СПРАВКА-ПАМЯТКА
по противодействию современным видам дистанционного мошенничества с использованием технологий искусственного интеллекта (дипфейков) и социальной инженерии

Самое опасное: Мошенничество с использованием дипфейков (Deepfake)

Это технологии, позволяющие подменить лицо и голос человека в режиме реального времени. Преступники создают виртуальную копию вашего знакомого, начальника или родственника.

Схема №1: «Звонок от руководителя».

Сценарий:
Сотрудник получает сообщение в Telegram/WhatsApp якобы от директора компании: «Сейчас тебе позвонят из МВД/ФСБ/Центробанка, окажи полное содействие, это важно для проверки». Следом идет видеозвонок.

Пример:
На экране появляется лицо вашего директора, его голос, мимика, интерьер его кабинета. «Директор» говорит: «Иван, переведи резервные средства на безопасный счет, который продиктует куратор. У нас внеплановая налоговая проверка, я не могу сейчас говорить официально, действуй неформально, отчет пришлю позже. И главное — не распространяйся бухгалтерии, чтобы не создавать панику».

Как это работает: Преступники берут запись с публичного совещания или интервью руководителя и накладывают нужные слова на его голос и артикуляцию.

Схема №2: «Мама, я сбил человека»

Сценарий:
Звонок пожилому человеку с неизвестного номера. В трубке слышен плач и голос, неотличимый от голоса сына/дочери: «Мама, я попал в аварию, меня везут в участок».

Пример:
Голос (с характерными интонациями вашего ребенка): «Мамочка, прости, я сбила пешехода на переходе. Тут полицейский, он готов замять дело за 500 тысяч, иначе меня посадят. Дай ему трубку, он скажет куда везти деньги. Только папе не звони, он меня убьет!».

Техническая деталь: Для создания клона голоса ребенку достаточно прислать в мессенджере короткое голосовое сообщение или записать диалог во время обычного звонка из колл-центра.

ПРАВИЛА ЗАЩИТЫ ОТ ДИПФЕЙКОВ:

1. Стоп-слово. Договоритесь с семьей о секретном слове или вопросе, на который знает ответ только живой человек (например, «Как звали хомяка, который жил у нас 3 года назад?»). Если звонящий ошибается или тянет паузу — это фейк.
2. Искажение лица. Во время видеозвонка попросите собеседника резко повернуть голову в профиль или провести рукой перед лицом. Алгоритмы дипфейков часто сбоят на резких движениях и перекрытии контуров лица (появляются артефакты, размытие).
3. Перепроверка через второй канал. Сразу же перезвоните человеку на его настоящий, старый номер или напишите в мессенджер дублирующий вопрос. Нельзя использовать кнопку «перезвонить» на входящем вызове.

2. Схема «Безопасный счет» (с элементами запугивания)

Классика, которая эволюционировала. Теперь звонят не просто «из банка», а используют гибридные схемы с подделкой документов.

Разбор типичного звонка:
Вы: Алло.
Злоумышленник: (Спокойный, официальный тон) Иван Иванович? Беспокоит старший следователь Главного управления МВД майор Алексеев. Ознакомьтесь: на вас только что оформили доверенность в отделении банка на проспекте Мира. Вы это делали?
Вы: Нет, я вообще в другом городе!
Злоумышленник: Я так и думал. Сейчас мы зафиксируем попытку хищения. Но проблема в том, что в банке утечка, и там сидят недобросовестные сотрудники. Чтобы спасти ваши деньги, мы временно переведем их на «защищенные ячейки Центробанка». Никому не сообщайте, это тайна следствия. Сейчас пришлем фото удостоверения.
(Присылает в WhatsApp фото поддельного удостоверения с фотографией реального полицейского, взятой из сети).

Индикаторы обмана:

· Срочность: «Сделайте это немедленно, иначе украдут всё».
· Секретность: «Никому не говорите о разговоре».
· Несуществующие сущности: В природе не существует «безопасного счета Центробанка» для физических лиц.

3. Схема «Взлом Госуслуг» (и продление сим-карты/полиса ОМС)

Сценарий:
Звонок от имени оператора связи: «Ваш договор на номер зака

нчивается завтра, продлим дистанционно, продиктуйте код из СМС».
Пример развития атаки:

Как только вы диктуете код, аккаунт на Госуслугах перехвачен. Через 2 минуты вам звонит «Росфинмониторинг»: «Мы видим, что от вашего имени прямо сейчас запрашиваются кредиты в пяти банках. Чтобы отменить заявки, нам нужно идентифицировать вас через биометрию. Скажите под запись: «Я, ФИО, подтверждаю получение кредита на 300 тысяч»

Итог: Вы сами произносите фразу для биометрической системы банка, и кредит уходит мошенникам.

4. Инвестиционное мошенничество (Лжеброкеры и трейдинг)

Схема «Свинобойня» (Pig Butchering):
С вами неделями дружат в соцсетях, ведут романтическую переписку или просто общаются. Новый знакомый случайно проговаривается, что работает аналитиком и знает инсайд.
Пример:
«Друг»: «Слушай, есть инсайдерская информация по газу/крипте. Я сам в доле, но как друг дам тебе доступ к платформе. Закинь 50$ ради интереса».
> *Вы закидываете, видите на сайте рост графика, можете вывести даже 100$ прибыли.*
«Друг»: «Видишь, работает! Давай бери кредит, сейчас скачок акций Теслы, закроем сделку и купим тебе квартиру».
Ловушка: Сайт — поддельная платформа, где график рисуется вручную. Как только сумма вклада становится крупной (миллион рублей и более), кнопка вывода перестает работать, «брокер» испаряется.

УНИВЕРСАЛЬНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

1. Код — это пароль. Запомните: ни одна государственная служба (Госуслуги, банк, полиция) НИКОГДА не просит продиктовать код из СМС. Фраза «продиктуйте код» — стопроцентный признак афериста.
2. Правило нулевого доверия. Если разговор начался с финансов, недвижимости или безопасности — нажмите «Отбой». Невозможно понести ущерб от мошенника, если вы первым прервали диалог.
3. Анализ номера. Если звонок идет якобы из банка, но с мобильного номера +7-9XX-XXX-XX-XX — это обман. Реальные звонки из контакт-центров часто идут с коротких номеров или 8-800.
4. Биометрия. Никогда не произносите вслух фразу «Я подтверждаю» или «Да» в разговоре с неизвестными. Ваш голос могут записать и скормить системе голосовой идентификации банка.
5. Контакт-центр. Если вам сообщили о подозрительной операции, кладите трубку и перезванивайте по номеру, написанному на обороте вашей пластиковой карты.

Что делать, если вы уже стали жертвой:

1. Немедленно позвонить в свой банк и заморозить счета (сообщить о несанкционированной операции).
2. Подать заявление в ближайшее отделение полиции. Чем быстрее (минуты, а не дни), тем выше шанс заблокировать перевод на счете получателя.
3. Сменить пароли от Госуслуг и почты, привязанной к ним.

Помните: мошенники играют на эмоциях — страхе, жадности и любви. Эмоциональная пауза в 10 секунд перед любым финансовым решением спасает сбережения.