Цифровая грамотность в Республике Беларусь

НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ БЕЛАРУСЬ

С заботой о себе и близких!

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

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

Включает в себя:

- Цифровые компетенции (личная осведомленность)
- Цифровую безопасность
- Цифровое потребление

Ликбез. Безопасность. Грамотность

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 ряде интернет-магазинов).
- **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*!

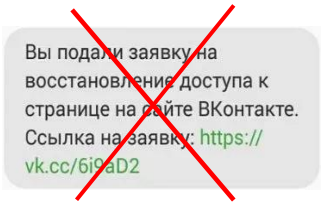
1. Кража данных карточек (скимминг – установка камер и считывающих устройств на банкоматы).

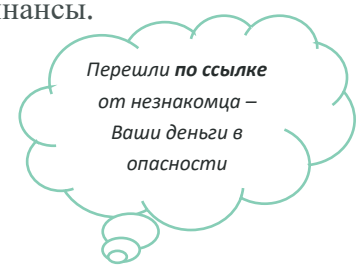

2. Злоумышленники могут создать подделку сайта, идентичную оригинальному. Когда Вы введете свои данные, они смогут их получить.

https://www.21wek.by – **w вместо v**
https://www.2Ivek.by – **I вместо 1**
https://www.21vek.by – ***оригинальный сайт***

Будьте зоркими, как орлы!

3. Перейдя по **ссылке от незнакомца** (”честные“ продавцы), Вы подвергаете опасности свои данные и финансы.





4. Вам может написать/позвонить якобы сотрудник банка и запросить информацию по вашей карте, возможен шантаж (***ЗАПОМНИТЕ:*** банк никогда не будет запрашивать Ваши пароли и другие секретные данные).

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

6. **Сайты-”разводилы “** – предлагают сыграть в игру типа интернет-казино. Сайты направлены исключительно на то, чтобы завладеть Вашими денежными средствами.

7. Передача телефона третьим лицам.

Под предлогом совершения звонка злоумышленник просит смартфон, устанавливает на нем программное обеспечение (регистрируется в интернет- или мобильном банкинге, получает доступ для совершения операций в системе расчетов с использованием электронных денег и т.п.), посредством которого осуществляет переводы денежных средств (электронных денег).

ПРОСТЫЕ СОВЕТЫ:

НИ ПОД КАКИМ ПРЕДЛОГОМ НИКОМУ НЕ СООБЩАЙТЕ:

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

Меры безопасности:

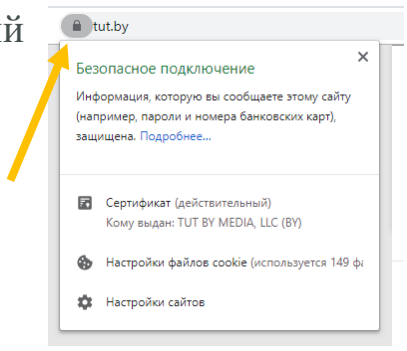
- ✓ Установите лимиты по расходованию средств
- ✓ Заведите дополнительную карту для оплаты в интернете
- ✓ Не разглашайте в интернете данные Ваших карт
- ✓ Имейте бдительность и осторожность при беседе с сотрудниками банка и знакомыми
- ✓ Не держите в открытом доступе (например, в облачном хранилище) сканы и ксерокопии личных документов
- ✓ Установите пароль или другой способ идентификации на своем смартфоне
- ✓ Не передавайте кому-либо свои карточки в пунктах оплаты
- ✓ Игнорируйте и тем более не вводите свои данные на незнакомых сайтах
- ✓ Пользуйтесь антивирусным программным обеспечением
- ✓ Установите СМС-оповещения

✓ **НЕ** разглашайте в интернете Ваши личные данные (как один из способов, мошенники взламывают личные страницы и обманным образом узнают данные карточек)

✓ **НЕ** вводите свои данные на незнакомых сайтах

Правила работы в Интернете:

1. Обращайте внимание на корректность написания адреса сайта.
2. Внимательно присматривайтесь к написанию сайта и к существованию специального “Замочка”, обозначающего защищенное соединение.
3. Открытый или перечеркнутый ЗАМОК – **безопасность не подтверждена.**



***Ваша** безопасность – в **Ваших** руках!*