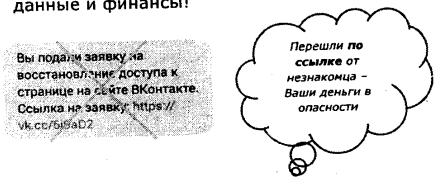
2. Злоумышленники могут создать ***подделку сайта***, похожую на официальный. Когда Вы введете свои данные, они смогут их получить.

https://www.21wek.by – **w вместо v**

https://www.2Ivek.by – **I вместо 1**

https://www.21vek.by – *оригинальный сайт*

3. Перейдя по ссылке от незнакомца ("честные" продавцы), Вы подвергаете опасности свои данные и финансы!



4. Вам может написать якобы сотрудник банка и запросить информацию по Вашей карте. (***ЗАПОМНИТЕ***: банк не будет узнавать Ваши пароли и секретные данные)

5. Установка на Ваше устройство программы-вируса (считывает Ваши данные). Не оставляйте без присмотра Ваши телефоны и гаджеты.

6. ***Сайты-„разводилы"*** предлагают сыграть в игру типа интернет-казино. Сайты направлены исключительно на то, чтобы завладеть Вашими личными данными и денежными средствами.

7. Звонки от "мнимых" сотрудников банка. Мошенник представляется сотрудником банка и просит сказать пароль и другие конфиденциальные данные. Возможен шантаж.

Никому не сообщайте:

- сеансовые пароли (секретные коды, которые приходят к Вам в СМС-сообщениях при входе в системы банка);
- пароль 3-D Secure (секретный код, который придет к Вам в СМС-сообщении на телефон при проведении какого-либо платежа);
- логины и пароли, личные паспортные данные;
- номер вашей банковской платежной карточки, а также срок ее действия;
- ПИН-код (выданный банком секретный код к карточке);
- CVV-код (3 цифры на обратной стороне Вашей карты).

РЕКОМЕНДУЕМ:

✓ Установите лимиты по расходованию средств
✓ Установите информирование о совершаемых операциях (СМС, push-уведомления)
✓ Заведите дополнительную карту для оплаты в интернете
✓ Не разглашайте данные Ваших карт
✓ Имейте бдительность и осторожность при беседе с сотрудниками банка и знакомыми
✓ Не держите в открытом доступе (например, в облачном хранилище) сканы и ксерокопии личных документов
✓ Установите пароль или другой способ аутентификации на своем смартфоне
✓ Будьте бдительны при переходе на незнакомые сайты и тем более при вводе своих личных данных
✓ Пользуйтесь антивирусным программным обеспечением

Будьте зоркими, как орлы!

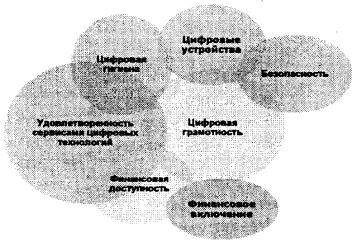
Цифровая грамотность в РБ

С заботой о себе и близких!

НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ БЕЛАРУСЬ

www.nbrb.by

Цифровая грамотность в финансовой сфере – *эффективное и безопасное использование цифровых технологий и ресурсов интернета в рамках совершения финансовых операций*



Цифровая трансформация банков в РБ включает:

- **Дистанционное банковское обслуживание** (*Интернет-Банк, Мобильный-Банк и др.)*
- **Платежные сервисы и приложения**
- **Карточные продукты**
- **Кросс-партнерство**
- **Кибербезопасность** *(защита персональных данных)*
- **Биометрия** *(распознавание) для контроля доступа к информации*
- **Использование платформ искусственного интеллекта**
- **Робоэдвайзинг**
- **Аналитика** *персонального подбора услуг* **под клиента**
- **Смарт-контракты**
- **Удаленная идентификация**

Возможности дистанционного банковского обслуживания:

- ✓ Пользование услугами банка не выходя из дома **24** часа **7** дней в неделю (МСИ, СДБО)
  - *Оформление депозита*
  - *Получение кредита*
  - *Оплата коммунальных услуг и др.*
- ✓ Возможность стать клиентом различных банков удаленно с использованием МСИ
- ✓ Расширение способов оплаты товаров и услуг
- ✓ Сокращение времени проведения платежей, онлайн-выбор банковских услуг
- ✓ Биометрия для контроля доступа к информации, в том числе поведенческая биометрия
- ✓ Расширенная аналитика на основе больших данных в облаке
- ✓ Персональный подбор банковских услуг

Ликбез. Безопасность. Грамотность

Всегда найдутся люди, которые попытаются украсть Ваши данные и получить Ваши деньги

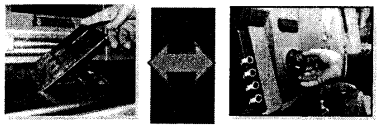
За какими же данными охотятся злоумышленники?

- Сеансовые одноразовые пароли. К ним относятся любые секретные коды, которые приходят к Вам в СМС-сообщениях при входе в системы банка. Завладев ими, можно от Вашего имени совершить финансовые операции. **ВАЖНО:** если Вы передали секретный код, это позволяет изменить данные в Вашем личном кабинете.

НИКОМУ НЕ СООБЩАЙТЕ, ДАЖЕ СОТРУДНИКАМ БАНКА, Ваши сеансовые пароли!

- Реквизиты карты (имея, например, только номер карты и срок ее действия, можно осуществлять покупки в некоторых интернет-магазинах)
- Информация, которую Вы разместили в сети Интернет (фотографии, например, фото авиабилетов; номер телефона; адрес) мошенники могут использовать, в частности, для вымогательства у Вас денежных средств.

Сосредоточьтесь, перед Вами *схемы* обмана!



1. Кража данных карточек (**скимминг** – установка камер и считывающих устройств на банкоматы)