ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ЦИФРОВАЯ ФИНАНСОВАЯ ГРАМОТНОСТЬ

ЦИФРОВАЯ ЭКОНОМИКА

Цифровая экономика – это деятельность, непосредственно связанная с развитием цифровых компьютерных технологий, в которую входят и сервисы по предоставлению онлайн-услуг, и электронные платежи, и интернет-торговля.

Обычно главными элементами цифровой экономики называют электронную коммерцию, интернет-банкинг, электронные платежи, интернет-рекламу и т.д.

РИСК И ПРОГРЕСС

- **Появились цифровые микроплатежи** - товары и услуги, стоимость которых столь незначительна, что при получении некачественного товара потребитель не видит смысла подавать претензию.

- **Скрытое воздействие маркетинга** - маркетологи придумывают сложные манипулятивные схемы, чтобы покупатели платили больше и покупали ненужные товары.

- **Подростки стали отдельной целевой аудиторией** потребителей финансовых технологий.

ЦИФРОВАЯ ФИНАНСОВАЯ ГРАМОТНОСТЬ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Цифровая финансовая грамотность – это знание и способность уверенно использовать цифровые инструменты для понимания, управления и принятия решений в отношении денег, знание цифровых финансовых продуктов и услуг, наличие цифровых компетенций, умение использовать современные цифровые устройства и приложения, осведомленность о цифровых финансовых рисках.

Она включает в себя:

- ✓ понимание преимуществ и недостатков различных способов сбережения, инвестирования и расходов,
- ✓ изучение вариантов цифровой валюты и использование финансовых технологий,
- ✓ знание прав потребителей и процедур возмещения ущерба, произошедшего в результате цифрового финансового мошенничества.

ПРЕИМУЩЕСТВА КАРТОЧКИ

БАНКОВСКАЯ КАРТОЧКА
КЛЮЧ К ВАШЕМУ
БАНКОВСКОМУ СЧЕТУ

КАЖДЫЙ РЕКВИЗИТ КАРТОЧКИ ИМЕЕТ ЗНАЧЕНИЕ

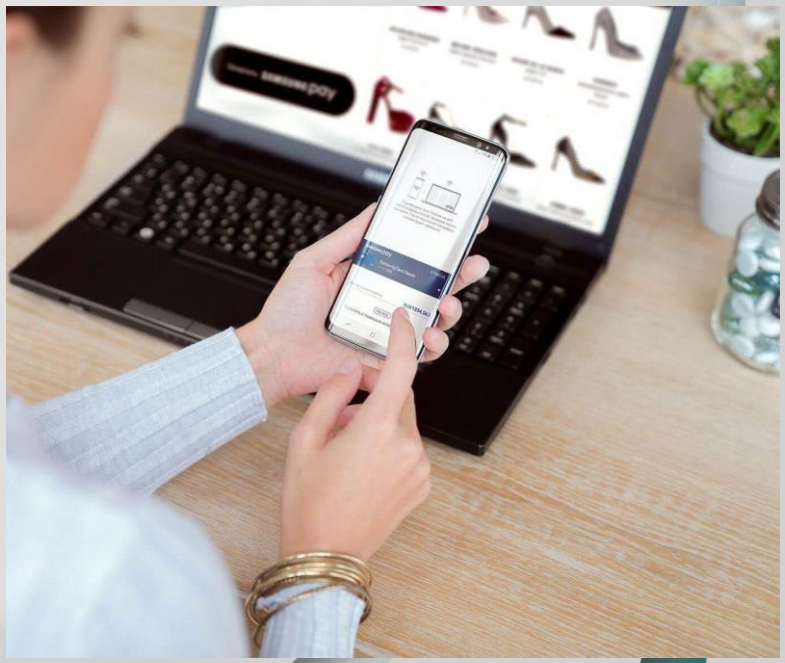
ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ

- Комплекс реквизитов
- Код безопасности
- Коды из смс подтверждений
- ПИН-код

СОХРАНЕНИЕ ДАННЫХ БАНКОВСКОЙ КАРТЫ В ОНЛАЙН-МАГАЗИНАХ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ

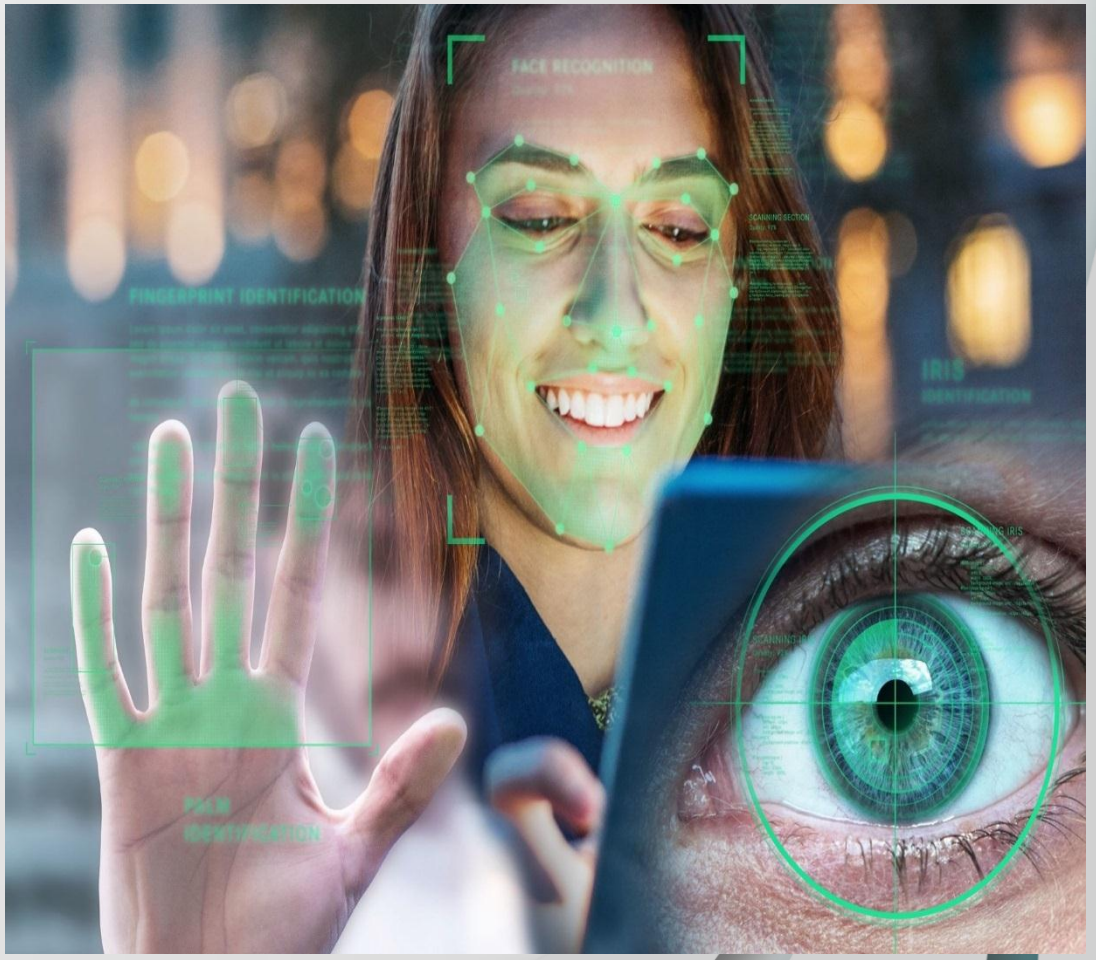
- Не сохраняйте данные вашей банковской карты в личных кабинетах онлайн-магазинов.
- Оставляя компьютер, выходите из личного кабинета в браузер так, чтобы при следующем посещении сайта пришлось бы заново вводить логин и пароль вручную.
- При вводе логина и пароля, следите, чтобы ваши дети, не могли их увидеть.
- Регулярно очищайте «историю» браузера. Не сохраняйте логин и пароль в браузере.



ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Биометрия — это наука, изучающая способы измерения различных параметров человека с целью установления сходства или различия между людьми и выделения одного конкретного человека из множества других людей.

На практике банки по желанию клиента осуществляют сбор биометрических данных - это сведения, характеризующие физиологические особенности человека, на основе которых можно установить его личность: цифровая фотография, отпечатки пальцев, изображение радужной оболочки глаз и иные биометрические персональные данные.



ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Преимущества биометрии
- Универсальность - биометрическими характеристиками обладают все люди
- Уникальность - биометрия является элементом отличающим одного человоека от другого
- Удобство - процесс идентификации на практике прост
- Невозможность подделки
- Стабильность

ВИДЫ ИНТЕРНЕТ – МОШЕННИЧЕСТВА

Термин	Пояснения
Фишинг	мошенническая техника, которая используется для кражи личных данных (например, логина и пароля от электронной почты, номера телефона или данных банковской карты). Сайты, на которых используется фишинг, «притворяются» другими, популярными и известными, сайтами.
Вишинг	идентичен фишингу, с той только разницей, что злоумышленники звонят по телефону, представляясь сотрудниками банка, покупателями товаров и так далее, таким образом пытаясь выманить у держателя PIN-код или заставить его совершить определенные действия со счетом
Претекстинг	атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию узнает конфиденциальную информацию. Эта атака подразумевает должную подготовку, как то: день рождения, ИНН, номер паспорта либо последние цифры счета, для того, чтобы не вызвать подозрений у жертвы. Обычно реализуется через телефон или электронную почту.
Социальная инженерия	наука, которая позволяет найти коммуникации с людьми и выяснить все что вам необходимо. В статье мы раскроем основы этой интересной науки. Согласно статистике и практике взломов высокозащищённых ресурсов в большей мере уязвимость находится со стороны людей, которые в силу непрофессионализма, безответственности или недостатка знаний подвергли сервера атакам.

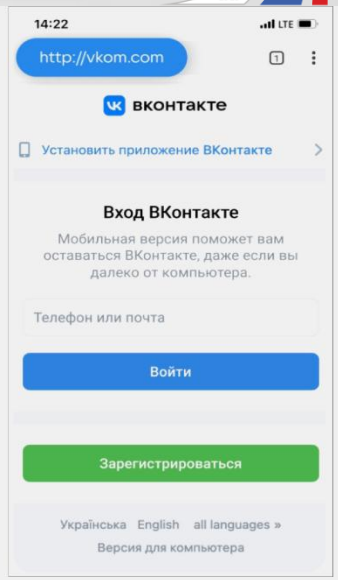
КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

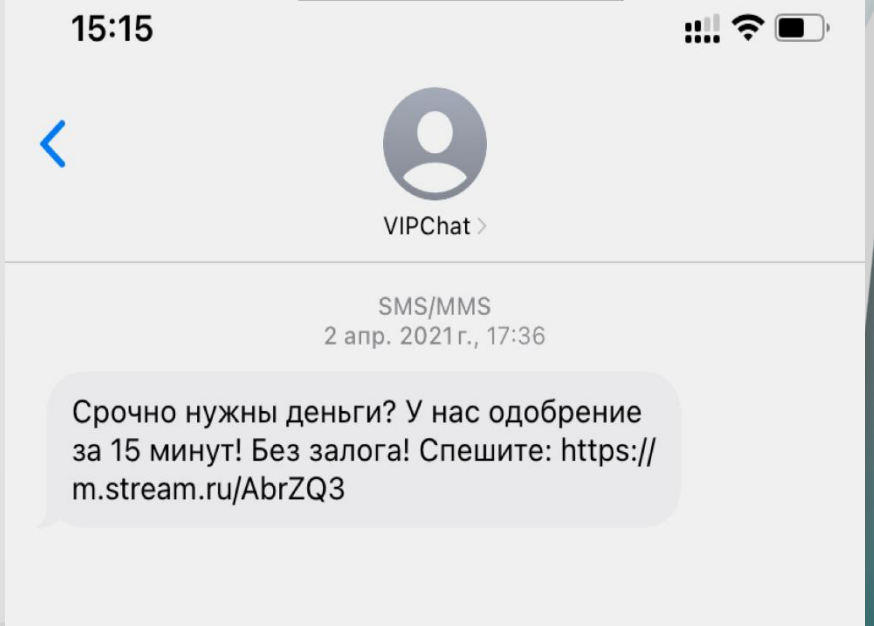
1.Перед тем как ввести платежные реквизиты и пароль, необходимо обратить внимание на начало адресной строки. Поскольку передача сведений происходит по защищенным каналам, в начале адресной строки должны находиться буквы «http://.»

2.Важно внимательно изучить адрес сайта в адресной строке. Ни в коем случае нельзя вводить личные данные на странице сайта, в адресной строке которого изменена хотя бы одна буква

3.Пользователь должен остерегаться перехода по непроверенным рассылкам со взломанных страниц

4.Нужно использовать только проверенные страницы интернет-магазинов. Опасность малоизвестных интернет-магазинов в том, что они не только обманут клиентов с платежной системой, но и просто не вышлют заказанный товар. В результате клиенты лишатся и денег, и покупки.





Основные виды социальной инженерии в эпоху цифровизации

Фишинговые сайты

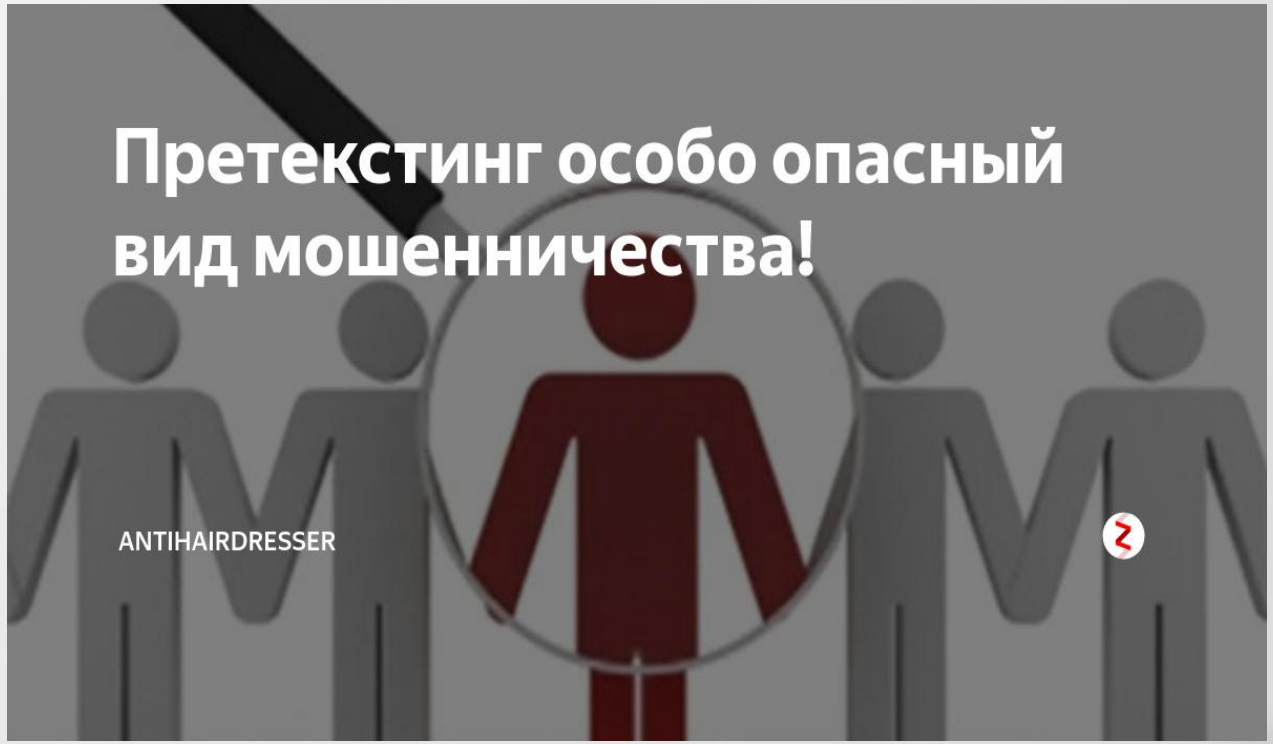
СМС - фишинг

Электронная почта

Фишинг в социальных сетях

ПРЕТЕКСТИНГ

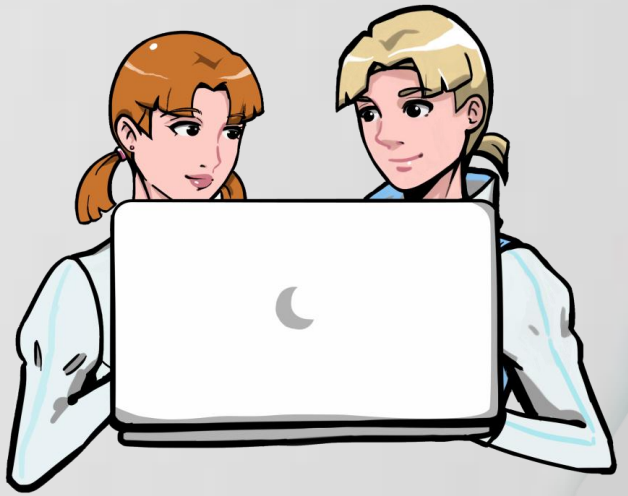
Мошенник озвучивает заранее заготовленный текст со всеми заготовленными психологическими ловушками



«ПРОДАВЦЫ» И «ПОКУПАТЕЛИ»

ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- ...дите переписку только на интернет-площадке
- Не переходите по ссылкам, которые вам высылают
- Проверьте доменное имя сайта
- Обратите внимание на ошибки на сайте

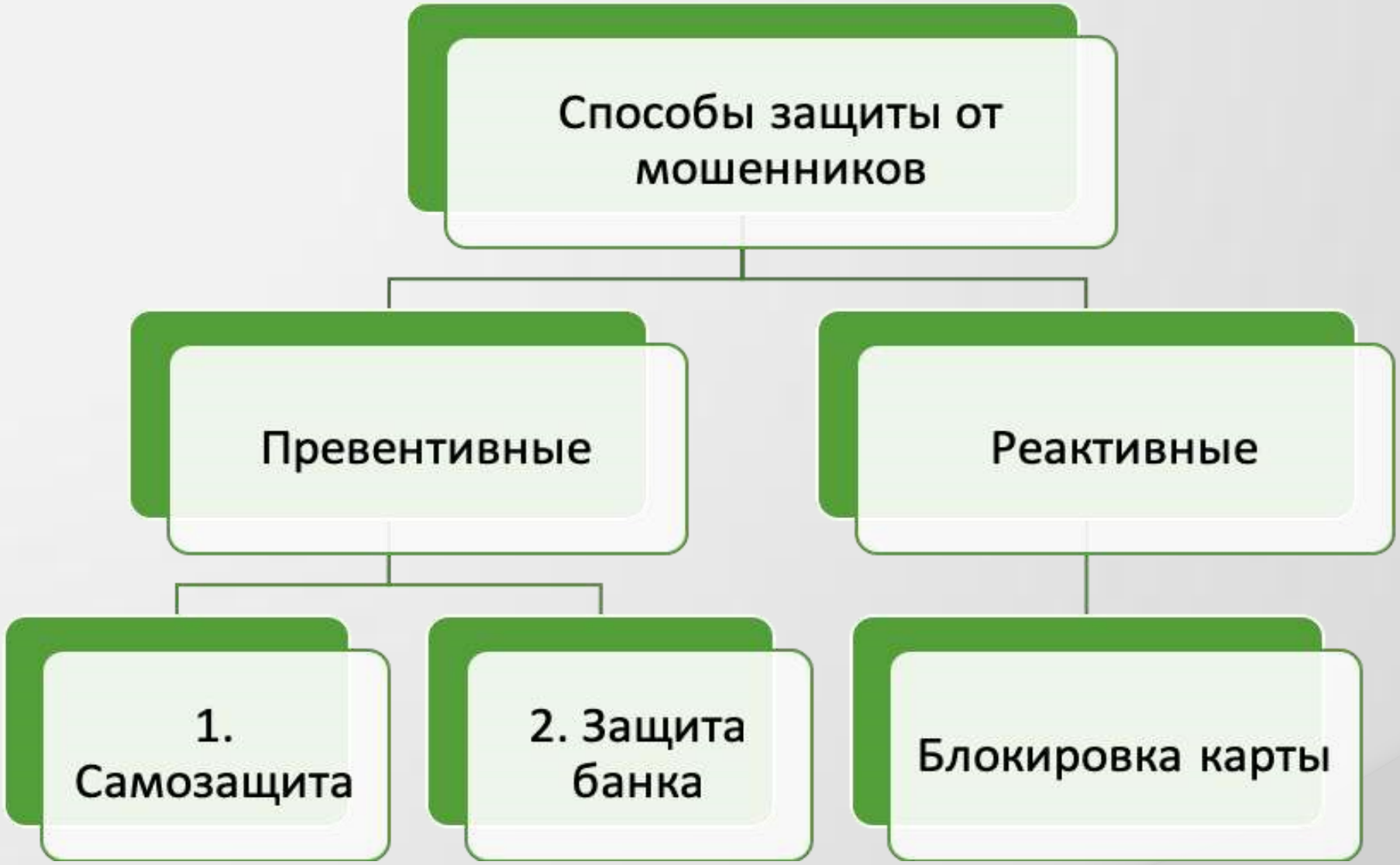


ВЗЛОМ СОЦИАЛЬНЫХ СЕТЕЙ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Свяжитесь с собеседником альтернативным способом
- Используйте сложный пароль
- Не пользуйтесь чужими устройствами
- Пользуйтесь антивирусными программами

СПОСОБЫ ЗАЩИТЫ ОТ МОШЕННИКОВ



ПРЕВЕНТИВНЫЕ МЕРЫ

Собственные действия

- Подключить смс-оповещения об операциях по карте
- Использовать сложные пароли
- Завести специальную карту для интернет-покупок
- Завести бесконтактную карту
- Соблюдать правила безопасности (при работе с банкоматами, терминалами оплаты)
- Записать номер телефона службы поддержки банка в свои контакты
- Оперативно связаться с банком в случае риска мошеннических операций

Действия банков*

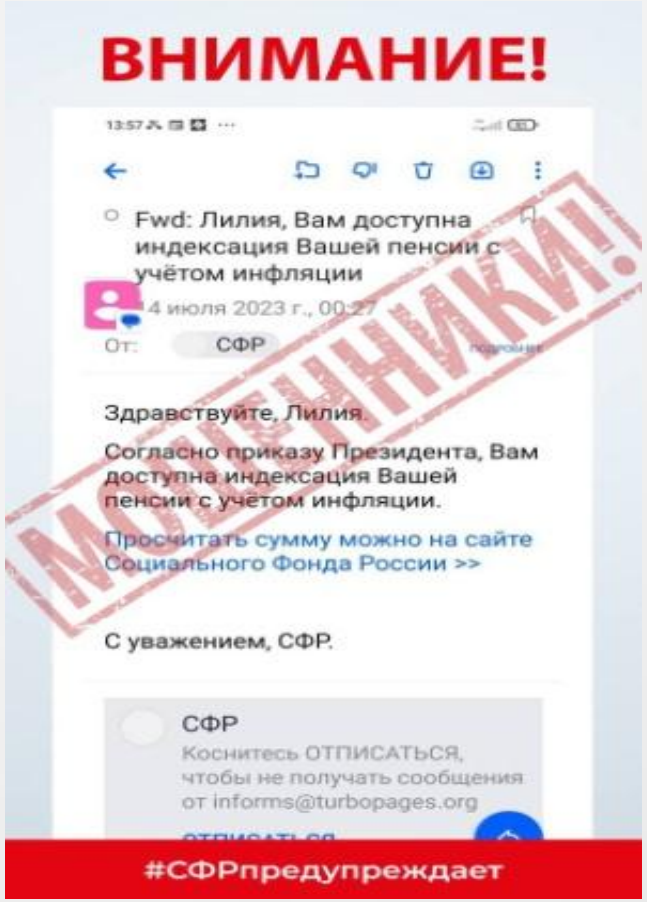
- Блокирование подозрительных операций до связи с клиентом / максимум на 2 дня
- Подтверждение статуса операций у клиента

** обязательны по закону*

РЕАКТИВНЫЕ МЕРЫ

1. Утеря карты 2. Компрометация реквизитов карты	• Немедленно заблокируйте карту (по телефону / в банке)
3. Несанкционированное списание денег с карты	• Заблокируйте операцию (по телефону / в банке)

Фонд пенсионного и социального страхования Российской Федерации (Социальный фонд России)



Если вам позвонили с неизвестного номера и представились сотрудником Социального фонда, то попросите этого человека озвучить свои ФИО, должность и орган СФР, где он работает. Никогда не называйте свои персональные данные: паспорт, СНИЛС, номер банковской карты, пин- и cvc-коды.

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Спасибо за внимание!