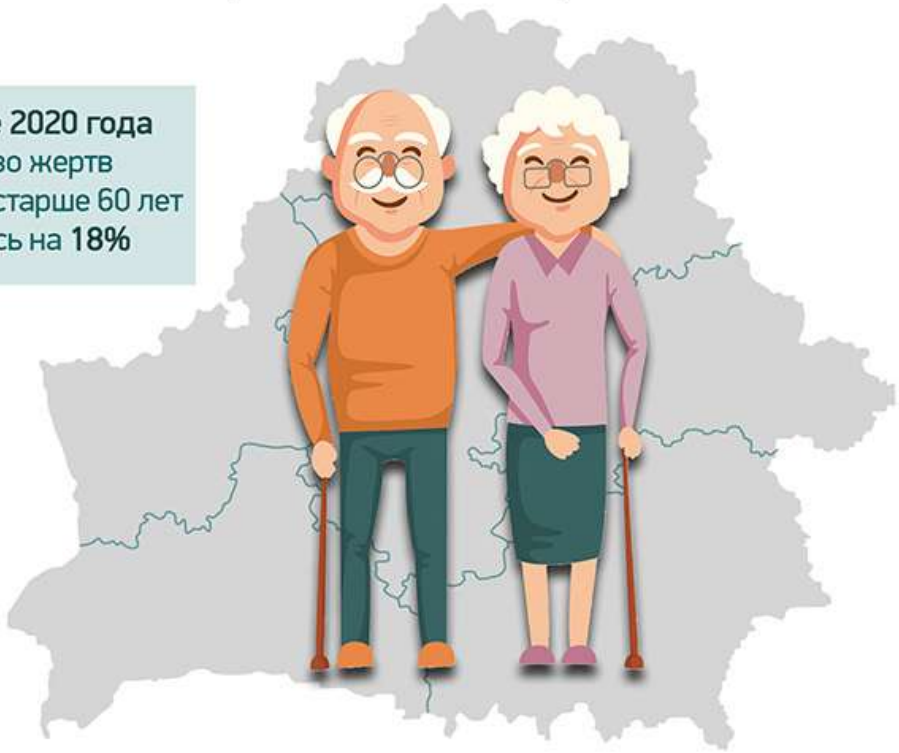
**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*

Источник: МВД Беларуси.

ЗАЩИТИМ ПОЖИЛЫХ ЛЮДЕЙ ОТ ПРЕСТУПНИКОВ

В МВД Беларуси отмечают рост преступлений, совершенных в отношении лиц преклонного возраста: чаще всего это кражи и мошенничества. Под особым прицелом злоумышленников - одиноко проживающие пенсионеры и пожилые люди с ограниченными возможностями.

В **I квартале 2020 года** количество жертв преступлений старше 60 лет увеличилось на **18%**



Наиболее распространенный способ обмана стариков - посещение на дому под видом работников социальных или коммунальных служб, торговли, сотрудников системы здравоохранения, представителей религиозных конфессий.

МВД ПРОСИТ ПОЖИЛЫХ ЛЮДЕЙ, ИХ РОДСТВЕННИКОВ И БЛИЗКИХ В ПОДОБНЫХ СИТУАЦИЯХ СРАЗУ ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ В МИЛИЦИЮ.

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

- ни под каким предлогом не открывайте двери незнакомцам,
- проявите осторожность при общении с незнакомыми людьми,
- по возможности позвоните родственнику или соседу, если же по каким-либо причинам не можете этого сделать, попросите визитеров прийти позже,
- разговаривайте с посетителем на лестничной клетке, возле подъезда, на улице, исключите общение с ним в стенах собственного жилья,
- не передавайте банковские карточки, документы, деньги и ценности незнакомцам,
- запишите на видном месте список телефонов коммунальных, социальных, аварийных служб, своих соседей, а также участкового инспектора милиции и органа внутренних дел.

Источник: Министерство внутренних дел

КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;

никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.