Пятый этап Всероссийской просветительской Эстафеты «Мои финансы»

Минфин России

мои финансы

# «Финансовая безопасность для всей семьи»

# РАЗМИНКА

**1** СМС-сообщение говорит о том, что мне необходимо оплатить штраф за нарушение правил парковки на конкретный номер телефона. **Платить или нет?**

**2** Звонок от человека, который представился сотрудником службы безопасности банка и сообщил, что моя карта заблокирована в связи с подозрительной транзакцией. Называл меня по имени и отчеству, упоминал номер карты и просил продиктовать остальные реквизиты «для проверки». **Мои действия?**

**3** При работе в сети Интернет появилось всплывающее окно с приглашением войти в бесплатную онлайн-игру с большими выигрышами. **Что делать?**

**4** Новый для меня интернет-продавец предлагает товар намного дешевле, чем все остальные, и просит 100% предоплату на номер телефона или электронный кошелек. **Мои действия?**

**5** В мессенджере получено сообщение от имени начальства. Руководитель пишет, что в компании произошла утечка данных, поэтому в ближайшее время сотрудникам будут звонить люди из органов, которым нужно оказать содействие. **Что делать?**

# ОПРЕДЕЛЯЕМ СВОЮ ЦИФРОВУЮ ФИНАНСОВУЮ ГРАМОТНОСТЬ

# ПЕРВОЕ ИЗМЕРЕНИЕ —

это базовые знания о современных цифровых финансовых продуктах и услугах

| Продукты | Мои знания (+/-) |
|---|---|
| **Платежи:** электронные деньги, кошельки для мобильных телефонов, криптоактивы, услуги денежных переводов | |
| **Управление активами:** интернет-банкинг, онлайн-брокеры, робо-советники, торговля криптоактивами, управление личными финансами, мобильная торговля | |
| **Альтернативное финансирование:** краудфандинг, одноранговое кредитование (P2P), кредитование онлайн-баланса, финансирование счетов-фактур и цепочки поставок и т. д. | |
| **Прочее:** страховые услуги через Интернет и т. д. | |

# ВТОРОЕ ИЗМЕРЕНИЕ —

это осознание цифровых финансовых рисков

| Продукты | Мои знания (+/-) |
|---|---|
| Фишинг | |
| Фарминг | |
| Шпионское ПО | |
| Замена SIM-карты | |
| Профилирование | |
| Взлом | |

# ТРЕТЬЕ ИЗМЕРЕНИЕ —

это цифровой контроль финансовых рисков, связанный с пониманием того, как можно себя защитить

| Продукты | Мои знания (+/-) |
|---|---|
| Как использовать компьютерные программы и мобильные приложения, чтобы избежать рассылки спама, фишинговых сообщений и т. д.? | |
| Как защитить свой личный идентификационный номер (PIN) и другую личную информацию при использовании финансовых услуг, предоставляемых с помощью цифровых средств? | |

# ЧЕТВЕРТОЕ ИЗМЕРЕНИЕ —

это знание прав потребителей и процедур возмещения ущерба в случаях, когда пользователи становятся жертвами вышеупомянутых рисков

| Продукты | Мои знания (+/-) |
|---|---|
| Понимаете ли вы свои права и знаете ли, куда можно обратиться и как получить компенсацию, если вы стали жертвой мошенничества? | |
| Понимаете ли вы свои права в отношении своих персональных данных? | |

# ФИНАНСОВОЕ МОШЕННИЧЕСТВО

***Финансовое мошенничество*** — совершение противоправных действий в сфере денежного оборота путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения

- Финансовые пирамиды
- Инвестиционные махинации на финансовых рынках
- Кредитные аферы
- Аферы с использованием банковских карт

# КТО ПОДВЕРЖЕН РИСКАМ?

- ✓ Страх потерять близких
- ✓ Боязнь заболеваний
- ✓ Страх потерять деньги
- ✓ Желание помочь семье
- ✓ Отсутствие финансовой подушки безопасности

- ✓ Доверчивость
- ✓ Внушаемость
- ✓ Переоценка своей цифровой и финансовой грамотности
- ✓ Переоценка жизненного опыта

- ✓ Невысокий уровень дохода
- ✓ Стремление к финансовой независимости
- ✓ Азарт
- ✓ Увлеченность онлайн-покупками

# ПСИХОЛОГИЧЕСКИЙ ПОРТРЕТ ЖЕРТВ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Выраженные ценности безопасности

Интересы группы выше собственных

Склонен к сотрудничеству

Возраст 50+

Высокий самоконтроль

# ПРИЕМЫ РАБОТЫ МОШЕННИКОВ С СОПРОТИВЛЕНИЕМ КЛИЕНТОВ

**Пользуясь недостаточным уровнем финансовой грамотности населения, мошенники:**

- ✓ Используют специфическую терминологию
- ✓ Создают иллюзию срочности или безотлагательности конкретных действий
- ✓ Используют угрозы

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

***СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ —***
это совокупность методов и тактик воздействия, основанных на психологическом манипулировании, с целью контроля поведения человека и доступа к конфиденциальной информации

***ОБРАТНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ —***
это техника манипулирования, противоположная классической схеме, при которой преступник первым инициирует контакт. При обратной социальной инженерии человека обманом вынуждают самостоятельно связаться со злоумышленником

# ЭТАПЫ СОЦИОИНЖЕНЕРНЫХ АТАК

**1** Подготовка

**2** Установление контакта

**3** Начало атаки

**4** Отключение

# ПРИЗНАКИ ИСПОЛЬЗОВАНИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

- ✓ Ведение диалога по типу «суфлера»
- ✓ Использование заученных фраз
- ✓ Смена ролей: от представителей кредитных организаций до сотрудников правоохранительных органов
- ✓ Призывы помочь поймать преступников

**Приемы манипуляции:**

- ✓ Образ авторитетного лица
- ✓ Образы попавших в беду близких людей
- ✓ Эффект неожиданности
- ✓ Ограниченность времени для принятия решения
- ✓ Конструкция «или-или»
- ✓ Упоминание только положительных или только отрицательных фактов

# ПРИМЕРЫ ИСКАЖЕНИЙ, КОТОРЫЕ МЕШАЮТ ОБЪЕКТИВНО ОЦЕНИВАТЬ ИНФОРМАЦИЮ

ЭФФЕКТ ТРЕТЬЕГО ЛИЦА

ЭФФЕКТ ОДНОРОДНОСТИ ЧУЖОЙ ГРУППЫ

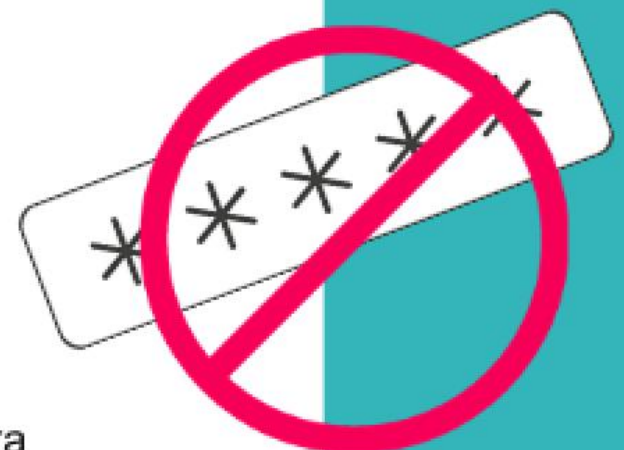
ОШИБКА ВЫЖИВШЕГО

ПРЕДВЗЯТОСТЬ ОПТИМИЗМА

ЭФФЕКТ ЯКОРЯ

# СПОСОБЫ ЗАЩИТЫ ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

- ✓ Не предоставлять личную информацию, если нет уверенности в том, кто ее запрашивает
- ✓ Не раскрывать личную или финансовую информацию в электронной почте, социальных сетях, мессенджерах, не отвечать на подобные сообщения и не переходить по ссылкам из них
- ✓ Не отправлять конфиденциальную информацию через интернет, не проверив безопасность веб-сайта



# УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ

- ✓ Адрес электронной почты
- ✓ Номер телефона
- ✓ Фактический адрес
- ✓ Дата рождения, пол
- ✓ Логин, пароль
- ✓ История покупок в онлайн-магазинах
- ✓ Данные банковских карт

# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

- ✓ Нельзя передавать третьим лицам пароли, коды подтверждения, присылаемые банком
- ✓ Не заходить в свой интернет-банк, соцсети и почту с компьютеров других людей
- ✓ При оплате онлайн-покупок в интернет-магазинах окно для ввода номера карты должно появляться сразу после нажатия кнопки «Оплатить»

# НЕКОТОРЫЕ АКТУАЛЬНЫЕ СХЕМЫ МОШЕННИКОВ

| Схема | Суть | Что делать |
|---|---|---|
| «Пришлите QR-код» | Злоумышленники звонят россиянам под видом сотрудников банка, сообщают, что к ним поступил несанкционированный запрос на снятие денег со счета, и просят прислать QR-код, чтобы отменить операцию, а затем получают по нему средства в банкомате. | Сразу прервать разговор: банки рассылают информацию только через свои официальные каналы. Вы сами можете позвонить в банк. |
| «Одолжишь 50 тысяч рублей до вечера?» | Злоумышленники научились подделывать аудио и видео с помощью нейросетей. Россияне получают в Telegram или во ВКонтакте аудиосообщения и «видеокружочки» от знакомых или родных с просьбой одолжить денег. | Связаться с человеком в другом мессенджере или позвонить ему, чтобы уточнить, действительно ли он обращался к вам с такой просьбой. |
| «Ваше банковское приложение устарело» | Злоумышленники звонят от имени банков с просьбой обновить мобильное приложение, потому что предыдущее скоро перестанет работать. | Как можно быстрее закончить разговор, дождаться, когда уровень адреналина упадет и вернется способность мыслить логически. Банки рассылают информацию только через свои официальные каналы. |
| «Обменяем кешбэк на рубли» | Злоумышленники под видом сотрудников банка звонят россиянам и предлагают обменять накопленный за покупки кешбэк, бонусные баллы или мили на рубли. | Сразу положить трубку и набрать номер горячей линии банка, чтобы прояснить ситуацию — с вероятностью 99,9% это были мошенники. |

# ФИНАНСОВАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОМ МИРЕ

***Цифровая финансовая грамотность*** — способность принимать разумные решения по использованию цифровых финансовых услуг и управлению цифровыми финансовыми активами наиболее экологичным и безопасным способом

# ФИШИНГ, ВИШИНГ, СМИШИНГ, ФАРМИНГ

**ФИШИНГ** (англ. phishing, от fishing – рыбная ловля, выуживание) — вид интернет-мошенничества, направленный на получение доступа к личным данным пользователей

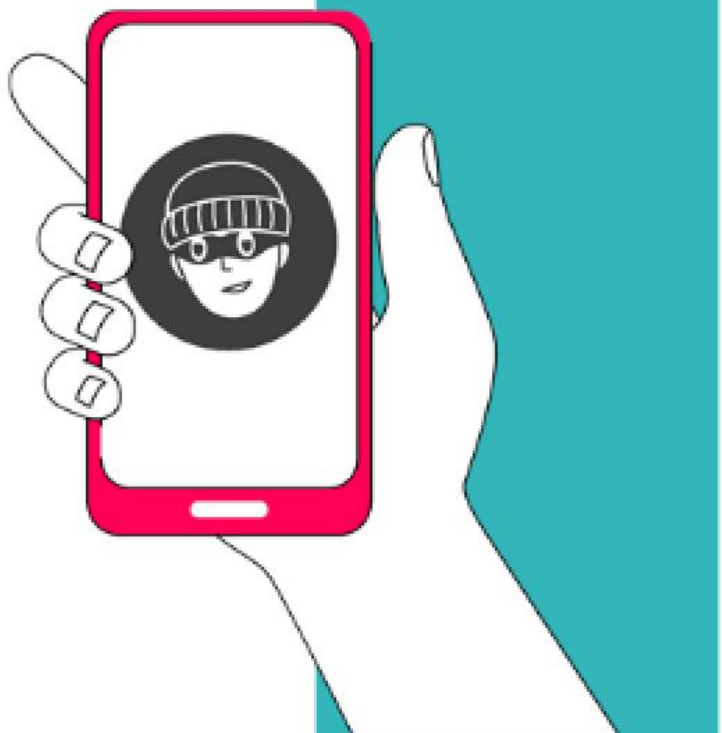
**ВИШИНГ** (англ. vishing – voice+phishing) — разновидность фишинга, при котором используются методы социальной инженерии с помощью телефонного звонка

**СМИШИНГ** (англ. smishing – sms+phishing) — схема, направленная на переход пользователя по вредоносной ссылке из SMS-сообщения

**ФАРМИНГ** (англ. pharming) — вид мошенничества, при котором вредоносный код устанавливается на компьютер или сервер жертвы

# КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА, ВИШИНГА, СМИШИНГА И ФАРМИНГА?

- ✓ Обращать внимание на отправителя и тему сообщения
- ✓ В письме с неизвестным отправителем не стоит переходить по предложенным ссылкам
- ✓ Не отвечать на письма, запрашивающие личную информацию
- ✓ Следить за ошибками в тексте. Если они есть, то, скорее всего, письмо – обман
- ✓ Файлы, прикрепленные к письму, с расширениями .exe, .msi, .bat, .pif, .com, .vbs, .reg, .zip, .apk могут устанавливать вредоносное программное обеспечение



# НАДЕЖНЫЕ ПАРОЛИ

сложные, длинные, нестандартные

Мнемоническая техника:

*Например:* **Люблю грозу в начале мая - Lgvnm_2520**

# СОВРЕМЕННЫЕ СПОСОБЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИИ

***Дипфейк (Deepfake)*** — это фейковый контент, который создают с помощью искусственного интеллекта

FACE-SWAPPING

LIP-SYNCING

FACIAL ATTRIBUTE MANIPULATION

PUPPET MASTER

ENTIRE FACE SYNTHESIS

# СОВРЕМЕННЫЕ СПОСОБЫ МОШЕННИЧЕСТВА — АТАКА С ПОДМЕНОЙ

***Атака с подменой*** — это ситуация, в которой человек или программа успешно подделывает свою личность и выдает себя за другого, чтобы получить доступ к конфиденциальной и засекреченной информации

# СОВРЕМЕННЫЕ СПОСОБЫ МОШЕННИЧЕСТВА – ДРОППИНГ

**ДРОПЫ** ***(дропперы, от английского drop – сбрасывать)*** **—** люди, которых мошенники используют для вывода или обналичивания украденных денег

| | | |
|---|---|---|
| «ДРОПЫ-ОБНАЛЬЩИКИ» | «ДРОПЫ-ТРАНЗИТНИКИ» | «ДРОПЫ-ЗАЛИВЩИКИ» |

# КАК БОРОТЬСЯ С МОШЕННИЧЕСТВОМ?

Обращать внимание, куда вам позвонили

Придумать кодовую фразу в общении с близкими

Проверять номер телефона

Не предоставлять никакую личную информацию

Использовать программы для определения номера

# КАК ЗАЩИТИТЬСЯ ОТ КРЕДИТНОГО МОШЕННИЧЕСТВА?

## ШАГ 1. Проверяйте кредитную историю

- ✓ Бюро кредитных историй

## ШАГ 2. Установите самозапрет на кредиты

**Запрет распространяется на**

- ✓ Банки
- ✓ МФО

**Запрет НЕ распространяется на**

- ✓ Уже полученные кредиты и кредитные карты
- ✓ Ипотеку (обеспечена залогом недвижимого имущества
- ✓ Автокредиты (обеспечены залогом транспортного средства)
- ✓ Основные образовательные кредиты (на оплату обучения, которая сразу перечисляется в образовательную организацию)

# ФИНАНСОВАЯ ГРАМОТНОСТЬ — ЗАЛОГ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ВСЕЙ СЕМЬИ

Рационально выбирает финансовые продукты и услуги?

Понимает права потребителя финансовых услуг и способен отстаивать их?

# Больше полезной информации можно найти на сайте Минфина

## а также на портале моифинансы.рф и в его социальных сетях

# СПАСИБО ЗА ВНИМАНИЕ!