Они сказали, что не мошенники: как не потерять персональные данные и сбережения — рассказали эксперты

24.09.2025

Не будем отрицать, что развитие цифровых технологий значительно облегчило выполнение рутинных задач, на которые раньше приходилось затрачивать больше усилий. Например, многие ежедневно пользуются доставкой готовой еды или продуктов из магазина, маркетплейсами, интернет-магазинами, чтобы сэкономить свое время. Кроме того, практически каждый имеет аккаунт на “Госуслугах” и активно ведет социальные сети, что может стать мишенью для кибермошенников.

Злоумышленники активно адаптируются к изменениям и придумывают все более изощренные сценарии для обмана людей. Существуют несколько основных:

- **Псевдозвонки.** Злоумышленники представляются операторами сотовой связи и утверждают, что у клиента якобы заканчивается контракт, по которому оказывают услуги. Так мошенники просят жертву предоставить персональные данные.
- **Звонки от лже-представителей служб безопасности банков или Центробанка**. Потенциальной жертве сообщают, что якобы предотвращают действия мошенников и просят её перевести деньги на “безопасный счет”.
- **Обращения для замены услуг домофона**. Мошенники представляются сотрудниками “общероссийского сервиса” и просят жертву назвать код из

> SMS. Таким способом злоумышленники пытаются завладеть доступом к банковскому приложению, личному кабинету или другому сервису.

По словам экспертов, в последнее время прослеживается тенденция вовлечения детей в преступления, связанные с кибермошенничеством. В преступном синдикате злоумышленников существует особая иерархия, на низшей её ступени находятся рядовые исполнители, которые выполняют самую рискованную работу, и следуют указаниям так называемых кураторов. Они могут предлагать детям стать дропперами — посредниками по отмыванию или обналичиванию денежных средств. Так, несовершеннолетние нередко становятся фигурантами уголовных дел.

Чтобы обезопасить детей от угроз, в России был создан Альянс по защите детей в цифровой среде, который занимается просвещением в вопросах кибербезопасности. Одним из основателей организации выступил ”Ростелеком”. Провайдер регулярно проводит семинары и обучающие мероприятия, а также создает разделы на информационных ресурсах с целью повышения цифровой грамотности населения.

Ещё одним действенным методом является функция «Защита звонка». С помощью искусственного интеллекта оператор в среднем за 18 секунд идентифицирует, является ли звонок мошенническим. При выявлении признаков мошенничества абонент получает голосовое предупреждение, которое слышит только он. Это позволяет безопасно завершить разговор, не раскрывая осведомленность.

Ирина Лебедева, вице-президент по продуктам массового сегмента «Ростелекома»:

> «Наши абоненты высоко оценили запущенные этим летом сервисы для безопасного использования домашнего интернета и мобильной связи. Новый продукт благодаря современным технологиям защищает “в прямом эфире”, даже если мы имеем дело с подменой номера или другими уловками. В условиях роста угроз киберпреступлений и постоянного появления новых мошеннических схем мы продолжаем развивать методы борьбы с ними и предлагаем новые решения, оставаясь лидерами в сфере кибербезопасности».

Как уточняют эксперты, злоумышленники стараются собрать как можно больше персональной информации о потенциальной жертве, поэтому следят за ней в интернете. По этой причине пользователям рекомендуют оставлять как можно меньше личных данных о себе в комментариях к записям других пользователей или на личной странице. В идеале можно закрыть аккаунты в социальных сетях.

Также важно информировать своих близких — детей и родителей — о наиболее массовых сценариях мошенничества, продумать стратегию взаимодействия в таких случаях. Как правило, злоумышленники звонят с разных номеров, не давая человеку времени проанализировать ситуацию. В таких случаях рекомендуется обратиться к третьей стороне — родственникам или правоохранителям, чтобы не принимать решение скоропалительно.

18+

г. Новосибирск, ул. Ермака, 39.