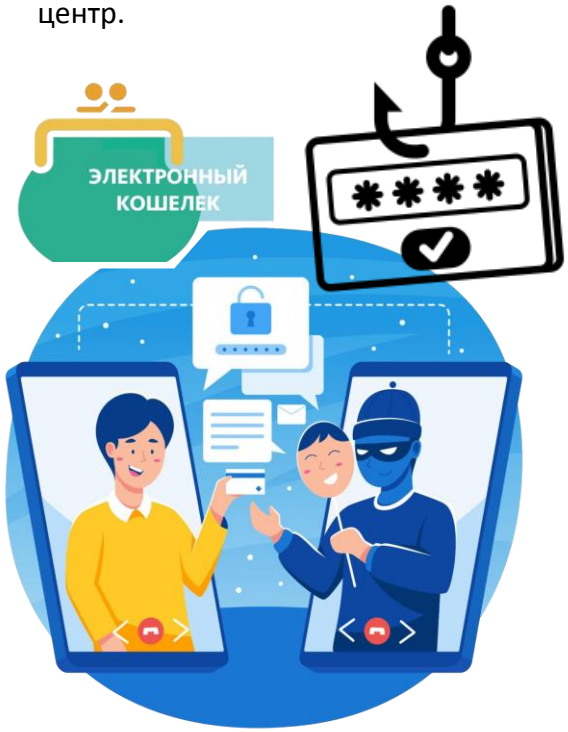
6. **Если вам стали приходить странные смс, похожие на банковские, сразу же звоните в банк.**

Сообщение может выглядеть так: «Подтвердите перевод на 1000 рублей. Код доступа - 56854». Если вы не инициировали эту операцию, значит, кто-то подобрал пароль к онлайн-банку и пытается вывести деньги с вашего счета. Главное - звонить по официальному номеру банка, указанному на оборотной стороне карты, а не по тому номеру, который указан в сообщении;

7. **Если вы поняли, что потеряли карту или что данные вашей карты могли попасть к мошенникам, лучше не искушать судьбу и заблокировать карту.**

Это можно сделать либо в мобильном приложении банка, либо позвонив в колл-центр.



Часы работы
Библиотеки-филиала № 1:

Пн. - **Пт**.: с **11-00** до **19-00**
Вс.: с **10-00** до **18-00**
Выходной - **суббота**

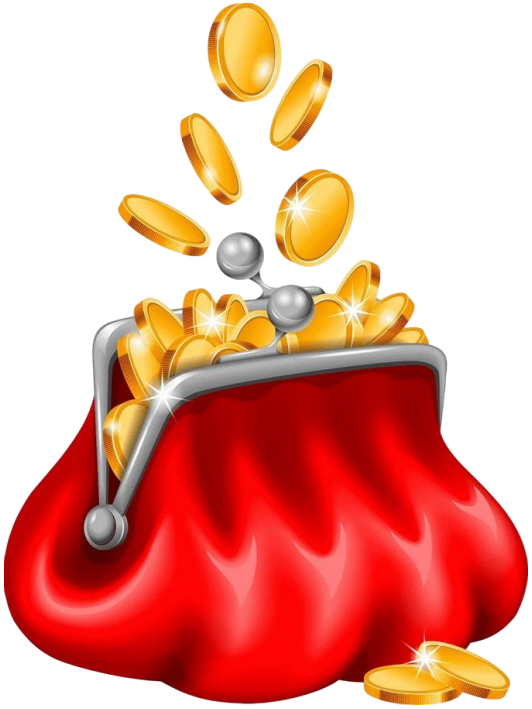
Последний четверг месяца –
санитарный день

Наш адрес:
2а мкр. «Лесников»,
ул. Советская, д. 33
Контактные телефоны:
8(3463) **42-92-28** (доб. **402**#),
8 982 200 08 94

Libraryf5@mail.ru
www.pytyahlib.ru

Составитель:
библиотекарь ЦОД А.А. Любарцева
Оформление: специалист по связям
с общественностью Т.В. Мосунова

Муниципальное автономное учреждение культуры
«Многофункциональный культурный центр «Феникс»
Библиотека-филиал № 1



ЗАЩИТИ СВОЙ КОШЕЛЁК!

Финансовая безопасность

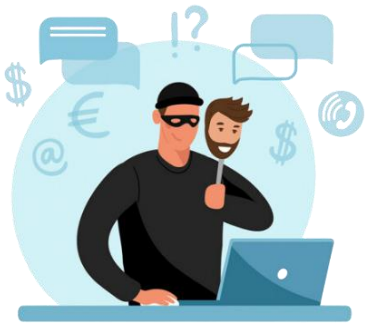
буклет

Пыть-Ях
2025

12+

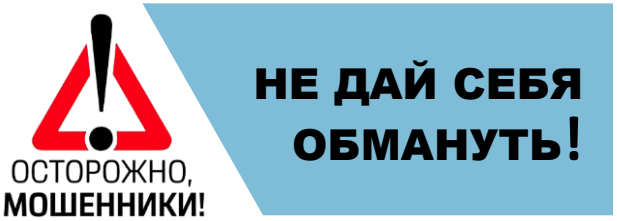
В настоящее время трудно представить современного человека без применения цифровых финансовых технологий.

Финансовая грамотность - крайне важный навык для любого человека вне зависимости от возраста. Мошенники находят всё новые и новые уловки, чтобы ввести в заблуждение владельцев карт. Необходимо знать о способах сохранения и приумножения денежных средств. Как сохранить свои деньги? Как не попасть в ловушку мошенников? Запомните простые правила защиты от злоумышленников.



Правила «О мерах безопасного использования банковских карт»:

- Мошенники имеют техническую возможность имитировать телефонные номера банков. Банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не выспрашивают конфиденциальные сведения и коды, связанные с картами клиентов;
- Храните Пин-код отдельно от карты;
- Не оставляйте карту без присмотра;
- Прикрывайте рукой клавиатуру при вводе Пин-кода как в банкомате, так и при оплате картой в магазине. Помните, что в случае раскрытия Пин, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц;
- В случае, если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом;
- Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в банк по телефону, указанному на банкомате, и далее следовать инструкциям сотрудника банка;
- Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах;
- Будьте внимательны к условиям хранения и использования банковской карты. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.



Соблюдение рекомендаций позволит обеспечить максимальную сохранность банковской карты и реквизитов. ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате.

Пошаговая инструкция по защите банковской карты:

1. **Не сообщайте никому постороннему секретные данные вашей карты: CVV (три цифры на обороте) и пин-код.**

   Единственное, что могут спрашивать у вас сотрудники колл-центра, - это кодовое слово. Но это происходит лишь в том случае, если вы звоните в банк, а не наоборот;

2. **Оставляйте как можно меньше личной финансовой информации в интернете.**

   Не публикуйте в социальных сетях фото банковской карты или сканы документов. Желательно даже не упоминать, клиентом какого банка вы являетесь;

3. **Установите двухфакторную идентификацию.**

   Чтобы при заходе в онлайн-банк и проведении операций нужно было не только ввести постоянный пароль, но и подтвердить свое решение одноразовым паролем, который приходит по смс;

4. **Не переходите по подозрительным ссылкам.**

   Иначе можно скачать себе вирус, который передаст все финансовые сведения мошенникам;

5. **Используйте сложные пароли.**

   Желательно, чтобы они были разными для разных устройств и ресурсов. Плюс желательно время от времени менять их;