развода на инвестиции. По мере развития криптовалют и финансовых пирамид они начнут продвигать фальшивые инвестиционные проекты, представляясь аналитиками или консультантами. В частности, аферист убедит жертву вложить деньги, обещая высокий доход, после чего исчезнет.

Обман с помощью клона Госуслуг

В сети Интернет появляются клоны Госуслуг в виде страницы для подачи заявления о мошенничестве в Центробанк. Человек заполняет форму, а для её отправки клон запрашивает код из СМС. Естественно, это код для входа на Госуслуги. Если человек отправляет код мошенникам, то теряет доступ к аккаунту. Коварство ситуации в том, что жертва может угодить в ловушку повторно: люди подают жалобу на мошенничество, с которым столкнулись, и тут же снова попадают на мошенников.

Как защититься

Код из SMS нужен только для входа на Госуслуги – это второй этап двухфакторной аутентификации. При подаче заявлений на портале никаких кодов не требуется.

Не переходите на Госуслуги по подозрительным ссылкам, пользуйтесь мобильным приложением или официальным сайтом с доменным именем gosuslugi.ru – любое другое название портала в адресной строке должно насторожить.

Предпраздничное «кидалово»

Подарочные сертификаты в магазины, салоны, спортзалы – популярные праздничные презенты, и мошенники решили заработать на этом. Они предлагают в мессенджерах и соцсетях купить сертификат по цене чуть ли не вдвое дешевле номинала, объясняя это акцией в честь праздника.

К сообщению или посту прилагают ссылку, которая ведёт на фишинговый сайт или в чат-бот. Там нужно заполнить форму обратной связи и, естественно, ввести код из SMS, чтобы открыть хакерам вход в свой онлайн-банк или на Госуслуги.

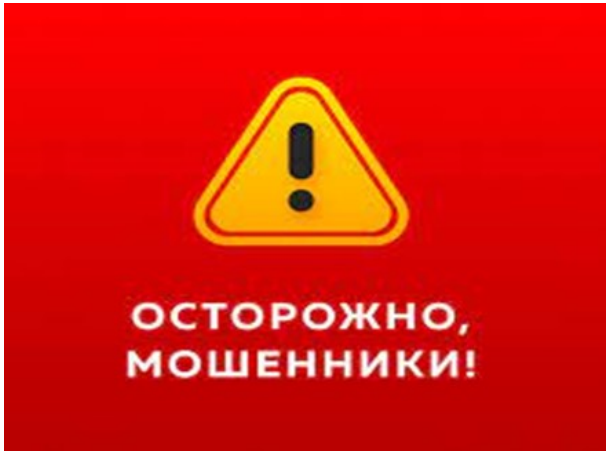
ОСТОРОЖНО!
Будьте бдительны, внимательны не поддавайтесь на уловки мошенников.
Если вы знаете о случаях мошенничества или сами стали жертвой злоумышленников, немедленно сообщите об этом в полицию по телефону 102.

УМВД России по Тюменской области
625000, г. Тюмень, ул. Водопроводная, 38,
тел. 8 (3452) 793-023 или 102,
тел. 8 (3452) 793-023 или 102
(для абонентов мобильной связи).

Совет при Тюменской областной Думе по повышению правовой культуры и юридической грамотности населения Тюменской области

Управление МВД России по Тюменской области

ПАМЯТКА



ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

г. Тюмень, 2025

Как мошенники обманывают детей

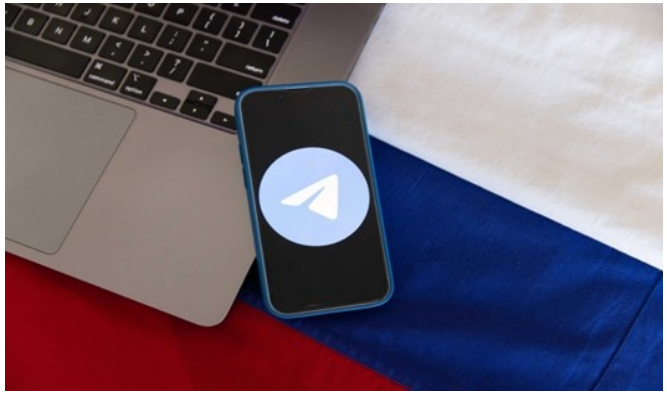
Преступники применяют методы социальной инженерии, чтобы добраться до счетов взрослых через их детей, запугивая с помощью звонков от «должностных лиц».

Мошенники звонят ребенку, представляясь сотрудниками полиции, службы безопасности или других организаций, и сообщают о «чрезвычайной ситуации». Злоумышленники призывают детей перевести деньги родителям, которым якобы угрожает опасность.

Мошенники также связываются с ребенком, чтобы сообщить ему о якобы выигранном призе в онлайн-игре или о возможности купить игровую валюту. Преступники просят школьника сообщить данные карты, чтобы «перевести заслуженные деньги».

Кроме того, преступники под предлогом защиты или помощи просят ребенка установить программы для получения удаленного доступа к смартфону. Таким образом, мошенники могут управлять банковскими приложениями взрослых членов семьи.

Какие появляются новые методы мошенничества



Обман в популярных мессенджерах Telegram и WhatsApp:

- создание фейковых аккаунтов компаний и служб поддержки;

- рассылка фишинговых ссылок (собирают конфиденциальную информацию, логины и пароли) через ботов;

- использование искусственного интеллекта для создания поддельных диалогов.

Мошенничество в финансово-технических сервисах:

- работа на поддельных криптовалютных платформах;

- кража данных через фальшивые банковские приложения;

- мошенничество на платформах NFT (продают уникальную цифровую валюту, часто в виде изображений).

Использование кризисов и актуальных событий:

- создание поддельных сайтов помощи;

- объявление о ложных благотворительных акциях;

- атаки, в том числе фишинговые (сбор конфиденциальных данных, логинов и паролей), на корпоративных пользователей.

Схемы с искусственным интеллектом:

- использование глубоких фейков для создания поддельных видео или аудио, имитирующих известных личностей или коллег;

- атаки с применением генеративных моделей ИИ для создания фишинговых писем, текстов и сообщений, которые трудно отличить от настоящих.\

Какие способы обмана придумают мошенники в 2025 году

В 2025 году телефонные мошенничества могут стать более изощренными за счет новых технологий и изменения привычек людей. Одной из главных угроз будут звонки с подменой номеров и синтезированным голосом. Это инструменты так называемого спуфинга – метода, при котором киберпреступник подменяет данные, чтобы выдать себя за другое лицо, организацию или устройство.

Злоумышленники уже используют спуфинг. С развитием искусственного интеллекта они смогут в реальном времени воспроизводить голос родственника, коллеги или сотрудника банка. Это приведет к появлению новых видов обмана, когда жертва будет уверена, что разговаривает с настоящим человеком.

Еще одним трендом станет утечка данных. Сейчас мошенники анализируют информацию из слитых баз, но в будущем их звонки станут еще более персонализированными. Они будут называть реальные номера заказов, имена друзей, данные о покупках и поездках, чтобы не вызвать подозрений у потенциальной жертвы. Например, человеку позвонят якобы из службы поддержки сервиса, которым он недавно пользовался.