**Кибербезопасность и защита от телефонных мошенников**

тезисы для ЕИД

1. **Кибербезопасность и защита от телефонных мошенников в сегодняшних условиях наиболее актуальное направление финансовой грамотности населения. Несмотря на все оперативные и профилактические мероприятия, наблюдается рост количества преступлений и украденных денежных средств. Во многом это обусловлено развитием цифровых технологий.**

Среди разнообразных схем работы мошенников угрозу №1 представляет социальная инженерия. Социальная инженерия - это совокупность психологических и социологических приёмов, которые позволяют обманным путем либо получить конфиденциальную информацию у гражданина (данные его банковской карты, пароль от личного кабинета на госуслугах, смс-коды для входа в мобильное приложение банка и т.п.), либо заставить человека самостоятельно перевести (передать) деньги мошенникам.

Более 90% преступлений в сфере информационных технологий совершены с использованием социальной инженерии. Рост доли бесконтактных преступлений с использованием социальной инженерии (главным образом телефонное мошенничество) за 10 лет составил более 827% .

Телефонными мошенниками в России совершается 8,6 млн. звонков в сутки.

В Чувашии только за 2022 год– более 3500 человек стали жертвами мошенников, ущерб составил - почти 500 млн.руб.

За 1-е полугодие 2023 года – потерпевших от мошенников уже 2 140 человек, ущерб составил более 400 млн.руб.

**2. Причины попадания граждан на удочку мошенников:**

* самоустранение от реалий современной жизни, самонадеянность граждан;
* недостаток цифровой грамотности в части защиты своих электронных устройств от проникновения и бережного отношения к своим персональным данным;
* отсутствие знаний о методах социальной инженерии, IP-телефонии, технологии DeepFake;
* доверие к *значимому «титулу»* звонящего (сотрудник банка, правоохранительных органов, социальной службы и т.п.) и предоставление ему критичной информации или осуществление иных действий;
* незнание технологии работы банков, правоохранительных или иных государственных структур;
* недостаточные навыки критического мышления.

**3. Как мошенники получают доступ к средствам людей:**

-Интернет мошенничество или удаленное получение критической информации о доступе к финансам граждан путем вирусного заражения цифровых устройств, через фишинг (рассылки смс, сообщений в социальных сетях и мессенджерах, электронных писем с опасными ссылками на сайты, где выманивают деньги или воруют персональные данные);

- Фальшивые интернет-магазины;

- Телефонное мошенничество (социальная инженерия) – жертва сама все делает по указке мошенника.

**4. Интернет мошенничество.**

Мошенники делают рассылку по электронной почте, смс, в соцсетях или в мессенджерах. Она состоит из мотивирующего текста письма и ссылки или QR-кода на мошеннический ресурс. Выглядят послания как отправленные из компаний, пользующихся доверием.

Примеры:

* Сообщение о блокировке профиля на другом ресурсе. Указываются причины: взлом пароля, рассылка спама, черный список, нехватка памяти.
* Предложение оплатить со скидкой штраф ГИБДД или другой подобный платеж.
* Предложение установить полезную программу, скачать книгу или фильм.
* Сообщение со взломанного аккаунта в соцсетях или мессенджерах с просьбой пройти опрос, проголосовать в фотоконкурсе и так далее.
* Предложение купить популярный товар с большой скидкой на сайте-подделке под известную торговую платформу.
* «Вам положена социальная выплата!».
* Выигрыш в лотерею или в конкурсе.

Как защититься:

* Установите и регулярно обновляйте программу-антивирус с функцией защиты от фишинговых писем и нежелательной рассылки.
* При получении ссылки по электронной почте проверьте адрес отправителя, серьезные компании не делают рассылок с бесплатных почтовых сервисов. Если поле «Отправитель» не заполнено, это наверняка массовая фишинговая рассылка.
* При получении ссылки в социальных сетях или мессенджерах не открывайте вложения и не переходите по ссылкам от даже от известных отправителей.
* Пользуйтесь браузерами со встроенной антифишинговой защитой.
* Даже если источник доверенный, тщательно проверьте адрес: он должен полностью совпадать с адресом официального ресурса, который можно найти через поисковик.
* Подключите подтверждение платежа по паролю, который банк присылает в смс.
* Подключите оповещения об операциях с банковской картой.
* Установите двухфакторную аутентификацию (по коду из смс) на все ресурсы, которые позволяют это сделать.

**5. Типы фальшивых интернет-магазинов:**

* Одностраничный сайт с огромной скидкой. Чаще всего без указания номера телефона и дополнительных контактных данных. Призывают к тому, что нужно поторопиться, например, «Только сегодня скидка составляет более 50%!»
* Интернет-магазин копия. Есть телефоны, социальные сети, юридическая информация. Отлично проработан дизайн, визуал сайта.
* Основные признаки мошеннического магазина:
* Нет дополнительных контактных данных.
* У магазина нет отзывов, домен новый.
* Нет способа оплаты картой или же оплата производится переводом на карту физического лица.
* Чрезмерно навязчивое общение по телефону с целью быстрой продажи.

Как защититься:

* Проверять наличие на сайте магазина реквизитов, контактов, адресов, информации о возврате, точного описания гарантий.
* Критически относиться к предлагаемой в Интернете стоимости товара или услуги (узнавайте среднюю стоимость аналогов).
* Изучать особенности домена. Он должен быть первого уровня (тип «названиемагазина.ru»), а не созданным на конструкторе (например, тип названиемагазина.narod.ru).
* Анализировать отзывы.
* Завести и использовать отдельную виртуальную карту или мгновенную карту для онлайн-оплаты и пополнять ее ровно на ту сумму, которая нужна для оплаты.
* Визуально проверять адрес сайта магазина. Безопасным является адрес сайта, использующий защищенный протокол https (если адрес сайта магазина начинаться с http, данные передаются в незашифрованном виде и могут быть похищены, даже в случае, если магазин это не планирует) и имеющий индикатор надежности в виде замка. Если браузер выдает предупреждения о том, что соединение «не защищено» не совершайте покупок на таком сайте.

**6. Телефонное мошенничество (социальная инженерия) самый распространенный способ:**

* + - ***Звонки по телефону.***
    - ***Звонки через мессенджер****. При таком звонке* ***на аватарке виден логотип известного банка, Госуслуг или эмблема МВД (ФСБ, Следственного комитета и т.п.), или другие легко узнаваемые логотипы,*** *присылают якобы фото документов и удостоверений и т.п.*
    - ***Видеозвонки через мессенджер.*** *Имитация звонка из офиса банка, подразделения полиции (ФСБ и т.п.) с последующими аналогичными действиями.*
    - ***Использование курьеров*** *для доставки фиктивных писем, получения денег.*
    - **Технология** **DeepFake.** *Это специальные методы обучения нейросетей. Такую сеть можно научить чему угодно: достаточно дать ей правильные данные, а она сможет воспроизвести голос, фото или видео изображение нужным образом. Несколько месяцев назад мошенники подделали голос директора банка и звонили подчиненным от его имени.*

**7. Наиболее частые предлоги, с которыми мошенники обращаются к жертве:**

* «Попытка хищения средств или имущества», «попытка получения кредита другим лицом»…
* «Оказание помощи полиции (прокуратуре, следственному комитету и т.п.), участие в операции по поимке злоумышленников в банке» для «Задержания работников банка с поличным».
* «Расследование по факту финансирования ВСУ».
* «Родственник «попал в беду», «Нужны деньги для проверяющих из вышестоящей организации».
* «Блокировка карты», «проблемы» с личным кабинетом на сайте Госуслуг, у оператора мобильной связи и т.п.
* «Компенсации» («страховки») за перенесенные заболевания, выплаты «в связи с СВО» и т.п.

После этого всегда - «необходимость»  дальнейшего перевода денег на «специальный счет», «безопасный счет» и иные счета, указанные преступниками, или «необходимость» подтверждения реквизитов (номера карт, пароли, поступившие смс, введение кодов на телефоне и т.п.) якобы для «разблокировки» счета, защиты и др.

**8.**  **Психологическая схема социальной инженерии:**

* Звонок с неизвестного номера от «значимого сотрудника ФСБ, МВД. Банка и т.п.» с использованием технологии подмены номера и специфической терминологии.
* Выведение жертвы из душевного равновесия (страх, эйфория).
* Закрепление, подтверждение «достоверности» информации из «другого источника» в т.ч. с использованием фиктивных документов. Фото служебных удостоверений и т.п.
* Нагнетание «срочности».
* Запрет на общение с другими лицами, инструктаж о «легенде».
* Длительное удержание жертвы «на телефоне».
* Управление по телефону действиями жертвы.

Дополнения:

* Воздействие с отлагательным эффектом: разделение звонков от «разных источников» по времени.
* Побуждение к совершению теракта, хулиганских, иных противоправных действий.

**9.** С**амые простые правила финансовой безопасности в сфере телефонного мошенничества:**

* Отнестись с недоверием к звонку и критически оценить информацию.
* Вспомнить, что мошенники существуют (независимо от нашего желания).
* Вспомнить, что возможна подмена номера, а также изображения и голоса (видеозвонок).
* Вспомнить, что ни банки, ни правоохранительные органы и иные госструктуры: никогда не требуют от Вас информацию, не требуют куда-то переводить Ваши деньги или получать кредиты, не просят передать деньги кому-либо или установить какие-либо программы, не используют каких-либо номеров, кроме официальных, или интернет-кошельки, не привлекают клиентов к оперативно-розыскным и следственным мероприятиям, не направляют фотографии своих удостоверений, не общаются по несколько часов непрерывно по телефону и т.п.
* Не совершать никаких действий.
* Сразу прервать разговор и лично перезвонить или зайти в ближайший филиал банка (подразделение полиции и др.).

**10. Вывод:** **главное правило – НИЧЕГО НЕ ДЕЛАТЬ!**

* + не сообщать вообще никаких сведений
  + не совершать никаких действий с деньгами и имуществом
  + не устанавливать никаких программ
  + не нажимать никаких кнопок на телефоне или ином гаджете
  + не переходить по присланным ссылкам и т.п.

**11. Единственное правильное действие:**

Немедленно прервать разговор, не брать телефон при повторных звонках, или (если ответили) не вступать в разговор, несмотря ни на какие уговоры, угрозы и т.п.

**Если закрались сомнения:**

* лично перезвонить в Банк, полицию и т.п. по известному вам номеру,  заблокировать свои карты, сообщить о звонке.
* позвонить своим близким (детям, родным, знакомым)

**12.**  **Если вы все же успели сообщить какие-то сведения о себе, своих счетах, картах и т.п., необходимо:**

- Немедленно прервать разговор.

- Срочно позвонить в Банк по известному вам номеру, сообщить о случившемся и немедленно инициировать блокировку своих карт, счетов, прекращение каких-либо сделок от Вашего имени.

- сообщить о данном звонке и о случившемся в полицию (сохранив номер звонившего).