Автор: Администрация
04.06.2021 09:26 - Обновлено 09.09.2021 12:37

Цифровая грамотность



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**

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)

2. Злоумышленники могут создать ***подде*** ***сайта***, похожую на официальный. Когда введете свои данные, они смогут их получи

https://www.21wek.by – **w вместо v**

https://www.2lvek.by – **l вместо 1**

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

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

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

5. Установка на Ваше устройство програм вируса (считывает Ваши данные). оставляйте без присмотра Ваши **телефон гаджеты**.

6. ***Сайты-„разводилы"*** предлагают сыграт игру типа интернет-казино. Сайты направл исключительно на то, чтобы завладеть Ваш личными данными и денежными средствами

7. **Звонки от "мнимых" сотрудников бан** Мошенник представляется сотрудником бан просит сказать пароль и дру конфиденциальные данные. Возможен шант