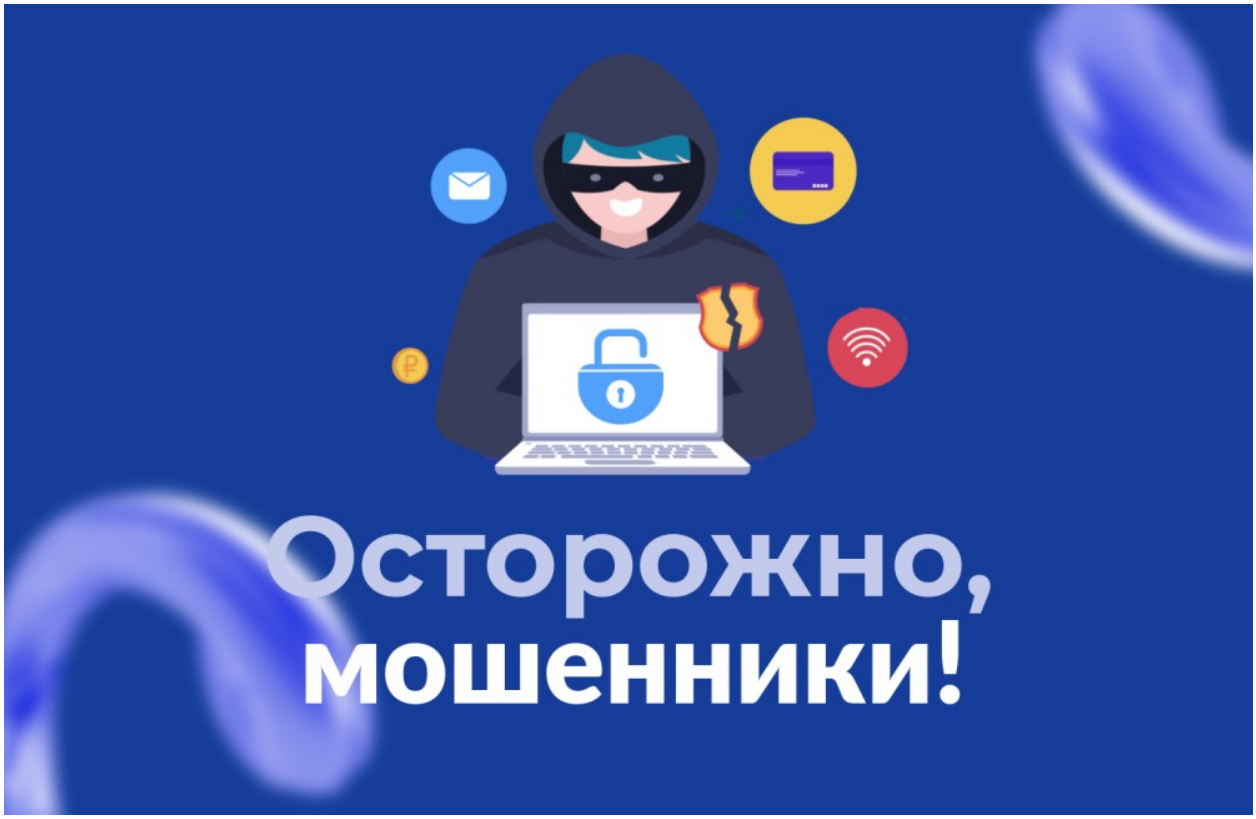
ТОП-5 онлайн-инструментов для защиты сбережений от финансового мошенничества



Несмотря на сложность полного устранения финансового мошенничества, существующие меры противодействия позволяют существенно снизить риски. Рекомендации по защите личных финансов представлены на основе интервью эксперта проекта НИФИ Минфина России «Моифинансы.рф» Ольги Дайнеко, опубликованного в издании «Газета.Ru».

1. **Использование сервисов «самозапретов» (доступны на портале Госуслуг либо через МФЦ).**
   Данные сервисы позволяют установить следующие ограничения:

- самозапрет на кредитование — исключает возможность оформления кредита или займа на имя гражданина третьими лицами;
- запрет на заключение договоров мобильной связи (оформление новых SIM-карт) — предотвращает использование персональных данных для противоправных действий и снимает с гражданина ответственность за возможные финансовые последствия;
- самозапрет на сделки с недвижимостью — не допускает проведение регистрационных действий с объектами недвижимости без личного участия собственника (за исключением случаев наследования, нотариально удостоверенных сделок и регистрации прав на основании судебного решения).

2. **Применение доступных банковских сервисов.**
   К числу эффективных инструментов относятся:

- сервис «второй руки» — позволяет назначить доверенное лицо, которое будет участвовать в подтверждении или отклонении расходных операций в соответствии с перечнем, определённым клиентом. Сервис особенно актуален для лиц, подверженных влиянию методов социальной инженерии;
- настройка параметров банковского счёта — большинство банковских приложений и систем онлайн-банкинга предоставляют возможность установки лимитов (на суточные

расходы, снятие наличных, переводы), запрета на проведение отдельных типов операций (например, онлайн-платежей), а также определения пороговых значений сумм, при превышении которых требуется дополнительное подтверждение. Дополнительно предусмотрена возможность скрытия отдельных счетов и вкладов из общего перечня банковских продуктов в интерфейсе приложения;
- подключение СМС-уведомлений об операциях — обеспечивает оперативный контроль за транзакциями и позволяет своевременно принять меры в случае утраты или хищения банковской карты.

3. **Соблюдение правил цифровой гигиены.**
   Мошенники могут получить доступ к финансовым средствам через взлом личных кабинетов на маркетплейсах, что создаёт риски несанкционированных покупок, вывода средств и оформления кредитных лимитов. Для минимизации рисков рекомендуется:

- не передавать третьим лицам коды из СМС и пуш-уведомлений, а также конфиденциальные данные, обеспечивающие доступ к цифровым кошелькам и виртуальным банковским картам;
- избегать привязки к платёжным инструментам маркетплейсов банковских карт, на которые поступают регулярные денежные средства;
- использовать для онлайн-покупок отдельную банковскую карту, пополняемую непосредственно перед совершением платежа на сумму, соответствующую стоимости приобретаемого товара;
- воздерживаться от проведения финансовых операций через публичные сети доступа к сети Интернет.

4. **Предотвращение попадания в фишинговые ловушки.**
   Для снижения риска компрометации персональных и платёжных данных необходимо:

- отказаться от перехода по подозрительным ссылкам, в том числе содержащим предложения о выгодных распродажах, скидках, высокой доходности либо просьбы о голосовании;
- не осуществлять платежи на неофициальных интернет-площадках;
- устанавливать банковские приложения и платёжные сервисы исключительно из официальных и проверенных источников — это позволяет исключить загрузку вредоносного программного обеспечения, которое может перехватывать уведомления, предоставлять удалённый доступ к устройству либо способствовать утечке конфиденциальных данных.

5. **Использование антивирусного программного обеспечения на пользовательских устройствах.**
   Антивирусные решения позволяют своевременно выявлять угрозы, блокировать несанкционированный доступ к данным (включая сведения финансового характера) и информировать пользователя о потенциальных уязвимостях в системе защиты устройства.

Комплексное применение указанных инструментов в сочетании с соблюдением базовых правил информационной безопасности является эффективным способом минимизации рисков финансового мошенничества.